В наше время технологический прогресс проникает в любую сферу жизни. Не стали исключением как бытовые аспекты, так и производственные. Несмотря на то, что технологии призваны помогать людям и упрощать их жизнь, они одновременно с этим выступают как опасные элементы.

С помощью технологий в современных реалиях можно достичь много, но зачастую, помимо развития и помощи, научно-технический прогресс используют как оружие. В условиях рыночных отношений, где конкуренция, увы, не всегда носит честный и добросовестный характер, техника и технологии превращаются в инструмент шпионажа и воровства. Именно высокий уровень информационно-технологических угроз обуславливает актуальность выбранной темы. Целью данного эссе ставится отражение объективной картины применения технологических средств в целях промышленного шпионажа.

В данном эссе планируется отразить ответы на следующие вопросы:

- что такое промышленный шпионаж и какие технические средства применяются для добычи секретной информации?

- какова объективная статистика, отражающая последствия промышленного шпионажа;

- что можно сделать для того, чтобы обезопасить себя и свою компанию от шпионов.

Отвечая на данные вопросы, будет раскрыта выбранная тема эссе в требуемом качестве.

Сущность технологического шпионажа и его последствия

Промышленный шпионаж – это одна из форм недобросовестной конкуренции. По сути представляет собой добыча секретной информации/корпоративной тайны чужого предприятия незаконным путем. Целью такой деятельности служит получение информации о слабых местах своих конкурентов, чтобы получить преимущество своей компании на рынке, а заодно уничтожить или подавить своего противника.

Не стоит путать «промышленный шпионаж» и «промышленную разведку». Первое – это грубое нарушение закона, преследующее опасные цели. По сути, такое может погубить национальную экономику.

Формы промышленного шпионажа разнообразны: взяточничество, шантаж, кража носителей информации, внедрение своего агента в компанию-конкурента, незаконный доступ к секретной информации, слежка и техническое наблюдение за объектом шпионажа.

Нетрудно догадаться, что все это не обходится без использования технологий. Например, к акустическим средствам можно отнести средства прослушки (жучки), которые легко можно оставить в кабинете нужного нам лица, тем самым сразу же получать доступ ко всей интересующей нас информации. Они обеспечивают прослушивание переговоров на больших расстояниях за счет узкой направленности приемных устройств. Основа таких микрофонов - это узконаправленные антенны, настроенные на определенную частоту, за счет этого воспринимается приходящий сигнал только расчетной частоты и не воспринимаются сигналы с других направлений. Конечно, бывает и такое, что качество звука не всегда на высоте, потому шпион не получает 100% нужной информации.

Существуют и проводные каналы, используемые в качестве средства шпионажа. Данный канал утечки информации использует устройства, преобразующие акустический сигнал в электромагнитный - микрофон, диктофон. Уловленный акустический сигнал специально проложенными двумя проводами передается в соседнее помещение (где находится агент) и телефоном преобразуется из полученного электромагнитного сигнала обратно в прослушиваемый акустический.

Визуальные способы – фотография/видеосъемка. Сейчас очень легко с помощью мобильных телефонов передать любую информацию, а также запечатлеть ее на долгую память.

Наиболее популярный способ – электромагнитные каналы утечки. Перехват электромагнитных волн, которые излучаются, например, при телефонных переговорах, позволяет подслушать важный разговор. Также можно легко считать информацию с компьютерного дисплея, что сразу позволяет получить доступ ко всем данным учетной записи конкретного пользователя.

Помимо того, что шпион получает всю ненужную о конкуренте информацию, которую он может с легкостью использовать против него, совершив рейдерский захват, это может разрушать национальную экономику (ведь компании гибнут,

начинается становление монополии, что приводит к снижению качества жизни населения), да и рост уголовных преступлений на фоне это растет: взяточничество, рейдерство и ряд других преступлений – это негативно сказывается как на экономике, так и на состоянии общества.

Что можно сделать для того, чтобы обезопасить себя и свою компанию? Не секрет, что успех защиты организации от утечек информации и от промышленного шпионажа во многом определяется её кадровой политикой. Именно поэтому важно обращать внимание на психологическую составляющую обеспечения информационной безопасности организации.

Однако и без технических средств, понятное дело, тоже никуда. Наиболее эффективным решение против промышленного шпионажа сегодня являются DLP-системы – программные продукты, действующие по принципу виртуального защитного контура информационной безопасности, окружающего каждую рабочую станцию в корпоративной информационной сети. Сокращение DLPрасшифровывается как DataLeakPrevention, то есть, предотвращение утечек данных. При обнаружении в передаваемых данных конфиденциальной информации DLP-система сообщит об этом в реальном времени специалистам по обеспечению информационной безопасности, и если это необходимо, то блокирует дальнейшую передачу данных. По оценкам экспертов, внедрение DLP-системы снижает вероятность успешного промышленного шпионажа против внедрившей такую систему компании, в среднем, в 2,5 раза.

Выводы

Подводя итоги, стоит подметить, что с промышленным шпионажем сталкивается любая компания, рано или поздно. На это не влияет ни размер, ни капитализации, не экономические показатели. Каждая компания одинаково подвергается риску.

Стоит обращать внимание не только на внешнюю защиту компании, но и тщательно следить за тем, что происходит внутри организации. Любой предприниматель должен помнить: что уровень уязвимости его предприятия зависит от того, какую политику защиты данных и политику информационно безопасности он выбирает. Пренебрегать этим в условиях рыночных отношений и высоких темпов развития технологий – крайне опасно.

Список использованной литературы

1. https://blogs.klerk.ru/users/1793540/post153814/ (Дата обращения: 07.12.2019)

2. https://aif.ru/money/business/11368 (Дата обращения: 07.12.2019)

3. https://nauchforum.ru/studconf/tech/xlvii/22849 (Дата обращения: 07.12.2019)