Теория и практика управления

УДК 334:681.3

КОНТРОЛЬ РЕЧЕВОЙ ИНФОРМАЦИИ – ОДНА ИЗ ГЛАВНЫХ СОСТАВЛЯЮЩИХ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Азаренко Е.В., Дивизинюк М.М., Рыбко В.В., Смычков Е.Е, Шумейко И.П.

Показано, что одним из главных каналов утечки информации, определяющим экономическую безопасность предприятия, является речевой канал.

Ключевые слова: *экономическая безопасность предприятия; конфиденциальная информация; угрозы информации; каналы утечки информации; речевой канал утечки информации.*

Экономическая безопасность предприятия ведущими специалистами [1-3] трактуется как наличие конкурентных преимуществ, обусловленных соответствием материального, финансового, кадрового, технико-технологического потенциалов и организационной структуры предприятия его стратегическим целям и задачам. Она складывается из ряда функциональных составляющих, которые для каждого конкретного предприятия могут иметь различные приоритеты в зависимости от характера существующих угроз. Одной из главных угроз, которой теоретически могут подвергаться абсолютно все предприятия – экономический шпионаж [4]. Он проводится в интересах укрепления своего положения за счет ослаблений позиций конкурентов, вплоть до их вытеснения с рынка и полного уничтожения за счет получения конфиденциальной информации, разглашение которой наносит ущерб фирме – собственнику этой информации.

Целью данной работы является характеристика речевого канала передачи информации как одной из главных составляющих экономической безопасности предприятия. Для достижения данной цели необходимо решить следующие научные задачи. Во-первых, определить, какая информация на предприятии является конфиденциальной. Во-вторых, рассмотреть возможные каналы утечки информации. В-третьих, рассмотреть свойства речевого канала передачи информации.

Конфиденциальная информация предприятия условно разделяется на две группы, а именно информацию ограниченного доступа и секретную (необходимо заметить, что эти «секреты предприятия» не обязательно являются государственной тайной).

К первой группе относятся сведения, разглашение которых причиняет ущерб тактическим интересам предприятия, то есть срыв конкретного контракта, снижение прибыли от проведенной сделки, осложнение условий выполнения отдельных соглашений, наложение финансовых или иных санкций со стороны партнера и другие. Разглашение секретной информации наносит серьезный ущерб стратегическим интересам фирмы, может поставить под угрозу само ее существование в дальнейшем. Ее составляют сведения, ознакомление с которыми конкурентам, неразборчивым в средствах, подорвать репутацию фирмы в глазах партнеров, причинить ей значительный финансовый ущерб, привести к конфликту с государственными органами, оставить в зависимость от криминальных структур и др.

Определение степени конфиденциальности служебной информации осуществляет, как правило, руководство фирмы, однако в любом случае к ней относится следующее. Это уставные документы предприятия, условия аренды помещений и техники, сводные валютные и гривневые отчеты, кредитные и другие договора, сведения о перспективных рынках, партнерах, источниках сырья и любая другая информация, предоставленная партнерами, за разглашение которой предусмотрены штрафные санкции.

Таким образом, конфиденциальная информация существует в материальной форме, а именно: в различных документах, чертежах, планах, схемах, фотографиях, отчетах, аналитических обзорах, образцах товаров и тому подобных, зафиксированных на бумаге, фотографиях, слайдах, дискетах, флэш-памяти, памяти персональных ЭВМ и других магнитных носителях.

Рассматривать возможные каналы утечки экономической информации будем при первом ус-

ловии, что весь персонал предприятия не участвует в шпионских акциях, т.е. фактор подкупа сотрудников полностью отсутствует. Второе условие заключается в том, что экономический шпионаж осуществляется только техническими средствами.

Первый – визуальный канал, в котором наблюдение ведется с помощью оптических устройств, сопряженных с фото- и видеоаппаратурой документирования. Это позволяет фиксировать людей заходящих и выходящих из дверей фирмы, вести наблюдения за окнами и другими объектами, входящими в поле деятельности предприятия.

Второй – инфракрасный (тепловизорный) канал, который позволяет вести визуальное наблюдение ночью, а так же распознавать людей и предметы за зашторенными окнами.

Третий – компьютерный канал, организуется атака на локальные сети предприятия с целью проникновения в базы данных, копирования электронных документов, чертежей и любой другой информации, находящейся в персональных компьютерах. Целью атак так же может быть уничтожение ряда документов, находящихся на сервере и персональной ЭВМ руководителя.

Четвертый канал – прослушивание телефонных переговоров, телефонов использующих проводные линии связи. Съем этой информации можно осуществлять в переходных коробках, устанавливаемых в подъездах; в связных колодцах, предназначенных для обслуживания кабелей связи; на телефонных станциях недобросовестными подкупленными сотрудниками, которые не являются сотрудниками предприятия, против которого осуществляется шпионаж.

Пятый канал – прослушивание радио и мобильных телефонов по радиоканалам с использованием специальной радиоприемной аппаратуры, стационарно установленной в соседних зданиях и мобильной, носимой агентами, осуществляющими сбор информации.

Шестой канал – подслушиванием разговоров, путем установки специальных устройств в непосредственной близости от окон, дверей офиса, личных квартир сотрудников предприятия, а так же в стенах смежных с офисом помещений.

Седьмой – лазерный канал, использование специальной лазерной техники, осуществляющей съем речевой информации за счет вибрации стекол на окнах помещений.

Таким образом, из семи возможных каналов утечки экономической информации при полной лояльности персонала, в четырех из них циркулирует речевая информация, съем которой и осуществляется.

Речевой канал передачи и утечки информации характеризуется шестью свойствами, отличающего его от других.

Во-первых, он наиболее информативен. Собеседникам в устной форме проще объяснить, что случилось, что надо делать и т.д. Те же события описать гораздо сложнее и потребуется гораздо больше времени. Кроме того, при беседе к передаче объективной информации за счет интонаций и мимики добавляется субъективная – личностная составляющая, которая для шпионских целей может быть важнее объективной информации.

Во-вторых, он является наиболее часто используемым. Любой руководитель, если у него есть возможность личного общения с исполнителем, всегда воспользуется каналом личного речевого общения. С другой стороны подчиненный, получивший определенный результат, с большим рвением об этом доложит руководителю, эмоционально рассмотрит все положительные и отрицательные моменты, которые в письменном виде излагать не станет.

В-третьих, этот канал не требует никакой дополнительной обработки при установлении прослушивания. Это свойство называют его доступностью.

В-четвертых, этот канал передачи информации легко документируется, что осуществляется включением диктофона или любого другого устройства, записывающего акустические волны, человеческую речь.

В-пятых, речевой канал передачи информации наиболее уязвим. Ранее выполненный анализ, который производился при полной лояльности персонала, показал, что в большей части каналов утечки информации циркулирует речевая информация.

Таким образом, речевой канал передачи информации характеризуется пятью свойствами, а именно: наиболее информативен, наиболее часто используем, наиболее доступен, легко документируем, наиболее уязвим.

ВЫВОДЫ

1. Конфиденциальная информация существует в материальной форме, а именно: в различных документах, чертежах, планах, схемах, фотографиях, отчетах, аналитических обзорах, образцах товаров и т.п., зафиксированных на бумаге, фотографиях, слайдах, дискетах, флэш-памяти, памяти персональных ЭВМ и других магнитных носителях.

2. Из семи возможных каналов утечки экономической информации, при полной лояльности персонала, в четырех из них циркулирует речевая информация, съем которой и осуществляется.

3. Речевой канал передачи информации характеризуется пятью свойствами, а именно наиболее информативен, наиболее часто используем, наиболее доступен, легко документируем, наиболее уязвим.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Концепции безопасности. Книга 1. /Бурышев В. С, Лутаев И. В., Прохоров С. Л. - К.: А-ДЕПТ, 2005. – 358 с.

2. Грамматчиков А. Информационная оборона // Эксперт. – 2006. – № 3 (503). – Режим доступа к журналу: http: // www.expert.ru/printissues/expert/2006/09/

3. Гладишенко М. Правові та організаційні аспекти діяльності підприємниця для захисту комерційної таємниці.// Персонал. – 2005. – № 3. – С.51-55.

4. Безопасность бизнесмена и бизнеса. Практическое пособие. /Тарас А.Е. – Минск: Сэкай, 1996. – 184 с.