

Индивидуальная работа
по дисциплине
«Экономика и организация работ по защите информации»

На тему:
«Защита телефонной линии на предприятии»

Выполнил студент Иванов Д.Я.

Задание

Определить возможные убытки при несанкционированном доступе к информации на предприятии. Определить необходимое оборудование и его суммарную стоимость для защиты телефонных переговоров.

Вероятность несанкционированного доступа $P=0,5$. Годовой оборот фирмы 1 млрд. руб.

Введение

Проблема защиты телефонных переговоров в условиях широкой телефонизации общества становится весьма актуальной, так как злоумышленники широко пользуются подслушиванием и служебных и домашних телефонов. При этом широко используются такие способы, как подключение к телефонным линиям, установка в телефонную линию телефонных радиозакладок, высокочастотное навязывание и другие варианты подслушивания. Наибольшее распространение получает установка телефонных радиозакладок.

В пространственно плане телефонная радиозакладка может быть установлена в помещении, где злоумышленнику необходимо контролировать телефонные переговоры. За пределами помещения радиозакладка может быть установлена в распределительной коробке и распределительном шкафу здания. Внутри здания особенно уязвим тракт от телефонного аппарата до распределительного шкафа. В этом случае возможна как установка радиозакладок, так и подключение к линии контактным или бесконтактным способом.

От распределительного шкафа до АТС положен многожильный кабель, подключение к которому весьма затруднительно.

На самой АТС возможно подключение и установка радиозакладки непосредственно к той или иной ячейке [1].

Многообразие возможных ситуаций определяет многообразие мер и способов защиты телефонных разговоров. Очевидно, что обеспечить безопасность телефонного канала связи сложно и дорого. В связи с этим часто используют устройства, позволяющие закрыть сообщения, передаваемые по телефонным каналам. Немаловажно поддержание дисциплины и четкая организация на предприятии.

Экономический подсчет

Проведем простейший подсчет возможных потерь на предприятии в следствии неуделения должного внимания защите телефонных линий.

В условиях рыночной экономики и жесткой конкуренции, благосостояние предприятия во многом зависит от подконтрольной ему доли рынка. В то же время, конкуренты перманентно совершают попытки “выдавить” предприятие со своей ниши, перехватить заказы, переподчинить себе долю рынка. В такой ситуации, потеря конфиденциальной информации зачастую влечет за собой потерю заказов, контрактов, и как следствие, прибылей.

В соответствии с заданием, вероятность попыток несанкционированного доступа (НСД) составляет 50%. Будем считать, что половина сделок фирмы может сорваться в следствии НСД со стороны конкурентов и прочих злоумышленников.

Таким образом, возможные потери (риск) предприятия определяются следующим выражением:

$$\text{Потери} = 0,5 \cdot 1 \cdot 10^9 = 0,5 \cdot 10^9 = 500 \text{ млн. рублей в год.}$$

На предотвращение убытков в следствии НСД к конфиденциальной информации обычно используют 2...20% от возможных рисков.

Рассчитаем ориентировочно допустимые затраты на защиту от НСД:

$$\text{Затраты на ЗИ} = 0,02 \cdot 0,5 \cdot 10^9 = 0,01 \cdot 10^9 = 10 \text{ млн. руб}$$

Следует учитывать, что защита информации осуществляется в комплексе. И полученная из расчета сумма тратится не только на защиту телефонного канала связи, но и на другие аспекты защиты информации. Отведем на защиту телефонных переговоров 10% от суммы, то есть 1 млн.руб.

Необходимое оборудование

Определимся с объемом работ по защите телефонного канала связи. Для этого воспользуемся таблицей «Способы противодействия подслушиванию телефонных переговоров» [1, стр. 234]

Таблица 1. Способы противодействия подслушиванию телефонных переговоров

Способы подслушивания	Способы противодействия	
	Выявления	Противодействия
1. Микрофонный эффект	Спец. измерения телефонных аппаратов на наличие микрофонного эффекта	1. Замена аппарата 2. Отключение аппарата от линии 3. Использование специальных устройств
2. Контактное подключение к телефонной линии	Контроль телефонных линий: - на наличие подключений - на изменение электрических характеристик линий - на изменение напряжения и тока	1. Прокладка кабеля в защищенных коммуникациях 2. Непрерывный контроль электрических характеристик 3. Электрическое уничтожение подключенных средств 4. Использование скремб-

		леров
3. Бесконтактное подключение к телефонной линии	Обнаружение мест возможного подключения индукционных датчиков	1. Использование экранированных кабелей 2. Исключение параллельного прокладывания линий 3. Зашумление линии связи
4. Установка телефонной радиозакладки с передачей сигнала по эфиру	Контроль наличия радиоизлучения при ведении переговоров в диапазоне телефонных закладок	1. Постановка акустических помех 2. Постановка электромагнитных помех 3. Изъятие радиозакладки
5. Установка телефонной радиозакладки с передачей сигнала по проводам	Контроль радиоизлучения при ведении переговоров в диапазоне средних волн	1. Установка в линию подавляющих фильтров 2. Зашумление линий связи акустическими и электро-механическими помехами
6. Высокочастотное навязывание	Контроль наличия радиоизлучения	1. Постановка электромагнитных помех 2. Установка в линию специальных фильтров высокой частоты
7. Установка дистанционно управляемого микрофона (телефонное ухо)	1. Контроль элементов телефонной сети 2. Запись на магнитофон сигналов в линии связи за пределами помещений	1. Постановка активных акустических помех микрофону

Для защиты телефонного канала связи на предприятии будем использовать следующий комплект оборудования:

Название	Описание	Характеристика	Цена
Прокруст-2000	Устройство защиты телефонных переговоров от прослушивания и записи.	Максимальная защита линии (от телефонного аппарата до АТС). Режимы работы: детектор, помеха, уровень, стробирование, блокировка.	29800 руб
TRTD-061	Анализатор телефонной линии	<p>Для обнаружения радиопередающих устройств на телефонной линии.</p> <p>Имеет многосегментную индикацию уровня радиополя на телефонной линии и вблизи телефонного аппарата, что позволяет с большей уверенностью определить наличие подслушивающих устройств. При обнаружении "жучка" прибор "не вешает трубку", что значительно упрощает эксплуатацию в сложной радиообстановке с большим количеством ложных срабатываний.</p> <p>Имеется настройка чувствительности измерителя радиополя.</p> <p>ВЧ-фильтр защищает Ваше помещение от прослушивания через телефонный аппарат и линию.</p> <p>Линейный выход позволяет вести запись телефонных разговоров на диктофон.</p> <p>Новая функция-индикация уровня напряжения на линии в звуковом диапазоне позволяет обнаруживать прослушивание через микрофон телефонного аппарата (секретная функция миниАТС).</p> <p>Имеет индикацию прослушивания через спикерфон, индикацию параллельного подключения к линии, фильтр против ВЧ-навязывания, выход для записи разговоров на диктофон.</p>	7500 руб
Итого:			37'300 руб

Полученная сумма затрачивается на покупку оборудования. Монтаж систем в стоимость не входит. Для приблизительной оценки стоимости монтажа воспользуемся правилом: стоимость монтажа соизмерима со стоимостью оборудования. Тогда суммарная стоимость оборудования и монтажа примерно 70 тыс. рублей (на один телефонный канал).

Следует добавить, что обладая достаточными финансовыми возможностями (см. выше), фирма может позволить себе покупку многофункционального прибора Улан-2. Это универсальный анализатор проводных коммуникаций. Использование этого прибора возможно не только при защите телефонных каналов но и при других работах по предотвращению НСД на предприятии. Стоимость прибора 80 тыс. рублей.

Прибор "ULAN-2" предназначен для обнаружения фактов несанкционированного подключения к различным проводным коммуникациям, таким как телефонные линии, электрические сети 220 В, компьютерные сети, линии охранной сигнализации и т.п. Прибор способен не только выявить и идентифицировать обнаруженные устройства, но и, используя метод импульсной локации, с высокой точностью измерить расстояние до места несанкционированного подключения.

Прибор Улан-2 позволяет обнаружить следующие виды несанкционированного подключения:

В телефонных линиях (без отключения от АТС и без наличия предварительной информации):

- последовательные подключения с эквивалентным сопротивлением более 30 Ом;
- параллельные подключения в режиме с током потребления более 0,1 мА;
- высокочастотные сигналы в линии в диапазоне 0,02 ÷ 30 МГц с эффективным напряжением более 10 мВ при симметричном и несимметричном подключениях,
- низкочастотные сигналы в диапазоне 20 ÷ 20000 Гц с эффективным напряжением более 10 мВ.

В линии электросети 220 В под напряжением:

- "сторожевые устройства" с током потребления более 0,1 мА.
- высокочастотные сигналы в диапазоне 0,02-30 МГц с эффективным напряжением более 10 мВ

В обесточенных линиях:

- параллельные подключения с активным сопротивлением до 200 МОм;
- последовательные подключения с активным сопротивлением более 1 Ом;
- параллельные подключения через конденсатор, с постоянной времени более 100 мкс;
- наличие элементов с выраженной нелинейностью от 5 % и выше в диапазоне напряжений 0 ÷ 100 В;
- наличие реактивных элементов с емкостью более 100 пФ и индуктивностью более 10 мГн (без учета собственных параметров линии).

Кроме указанного, прибор "ULAN-2" позволяет:

- производить измерения напряжения постоянного и переменного токов в проверяемой линии;
- производить измерения сопротивления, емкости и индуктивности проверяемой линии;
- производить измерения тока короткого замыкания и сопротивления шлейфа телефонной линии;
- прослушивать аудио сигналы в проверяемой линии с использованием головных телефонов;
- выводить на экран встроенного дисплея следующую графическую информацию о проверяемой линии: вольт-амперную характеристику, импульсную переходную характеристику, нагрузочную характеристику телефонной линии, параметрическую зависимость выходного тока от входного гармонического напряжения (т.н. фигуры Лиссажу), импульсные рефлектограммы линий;
- хранить числовые и графические результаты измерений в энергонезависимой памяти;
- передавать накопленную информацию в персональный компьютер по высокоскоростному интерфейсу USB;
- совместно с прибором UP-7 прослеживать трассу прокладки проверяемой линии в стенах и строительных конструкциях.

Изделие сертифицировано: Сертификат соответствия Госстандарта России № РОСС RU. АЕ63.Н00108, сертификат Гостехкомиссии России № 922

Вывод

Защита информации, и в частности защита телефонного канала связи от НСД, является дорогостоящим мероприятием. Однако, невыполнение работ по защите информации может привести к убыткам, во много раз превосходящим затраты на защиту информации, что делает её необходимым для любого современного предприятия.

Использованные источники:

1. В.И.Ярочкин «Информационная безопасность. Учебник для студентов вузов» – М.: Академический Проект, Гаудеамус, 2-е изд. – 2004. – 544 с.
2. www.centers.ru
3. www.felix-security.ru
4. www.infosecur.ru