

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Жлобо М.В.

Королев А.И. – к.т.н., доцент

21-й век демонстрирует исключительно бурное развитие средств связи. Особенно заметны эти изменения в технике и технологии телефонной связи.

Создавая новые сервисные возможности для пользователей, современная техника телефонной связи продолжает оставаться наиболее привлекательной для целей шпионажа, шантажа, устремлений преступных элементов и др.

За достаточно длительный период своего развития человечество накопило огромный опыт и массу знаний о способах и средствах ведения разведки. Естественно, вначале этот опыт носил в основном военный характер, но затем он нашел благодатную почву для "мирной" реализации на уровне промышленного шпионажа. Одним из основных способов ведения разведывательных действий является получение доступа к каналам передачи информации, которыми пользуется конкурирующая сторона. В первую очередь, как правило, нападению подвергаются каналы телефонной связи, по которым, кроме речевой информации, передаются факсимильные, модемные сообщения. Также линии связи с подключенными к ним телефонными аппаратами часто представляют собой нечто вроде "черного хода" в помещение, поскольку большинство телефонных аппаратов ввиду несовершенства конструкции допускают утечку из помещения акустической информации.

В телефонном аппарате (ТА) электрические сигналы распространяются в линиях связи в открытом виде. Практически любой злоумышленник, имея соответствующее оборудование, может получить доступ к конфиденциальной информации, передаваемой в ТА, используя: непосредственное подключение к телефонным линиям связи; бесконтактный съем информации и "жучки"; излучение в радио- и оптическом спектрах частот.

Возможный перечень угроз абоненту показан на рис. 1.



Рис. 1. Перечень угроз абоненту

Все разнообразие технических средств съема информации или их составных частей можно свести к 3-м основным группам:

- средства конспиративного подключения к телефонным линиям и средства передачи информации от них,
- средства коммутации и анализа телефонных каналов,
- средства одноканальной и многоканальной адресной записи телефонных разговоров.

Современные способы защиты телефонных линий можно разбить на две основные группы:

- организационные;
- технические.

Под **организационными способами** понимается комплекс организационно-правовых и организационно - технических мероприятий, проведение которых исключали бы или, по крайней мере сводили к минимуму возможность перехвата телефонных переговоров с линии. Данные способы основаны на ограничении физического доступа к линии и аппаратуре связи и на преобразовании сигналов в линии к форме, исключающей (затрудняющей) для злоумышленника восприятие или искажение содержания передачи.

Под **техническими способами** противодействия понимается применение на телефонных линиях средств анализа и контроля, специальных технических средств защиты

На рис. 2 приведена классификация средств и способов защиты телефонной линии.



Рис.2. Классификация средств и способов защиты телефонной линии

Для организации комплексной защиты информации необходим полный анализ всех возможных угроз, методов и средств защиты, а также экономический анализ целесообразности их применения.

Доступными для обывденного пользователя являются и постановщики активной заградительной помехи. Но, как правило, рекомендуется отказываться от практики постановки помех, ибо ряд современных АТС автоматически определяет стороннее переменное напряжение и отключает абонента от станции.

Наиболее эффективной мерой защиты информации является использование криптографических методов, делающих эту информацию недоступной как при прямом прослушивании телефонного тракта, так и при последующей обработке без знания соответствующих методик и алгоритмов дешифровки.

Список использованных источников:

1. Меньшаков Ю.К. Основы защиты от технических разведок. М.: ИПЦ «Маска», 2017г.
2. Бузов Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации М.: 2010г.
3. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации М.: Машиностроение, 2009г.