МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ ЧАСТНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ФИНАНСОВО-ПРОМЫШЛЕННЫЙ УНИВЕРСИТЕТ «УНИВЕРСИТЕТ»

Факультет ИСИТ

Кафедра «Информационные системы и технологии»

ЭССЕ

по Информационной безопасности и защите информации

на тему: Криптографическая защита телефонных сообщений

Выполнил:

Студент ВБИо-202 Ефремов Н. Д.

Проверил:

Грачев А. И.

Москва 2018

Введение

В современных условиях информация играет решающую роль как в процессе экономического развития, так и в ходе конкурентной борьбы на национальном и международном рынках. Противоборство развернулось за превосходство в тех областях, которые определяют направления научно-технического прогресса. В мире реального бизнеса конкуренция ставит участников рынка в такие жесткие рамки, что многим из них приходится поступать в соответствие с принципами “победителей не судят”, “цель оправдывает средства”.

В этих условиях становится реальностью промышленный шпионаж как сфера тайной деятельности по добыванию, сбору, анализу, хранению и использованию конфиденциальной информации. Это обусловлено тем, что получение сколько-нибудь достоверной информации об объектах заинтересованности законным путем становится невозможным из-за создания и поддержания определенной системы защиты ценной информации от несанкционированного, то есть противоправного, доступа со стороны злоумышленников.

Анализ различных способов получения информации о конкурентах позволил установить, что подслушивание телефонных переговоров в ряде случаев может являться одним из эффективных способов несанкционированного доступа к конфиденциальной информации. Это объясняется тем, что в настоящее время обмен информацией по телефону является очень распространенным и практически во всех случаях, когда абонентам не требуется письменного документа и имеется возможность воспользоваться телефонной связью, они ею пользуются. Мало того, даже в тех случаях, когда требуется письменный документ, абоненты довольно часто ведут по телефону предварительные переговоры, оправдывая это срочностью согласования определенных позиций.

Самым эффективным способом защиты телефонных сообщений от несанкционированного доступа является их криптографическое преобразование.

Общие принципы криптографического преобразования телефонных сообщений

Рассмотрим общие принципы криптографического преобразования телефонных сообщений (см. рис.1).

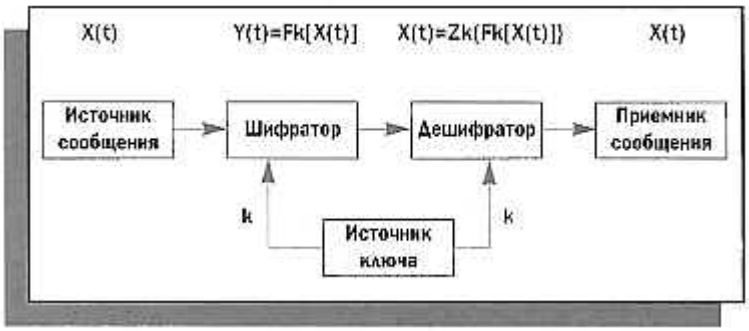

Рис 1. Обобщенная схема криптографической системы

Будем называть исходное телефонное сообщение, которое передается по радио- или проводному каналу, открытым сообщением и обозначать X(t).Это сообщение

поступает в устройство криптографического преобразования (шифрования), где формируется зашифрованное сообщение Y(t) с помощью следующей зависимости:

Y(t) = **F**k[X(t)],

где **F**k[.] - криптографическое преобразование;

k - ключ криптографического преобразования,

Здесь под ключом криптографического преобразования будем понимать некоторый параметр k, с помощью которого осуществляется выбор конкретного криптографического преобразования **F**k[.]. Очевидно, что чем больше мощность используемого множества ключей криптографического преобразования **K**, тем большему числу криптографических преобразований может быть подвергнуто телефонное сообщение X(t), а, следовательно, тем больше неопределенность у злоумышленника при определении используемого в данный момент криптографического преобразования **F**k[.].

Вообще говоря, при шифровании сообщения X(t) должны использоваться такие криптографические преобразования, при которых степень его защиты определялась бы только мощностью множества ключей криптографического преобразования **K.**

Зашифрованное сообщение Y(t) передается по радио- или проводному каналу связи. На приемной стороне это сообщение расшифровывается с целью восстановления открытого сообщения с помощью следующей зависимости

X(t) = **Z**k[Y(t)] = **Z**k{**F**k[X(t)]},

где - **Z**k[.] **-** обратное по отношению к **F**k[.] преобразование.

Таким образом, наличие у абонентов одинаковых ключей k и криптографических преобразований **F**k[.], **Z**k[.] позволяет без особых сложностей осуществлять зашифрование и расшифрование телефонных сообщений.

Очевидно, что для рассмотрения способов криптографического преобразования телефонных сообщений необходимо иметь представление о тех процессах, которые лежат в основе формирования этих сообщений.

Телефонное сообщение передается с помощью электрических сигналов, которые формируются из акустических сигналов путем преобразования микрофоном

телефонного аппарата этих акустических сигналов в электрические, обработки электрических сигналов и усиления до необходимого уровня. На приемной стороне в телефонном аппарате электрические сигналы подвергаются обработке и преобразованию в акустические с помощью телефона.

Любое сообщение X(t) характеризуется длительностью и амплитудно-частотным спектром S(f), т.е. сообщение X(t) может быть представлено эквивалентно как во временной, так и в частотной областях.

Заметим, что человеческое ухо может воспринимать акустический сигнал в диапазоне от 15 Гц до 20 кГц, хотя могут иметь место некоторые индивидуальные расхождения. Однако для того, чтобы сохранить узнаваемость голоса абонента по тембру, чистоту и хорошую разборчивость звуков совершенно необязательно передавать акустический сигнал в этом частотном диапазоне. Как показала практика, для этого достаточно использовать частотный диапазон от 300 Гц до 3400 Гц. Именно такую частотную полосу пропускания имеют стандартные телефонные каналы во всем мире.

Исходя из временного и частотного представлений открытого телефонного сообщения X(t) на практике могут использоваться криптографические преобразования, применяемые к самому сообщению X(t) или к его амплитудно-частотному спектру S(f).

Все криптографические преобразования, с точки зрения стойкости, представляется возможным разделить на две группы.

Первую группу составляют вычислительно стойкие и доказуемо стойкие криптографические преобразования, а вторую - безусловно стойкие криптографические преобразования.

К вычислительно стойким и доказуемо стойким относятся криптографические преобразования, стойкость которых определяется вычислительной сложностью решения некоторой сложной задачи. Основное различие между этими криптографическими преобразованиями заключается в том, что в первом случае имеются основания верить, что стойкость эквивалентна сложности решения трудной задачи, тогда как во втором случае известно, что стойкость, по крайней мере, большая. При этом во втором случае должно быть предоставлено доказательство, что раскрытие передаваемого зашифрованного сообщения Y(t) эквивалентно решению сложной задачи.

Примером вычислительно стойких криптографических преобразований являются сложные криптографические преобразования, составленные из большого числа элементарных операций и простых криптографических преобразований таким образом, что злоумышленнику для дешифрования перехваченного сообщения Y(t) не остается ничего другого, как применить метод тотального опробования возможных ключей криптографического преобразования, или, как еще называют, метод грубой силы. С помощью таких криптографических преобразований представляется возможным обеспечить гарантированную защиту передаваемого сообщения X(t) от несанкционированного доступа.

К вычислительно стойким криптографическим преобразованиям представляется возможным отнести и такие криптографические преобразования, при использовании которых злоумышленнику для несанкционированного доступа к сообщению X(t) требуется использовать лишь определенные алгоритмы обработки сообщения Y(t). Эти криптографические преобразования способны обеспечить лишь временную стойкость.

К безусловно стойким относятся криптографические преобразования, стойкость которых не зависит ни от вычислительной мощности, ни от времени, которыми может обладать злоумышленник. То есть такие криптографические преобразования, которые обладают свойством не предоставлять злоумышленнику при перехвате сообщения Y(t) дополнительной информации относительно переданного телефонного сообщения X(t).

Заметим, что безусловно стойкие криптографические преобразования реализовать очень сложно и поэтому в реальных системах телефонной связи они не используются.

Криптографическое преобразование аналоговых телефонных сообщений

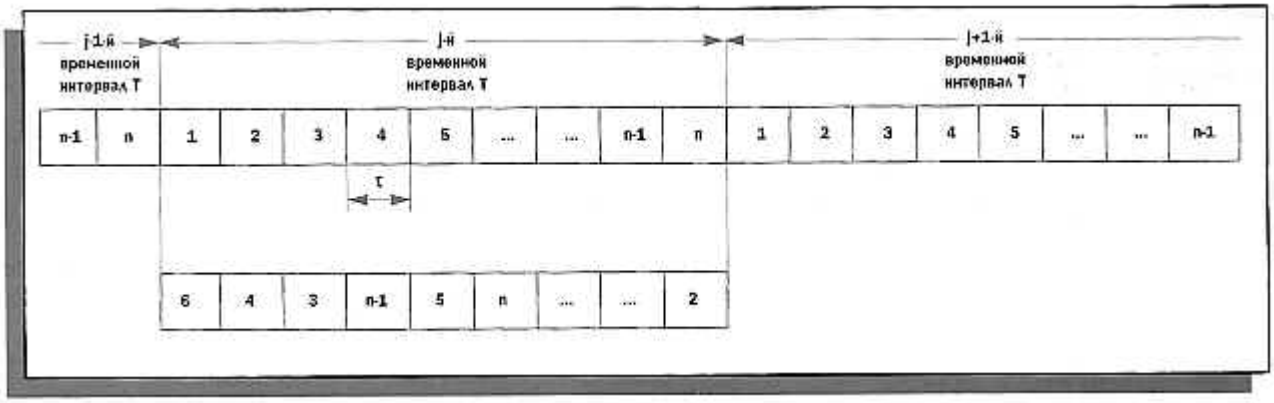

Рис. 2. Временные перестановки частей сообщения X(t)

Этот способ заключается в следующем. Длительность сообщения X(t) (см. рис.2) делится на определенные, равные по длительности временные интервалы T. Каждый такой временной интервал дополнительно делится на более мелкие временные интервалы длительностью t . При этом для величины n=T/t , как правило, выполняется условие n = m ...10m , где m - некоторое целое число, m <10. Части сообщения X(t) на интервалах времени tзаписываются в запоминающее устройство, “перемешиваются” между собой в соответствие с правилом, определяемым ключом криптографического преобразования k, и в виде сигнала Y(t) выдаются в канал связи. На приемной стороне канала связи, где правило перемешивания известно, т.к. имеется точно такой же ключ криптографического преобразования k, осуществляется “сборка” из сообщения Y(t) открытого сообщения X(t).

К преимуществам этого способа криптографического преобразования относится его сравнительная простота и возможность передачи зашифрованного телефонного сообщения по стандартным телефонным каналам. Однако этот способ позволяет обеспечить лишь временную стойкость. Это обусловлено следующим. Поскольку открытое телефонное сообщение X(t) является непрерывным, то у злоумышленника после записи сообщения Y(t) и выделения интервалов длительностью t (последнее достаточно легко сделать, т. к. в канале связи присутствует синхронизирующий сигнал) появляется принципиальная возможность дешифрования сообщения Y(t) даже без знания используемого ключа k. С этой целью необходимо осуществить выбор интервалов таким образом, чтобы обеспечивалась непрерывность получаемого сообщения на стыках этих интервалов. Очевидно, что при тщательной и кропотливой работе с использованием специальной техники можно достаточно быстро обеспечить такую непрерывность, выделив тем самым открытое сообщение X(t).

Поэтому такой способ криптографического преобразования открытых телефонных сообщений целесообразно применять только в тех случаях, когда информация не представляет особой ценности или когда ее ценность теряется через относительно небольшой промежуток времени.

Криптографическое преобразование цифровых телефонных сообщений

На практике для преобразования телефонного сообщения X(t) в цифровую форму на передающей стороне и восстановления этого сообщения на приемной стороне

используются речевые кодеки, которые реализуют один из двух способов кодирования телефонных сообщений: формы и параметров.

Основу цифровой телефонии в настоящее время составляет кодирование формы сообщений, кодирование параметров сообщений или, как называют, вокодерная связь используется значительно реже. Это обусловлено тем, что кодирование формы сигнала позволяет сохранить индивидуальные особенности человеческого голоса, удовлетворить требования не только к разборчивости, но и к натуральности речи.

При кодировании формы сигнала широко используются импульсно-кодовая модуляция (ИКМ), дифференциальная ИКМ и дельта-модуляция.

Кратко рассмотрим принципы осуществления ИКМ, дифференциальной ИКМ и дельта-модуляции.

ИКМ основана на дискретизации, квантовании отсчетов и кодировании номера уровня квантования (см. рис.3).

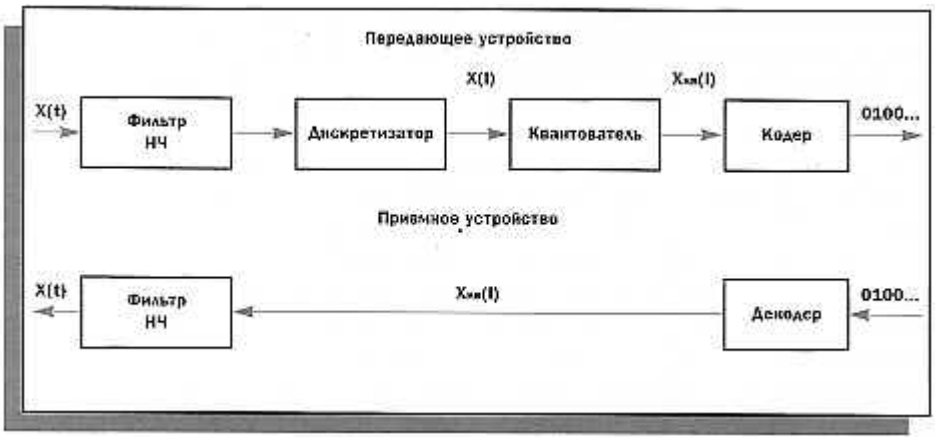

Рис. 3. Обобщенная схема системы с ИКМ

Телефонное сообщение X(t) длительностью T , имеющее ограниченный частотой fm спектр, после фильтрации преобразуется в последовательность узких импульсов X(l) = X(lD t), l =1,N, где N = T/D t, D t = 1/2fm, модулированных по амплитуде. Полученные мгновенные значения X(l),l=1,N, квантуются по величине с использованием равномерной, неравномерной или адаптивно-изменяемой шкалы квантования. Квантованные значения отсчетов Xкв(l), l=1,N, с помощью кодера преобразуются в кодовые слова, характеризуемые числом двоичных символов, которые выдаются в канал связи.

На приемной стороне кодовые слова с помощью декодера преобразуются в значения отсчетов Xкв(l), l=1,N, из которых с помощью фильтра нижних частот осуществляется восстановление сообщения X(t).

Дифференциальная ИКМ и дельта-модуляция отличаются от ИКМ тем, что в них использовано нелинейное отслеживание передаваемого телефонного сообщения.

При этом дифференциальная ИКМ отличается от простой ИКМ тем, что квантованию подвергаются не сами отсчеты телефонного сообщения X(l), l=1,N, а разность между соответствующим отсчетом X(l) и результатом предсказания Xпр(l), формируемым на выходе предсказателя. При этом в канал связи выдаются кодовые слова, содержащие коды этой разности и ее знака (полярности). И, наконец, дельта-модуляция отличается от простой ИКМ тем, что в канал связи выдаются только коды знака (полярности) в виде последовательности импульсов, временное положение которых позволяет восстановить на приемной стороне переданное телефонное сообщение X(t), например, с помощью интегратора.

Необходимо отметить, что дифференциальная ИКМ является наиболее предпочтительной при формировании цифровых сообщений. Это обусловлено, в основном, тем, что использование дифференциальной ИКМ позволяет сократить длину кодовых слов, т.к. передаче подлежит только информация о знаке и величине приращения. Кроме того, использование дифференциальной ИКМ позволяет исключить перегрузку по крутизне, с которой приходится сталкиваться при линейной дельта-модуляции.

Список литературы

- Криптографическая защита информации. Учебное пособие - Н.А. Гатченко, А.С. Исаев, А.Д. Яковлев.