Защита информации в каналах связи

Ковязин Евгений Витальевич,
преподаватель кафедры инженерно-технических средств охраны Пермского военного института внутренних войск МВД России, подполковник

Защита информации направлена на предотвращение возможности несанкционированного доступа к закрытой информации, передаваемой по каналам связи.

В соответствии с Федеральным Законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» любая информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1. информацию, свободно распространяемую (общедоступная информация);
2. информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях (коммерческая тайна);
3. информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению (информация преимущественно о деятельности государственных учреждений);
4. информацию, распространение которой в Российской Федерации ограничивается или запрещается (государственная тайна).

Различают две основные разновидности предотвращения утечки речевой информации из каналов связи:

1. средства физической защиты речевых сообщений, включающие в себя постановщиков заградительных помех, блокираторы, фильтры и средства поиска каналов утечки информации;
2. средства смысловой защиты речевой информации в каналах связи.

Средства предотвращения утечки информации из первой группы обладают рядом слабых мест и ограничений на их использование в той или иной практической ситуации, зависящих от типа линии связи, ее оконечного оборудования, технической квалификации личного состава и других факторов.

Как противодействие несанкционированному доступу к информации ограниченного пользования выступает необходимость обеспечения такого уровня ее защиты, чтобы время защиты превышало время, в течение которого она актуальна. Это время определяется областью применения данной информации и может составлять от нескольких часов или суток до многих месяцев или лет.

Сегодня средства смысловой защиты речевой информации в каналах связи можно разделить на три основные группы:

1. маскираторы, в которых для достижения неразборчивости используются нересурсоемкие операции преобразования сигнала в частотной и/или временной областях, при этом ключ преобразования в ходе сеанса связи не изменяется;
2. скремблеры, в которых используются более ресурсоемкие операции преобразования сигнала в частотной и временной областях, при этом осуществляется постоянное, динамическое изменение ключа преобразования в ходе сеанса связи;
3. шифраторы, в которых осуществляется преобразование волны и/или параметров сигнала в цифровую форму с последующим закрытием при помощи криптографических алгоритмов.

Техническое маскирование речи — это технологии маскирования речи, относящиеся к методам и средствам смысловой защиты речевой информации и имеющие цель обеспечения неразборчивости защищаемого речевого сообщения. Их реализация на практике может быть выражена в микшировании речи шумами и помехами или в модификации передаваемого сообщения по вычисляемым из его описаний параметрам по заранее известному закону преобразования (закрытия-восстановления).

Распространенным видом технического маскирования речи является микширование исходного сигнала с помехой с целью передачи в канал связи уже нового неразборчивого на слух звукового сигнала, как правило, лежащего в той же полосе частот, что и исходный. Зная характер изменения и вид помехи, на приемной стороне защищенного канала связи осуществляется нейтрализация ее влияния с дополнительной очисткой и усилением восстановленного сигнала.

Смысловая защита речевых сообщений посредством криптографических методов до сих пор рассматривается специалистами как единственная возможность гарантированной защиты различных каналов речевой связи независимо от условий ведения перегово-

ров, технических характеристик связной аппаратуры и других факторов.

Криптографическая защита представляет собой совокупность методов и средств, предназначенных для шифрования текстов, то есть для преобразования формы исходных (открытых) текстов сообщений таким образом, что их смысл становится непонятным для любого лица, не владеющего секретом обратного преобразования. Прямой процесс преобразования открытого текста с целью сокрытия его смысла называется шифрованием, а его результат — шифртекстом. Обратный процесс преобразования шифртекста в открытый текст с целью восстановления общепонятности сообщений называется расшифрованием.

В большинстве криптографических систем секретность способа шифрования данных базируется на двух элементах:

- алгоритме шифрования данных, представляющем собой набор математических правил, определяющих последовательность выполнения элементарных действий над данными, в совокупности обеспечивающих их шифрование или расшифрование;
- криптографическом ключе, однозначно определяющем конкретный вариант преобразования открытого текста в шифртекст и наоборот.

Из многообразия всех возможных вариантов, обусловленных алгоритмом шифрования, ключ обычно представляет собой число или последовательность символов и является параметром, позволяющим настроить алгоритм шифрования данных на конкретную работу. Используемые на практике алгоритмы шифрования обеспечивают столь большое количество возможных ключей, что дешифрование шифртекстов путем их полного перебора оказывается практически невозможным.

По характеру использования ключа известные алгоритмы шифрования можно разделить на два типа: симметричные (с одним ключом, по-другому с секретным ключом) и несимметричные (с двумя ключами или с открытым ключом). Несимметричные алгоритмы шифрования и дешифрования порой называют асимметричными.

В первом случае в шифраторе отправителя и дешифраторе получателя используется один и тот же ключ (Ключ 1). Шифратор образует шифрограмму, которая является функцией открытого текста. Конкретный вид функции преобразования (шифрования) определяется секретным ключом. Дешифратор получателя сообщения выполняет обратное преобразование по отношению к преобразованию, сделанному в шифраторе. Секретный ключ хранится в тайне и передается отправителем сообщения получателю по каналу, исключающему перехват ключа криптоаналитиком противника.

Во втором случае (при использовании асимметричного алгоритма) получатель вначале по открытому каналу передает отправителю открытый ключ (Ключ 1), с помощью которого отправитель шифрует информацию. При получении информации получатель дешифрирует ее с помощью второго секретного ключа (Ключ 2). Перехват открытого ключа (Ключ 1) криптоаналитиком противника не позволяет дешифровать закрытое сообщение, так как оно рассекречивается лишь вторым секретным ключом (Ключ 2). При этом секретный Ключ 2 практически невозможно вычислить с помощью открытого (Ключа 1).

Современные криптографические системы обеспечивают высокую стойкость шифрования, даже если алгоритм шифрования данных не является секретом. В этом случае стойкость шифртекстов полностью обеспечивается за счет поддержания режима секретности криптографического ключа, использованного в данном акте шифрования.

Основные правила криптозащиты:

Сохранение в тайне ключей

Исключение дублирования

Достаточно частая смена ключей

Под дублированием здесь понимается повторное шифрование одного и того же отрывка текста с использованием тех же ключей (например, если при первом шифровании произошел сбой). Нарушение этого правила резко снижает надежность шифрования, так как исходный текст может быть восстановлен с помощью статистического анализа двух вариантов зашифрованного текста.

Важнейшим правилом криптозащиты является достаточно частая смена ключей. Причем частота может определяться исходя из длительности использования ключа или объема зашифрованного текста. При этом смена ключей по временному графику является защитной мерой против возможного их хищения, смена после шифрования определенного объема текста — от раскрытия шифра статистическими методами.

Нельзя предоставлять злоумышленнику возможности направлять в систему ряд специально подобранных сообщений и получать их в зашифрованном виде. Такого взлома не может выдержать ни одна криптосистема!

Наиболее эффективным способом повышения степени защиты информации является комбинирование методов противодействия несанкционированному доступу к информации, предаваемой по каналам связи, представляющее собой использование нескольких различных способов шифрования.