ПРОГРАММНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОЙ СВЯЗИ

Хорошавин В.Д.

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

Балденко А.А.

Аннотация. В работе представлен обзор одного из современных алгоритмов шифрования, на основе которого возможно строить сети связи с повышенным уровнем безопасности без использования специализированной аппаратуры.

Войска связи в рамках Вооруженных Сил являются неотъемлемым звеном, обеспечивающим функциональное взаимодействие всех существующих родов войск. Исторический опыт ведения боевых действий показывает, что выполнение задач по предназначению невозможно в отсутствие качественной связи не только между командирами и подчинёнными, но и между взаимодействующими подразделениями в том числе. Совершенствование системы связи Вооруженных Сил ведется одновременно по нескольким приоритетным направлениям. Это перевод стационарной системы связи на цифровые способы передачи и обработки информации, модернизация имеющихся на вооружении подвижных комплексов связи для повышения их качественных показателей, разработка и внедрение современных средств и комплексов связи в различных звеньях управления, создание унифицированной автоматизированной системы управления связью на всех уровнях военного управления, обеспечение информационной безопасности системы связи [1].

Поскольку цифровизация является одним из приоритетных направлений в списке, приведённом выше, предлагается внедрить в процесс организации сетей связи открытый алгоритм шифрования RSA, с помощью которого представляется возможным без использования сложных и специализированных средств обеспечение безопасного зашифрованного обмена сообщениями. RSA является достаточно удобным и безопасным алгоритмом для применения в военных системах коммуникации. Это связано с тем, что он является асимметричным, т.е. для шифрования и расшифрования используются разные ключи. При его использовании создаётся пара ключей (закрытый и открытый). Закрытый ключ хранится у одного корреспондента и используется для расшифровки сообщений, а открытый распространяется свободно и используется для шифрования сообщений. Он является достаточно устойчивым к прямому взлому, т.к. требует подбора больших псевдослучайных чисел, что часто невыполнимо в разумные сроки по времени. К известным уязвимостям рассматриваемого алгоритма относятся атаки типа “Человек посередине”, когда у злоумышленника есть возможность подделывать входящие сообщения посредством выдачи себя за нашего корреспондента. Частным случаем такой ситуации может быть физический доступ к передающему устройству корреспондента. Также возможно возникновение проблем, связанное с неаккуратным выбором исходных параметров для генерации ключей. Хотя последний случай может быть несущественен в определённых ситуациях, как, например, в каналах с низкой продолжительностью существования или при скорой потере актуальности сообщения (т.е. при его расшифровании сообщение не будет иметь никакой ценности). Более подробно с деталями и доказательствами безопасности алгоритма можно ознакомится в работах [2, 3].

Далее рассмотрим на примере то, как возможно использовать описанный алгоритм для создания сети связи. Для простоты моделирования рассмотрим проводную сеть с иерархической топологией. Выбранный пример не означает, что решение не может быть распространено и на сети с другими средами распространения сигнала или топологиями. В нашем случае нужно будет обеспечить настройку и функционирование алгоритма на каждом из участков в сети. Т.е. для каждой пары узлов связи, непосредственно общающихся между собой, необходимо сгенерировать пару ключей. Причем очевидно, что для передачи сообщений с нижестоящих пунктов управления на вышестоящий достаточно будет сгенерировать только одну пару ключей. После этого необходимо со своими соседями обменяться открытыми ключами, что позволит начать использовать передачу зашифрованных сообщений. При задействовании схожей системы в рамках радиосети может получиться ухудшиться безопасность в случаях с широковещанием, т.к. в таком случае необходимо будет распространить закрытый ключ нескольким корреспондентам. При работе в радиосети возможно использование данного алгоритма. Для этого потребуется организовать отдельные направления или подсети, в которых и будут общаться конкретные корреспонденты.

Список использованных источников:

1. Войска связи: современное состояние и перспективы развития [Электронный ресурс]. — Режим доступа: https://www.mil.by/special/ru/news/press_center/press_releases/8439. — Дата доступа: 30.03.2023.

2. Asjad Sirajuddin. The RSA Algorithm. — University of South-Eastern Norway, Campus Kongsberg, 2019. — 23 p.

3. Michael J. Wiener. Cryptanalysis of Short RSA Secret Exponents. — Ottawa, Canada, 1989. — 14 p.