СОЛОВЬЕВ В.В.

УЛУЧШЕНИЕ ЗАЩИЩЕННОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ ПРИМЕНЕНИЯ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Иркутский государственный университет путей сообщения, Россия

В статье определяются необходимые для обеспечения информационной безопасности механизмы защиты информации, передаваемой по каналам связи, водящим в состав распределенной информационной системы. Рассматривается возможность улучшения защищенности распределенной информационной системы с помощью средств криптографической защиты информации, реализующих данные механизмы защиты. Выявляются конкретные продукты, реализующие криптографические механизмы защиты информации, в качестве решения по информационной безопасности в каналах связи.

Ключевые слова: информационная безопасность, распределенная информационная система, средство криптографической защиты информации, алгоритм шифрования.

В настоящий момент вслед за развитием автоматизированной обработки информации, сетевых технологий, обмена информацией через сети передачи данных общего пользования все более широкое развитие получают различные способы защиты передаваемой информации. Особую и важную роль при передаче какого-либо сообщения, составляющего информацию ограниченного доступа, по каналам связи играет шифрование данного сообщения. Шифрование, в свою очередь, тесно связано с такой наукой, как криптография.

Криптография — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства [1].

К средствам, обеспечивающим шифрование, в частности, относятся средства криптографической защиты информации (СКЗИ).

Под СКЗИ, в соответствии с Постановлением Правительства РФ от 16 апреля 2012 г. № 313, понимаются различные средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов, ключевые документы, аппаратные шифровальные (криптографические) средства, программно-аппаратные шифровальные (криптографические) средства [2].

В основу работы данных средств защиты положены различные алгоритмы шифрования, с помощью которых обеспечивается конфиденциальность, целостность либо проверка подлинности. Данные свойства могут

обеспечиваться как совместно, так и по отдельности, в зависимости от конкретно выбранного алгоритма щифрования.

Для современной криптографии характерно использование открытых алгоритмов шифрования, предполагающих использование вычислительных средств. Известно более десятка проверенных алгоритмов шифрования, которые при использовании ключа достаточной длины и корректной реализации алгоритма криптографически стойки. Распространенные алгоритмы:

– симметричные DES, AES, ГОСТ 28147-89, Camellia, Twofish, Blowfish, IDEA, RC4 и др.;

– асимметричные RSA и Elgamal (Эль-Гамаль);

– хэш-функции MD4, MD5, MD6, SHA-1, SHA-2, ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012.

Во многих странах приняты национальные стандарты шифрования. В 2001 году в США принят стандарт симметричного шифрования AES на основе алгоритма Rijndael с длиной ключа 128, 192 и 256 бит. Алгоритм AES пришёл на смену прежнему алгоритму DES, который теперь рекомендовано использовать только в коммерческих продуктах в режиме Triple DES. В Российской Федерации действует стандарт ГОСТ 28147-89, описывающий алгоритм блочного шифрования с длиной ключа 256 бит, а также алгоритм цифровой подписи ГОСТ Р 34.10-2001 [3] или ГОСТ Р 34.10-2012 [4].

Для обеспечения защиты распределенных информационных систем, в которых информация ограниченного доступа передается по каналам связи, как описывалось ранее, применяются средства криптографической защиты информации.

В настоящее время в Российской федерации наибольшее распространение среди СКЗИ получили средства защиты, в которых задействован алгоритм блочного шифрования, описываемый в стандарте ГОСТ 28147-89.

При обеспечении защищенности каналов связи, как правило, применяется комплекс СКЗИ, включающий в себя следующие основные средства защиты:

– основное средство администрирования сетью;

– координатор, выступающий в роли шлюза безопасности для защиты компьютерных сетей;

– клиентское приложение, предназначенное для обеспечения защищенного канала связи между рабочими станциями и шлюзом безопасности, через который передается информация в конечный пункт приема.

Одним из производителей подобных решений, обеспечивающих криптографическую защиту информации, является компания ИнфоТеКС (Информационные Технологии и Коммуникационные Системы), выступающая в качестве российского разработчика программно-аппаратных VPN-решений и СКЗИ.

Среди линеек продуктов, выпускаемых данной компанией, подходящих под критерии, рассмотренные выше, выделяются следующие:

– ViPNet Administrator;

– ViPNet Coordinator HW;

– ViPNet Client.

Шифрование данными СКЗИ осуществляется в соответствии с ГОСТ 28147-89 на ключах длиной 256 бит. Приведем основные из них.

1. Программный комплекс ViPNet Client предназначен для защиты рабочих мест корпоративных пользователей. ViPNet Client надежно защищает от внешних и внутренних сетевых атак за счет фильтрации трафика. Кроме того, ПК ViPNet Client обеспечивает защищенную работу с корпоративными данными через зашифрованный канал, в том числе для удаленных пользователей [5].

Данное ПО совместимо с различными операционными системами, в том числе: Windows, Linux, OS X, а также с виртуальными средами: Microsoft Hyper-V, VMWare Workstation, VMWare vSphere ESXi.

СКЗИ Vipnet Client поддерживает любые каналы связи, используемые в IP-сетях, в том числе: Ethernet, мобильные, Wi-Fi.

2. ViPNet Coordinator — семейство шлюзов безопасности. В зависимости от настроек ViPNet Coordinator может выполнять следующие функции в защищенной сети ViPNet:

– Маршрутизатор VPN-пакетов: маршрутизация зашифрованных IP-пакетов, передаваемых между сегментами защищенной сети;

– VPN-шлюз: туннелирование (шифрование и имитозащита) открытых IP-пакетов, передаваемых между локальными сегментами сети;

– Межсетевой экран: анализ, фильтрация и регистрация IP-трафика на границе сегмента сети;

– Транспортный сервер: маршрутизация передачи защищенных служебных данных в сети ViPNet, почтовых сообщений, передаваемых программой «ViPNet Деловая почта»;

– Сервер IP-адресов, сервер соединений: обеспечивает регистрацию и доступ в реальном времени к информации о состоянии объектов защищенной сети и о текущем значении их сетевых настроек (IP- адресов и т.п.).

Продукты ViPNet Coordinator адаптированы для использования в различных отраслях и сценариях применения. Семейство шлюзов безопасности ViPNet Coordinator подразделяется на решения, в зависимости от особенностей их исполнения, в том числе аппаратной платформы продукта, набора дополнительных сетевых сервисов, производительности, сетевых интерфейсов и других параметров [6].

3. ViPNet Administrator — программный комплекс, предназначенный для настройки и управления защищенной сетью, включающий в себя:

– ViPNet NCC (Центр управления сетью, ЦУС) — приложение для конфигурирования и управления виртуальной защищенной сетью ViPNet;

– ViPNet КСА (Удостоверяющий и ключевой центр, УКЦ) — приложение, которое выполняет функции центра формирования ключей шифрования и персональных ключей пользователей;

– Функции Удостоверяющего центра — издание сертификатов для аутентификации, электронной подписи, шифрования и других криптографических операций;

– Криптографические алгоритмы зависят от используемого криптопровайдера в данном случае это ViPNet CSP.

Основные функциональные возможности ViPNet Administrator:

– создание и изменение структуры защищённой сети, узлов и пользователей, связей между ними;

– конфигурирование параметров узлов и полномочий пользователей;

– генерация ключевой информации, выпуск ключевых контейнеров, компрометация ключей;

– централизованное (групповое или точечное) обновление ПО на узлах защищённой сети ViPNet;

– управление лицензией сети;

– управление журналами событий и журналами аудита [7].

Список использованных источников и литературы

1. Нечаев В. И. Элементы криптографии (Основы теории защиты информации) / В.И, Нечаев. — М.: Высшая школа, 1999. — 109 с.

2. Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя): Постановление Правительства РФ от 16.04.2012 № 313 // Собрание законодательства РФ. - 2012. - № 17. -Ст.1987.

3. Баричев С. Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров,Р.Е. Серов. — 3-е изд. — М.: Диалог-МИФИ, 2011. — 176 с.

4. Краковский Ю.М. Информационная безопасность и защита информации/ Ю.М, Краковский. – Иркутск: ИрГУПС, 2016. – 224 с.

5. Сайт компании ИнфоТеКС. ViPNet Client [Электронный ресурс] – URL: http://infotecs.ru/product/vipnet-client-.html.

6. Сайт компании ИнфоТеКС. ViPNet Coordinator HW [Электронный ресурс] – URL: http://infotecs.ru/product/setevye-komponenty/vipnet-coordinator-hw.

7. Сайт компании ИнфоТеКС. ViPNet Administrator [Электронный ресурс] – URL: http://infotecs.ru/product/vipnet-administrator-4-.html.