УДК 681.3.06

АЛГОРИТМЫ АУТЕНТИФИКАЦИИ В СЕТЯХ ISDN

к.т.н. А.А. Кузнецов, В.Е. Чевардин, И.В. Кучерявенко
(представил д.т.н., проф. Ю.В. Стасев)

Рассматриваются протоколы установления подлинности, уровни формирования имитостойких кодов согласно модели стека TCP/IP. Предлагаются алгоритмы аутентификации передаваемых по сетям ISDN данных, основанные на канальном разнесении передаваемой информации и служебных данных (имитовставок).

Постановка проблемы. Современный уровень развития информационно-управляющих систем выдвигает повышенные требования к качеству передаваемых данных, и, прежде всего, к их подлинности (аутентичности). При успешной реализации угроз аутентичности передаваемым данным, злоумышленник может нарушить управление, что приведет к невыполнению функциональных задач системы. Рост числа успешных атак на информационные ресурсы управляющих систем подтверждает актуальность проведения исследований, направленных на разработку и внедрение методов установления подлинности передаваемых данных.

Анализ последних исследований и публикаций. Одним из эффективных способов защиты от навязывания ложных сообщений является имитостойкое кодирование, которое заключается во введении в информацию избыточности (кода аутентификации, имитовставки), позволяющей с заданной вероятностью устанавливать подлинность передаваемого сообщения. Соглашения и инструкции применяемых на сегодняшний день процедур аутентификации изложены в стандартизированных сетевых протоколах [1 – 5]. На рис. 1 представлена схема соответствия модели взаимодействия открытых систем (модель ВОС, описанная в стандарте [6]) стеку TCP/IP. На рисунке отмечены протоколы установления подлинности передаваемых данных по сетям TCP/IP.

Представленные на рис. 1 протоколы безопасности данных позволяют обеспечить аутентичность передаваемой информации путем инкапсуляции аутентифицированных данных в пакет нижестоящего протокола. Вносимая при работе протокола избыточность, помимо положительного вклада (обеспечение аутентичности) несет и негативное воздействие на производительность сети (снижается информационная скорость передачи).

Постановка задачи. Проведенный анализ функционального назначения управляющего и информационного канала сети ISDN показал, что ресурсы управляющего канала позволяют передавать помимо пакетов с сигнальными сообщениями пакеты сетей X.25, Frame Relay. Эту потенциальную возможность целесообразно использовать для компенсации потерь относительной информационной скорости. В работе предлагаются алгоритмы подтверждения подлинности передаваемых данных в сетях ISDN, основанные на канальном разнесении передаваемой информации и служебных данных (имитовставок).

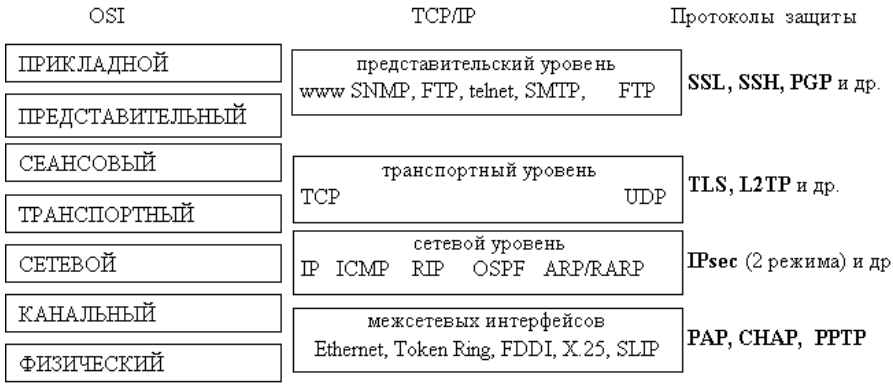

Рис. 1. Схема соответствия модели ВОС стеку TCP/IP с указанием уровней применения протоколов защиты данных

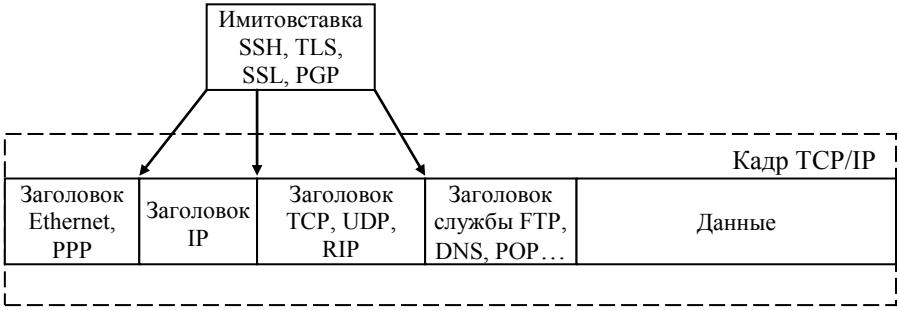

Рис. 2. Кадр стека TCP/IP

Повышение имитостойкости данных, передаваемых по сетям, обеспечивается формированием кодов аутентификации (имитовставок), и передачей их по сетям с коммутацией пакетов, таких, как TCP/IP, IPX, Novell NetWare. Как видно из рис. 1, формирование имитостойких кодов может осуществляться на различных уровнях стека TCP/IP. На данный момент такую защиту осуществляют такие протоколы, как (SSH, TLS,

SSL, PPTP, L2TP) для сетей TCP/IP (рис. 2). В зависимости от режимов работы и вида протокола имитовставка может вставляться на транспортном, сетевом или на представительском уровнях стека TCP/IP. В любом случае процедуру передачи пакета можно представить как передачу двух кадров различного размера и назначения. Рассмотрим особенности канального разнесения передаваемой информации и служебных данных (имитовставок) для различных вариантов формирования имитовставок.

Алгоритм аутентификации данных, основанный на формировании имитовставки для каждого пакета (дейтаграммы). Суть предлагаемого алгоритма состоит в канальном разнесении пакета данных и со-

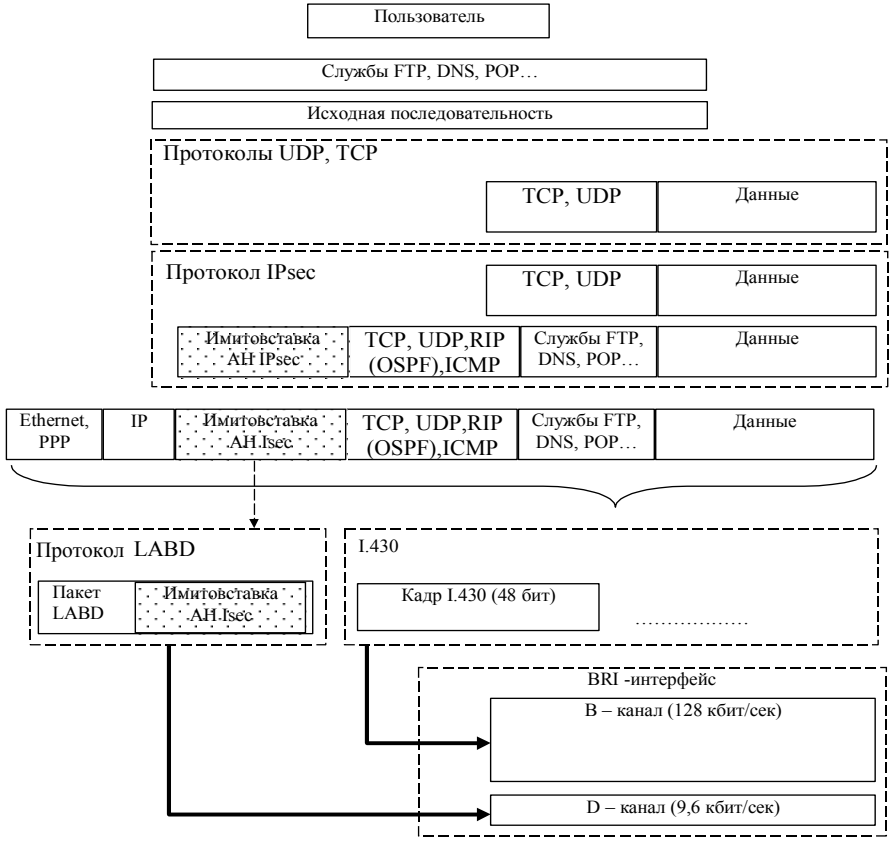

Рис. 3. Схема отделения имитовставки от пакета данных и передачи в D-канал

ответствующего ему имитостойкого кода. На рис. 3 представлен схематично алгоритм отделения имитовставки от пакета и передачи в D-канал (служебный управляющий канал сетей ISDN).

Приведенная на рис. 3 схема наглядно демонстрирует процесс отделения имитовставки для каждого IP (IPsec) пакета и передачи ее по управляющему каналу.

Алгоритм аутентификации данных, основанный на формировании имитовставки для каждого сообщения. Суть предлагаемого алгоритма состоит в канальном разнесении передаваемого сообщения и соответствующего ему имитостойкого кода.

Схематично алгоритм отделения имитовставки от сообщения и передачи в D-канал (служебный управляющий канал сетей ISDN) представлен на рис. 4.

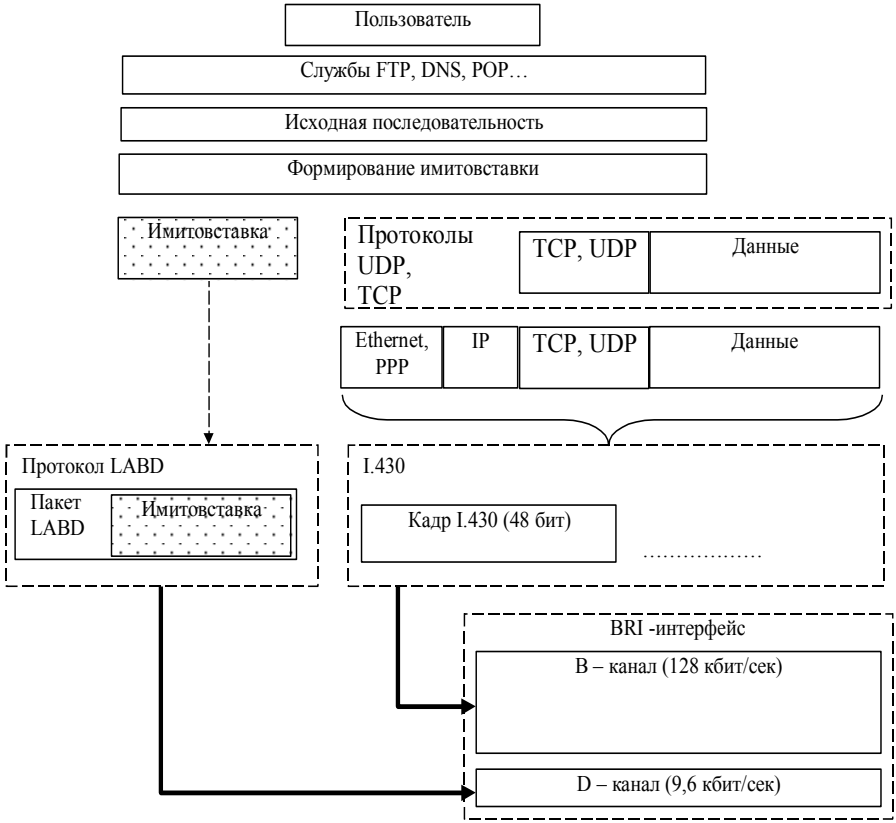

Рис. 4. Схема отделения имитовставки, сформированной для всего сообщения и передачи ее по управляющему каналу

Приведенная на рис. 4 схема наглядно демонстрирует процесс отделения имитовставки для каждого TCP (UDP) пакета и передачи ее по управляющему каналу.

Выводы. В результате проведенных исследований разработаны алгоритмы аутентификации передаваемых данных, отличительной особенностью которых является использование служебных каналов сетей ISDN для передачи имитовставок (кодов аутентификации). Это позволяет, в отличии от традиционных алгоритмов подтверждения подлинности, передавать данные с требуемой аутентичностью (вероятностью навязывания) без снижения информационной скорости. Недостаток предложенных алгоритмов заключается в дополнительной загрузке служебных каналов ISDN сетей.

Дальнейшие работы могут быть направлены на исследование системно-технических и временных затрат применения предложенных алгоритмов, сравнение их с известными протоколами.

ЛИТЕРАТУРА

1. *Кульгин М.В. Технологии корпоративных сетей. Энциклопедия. – С.-Пб.: Питер, 2000. – 704 с.*
2. *Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP-сетей.. – С.-Пб.: БХВ, 2000. – 512 с.*
3. *Уолрэнд Дж. Телекоммуникационные и компьютерные сети. – М.: Постмаркет, 2001. – 480 с.*
4. *Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – С.-Пб.: Питер, 1999. – 150 с.*
5. *Tanenbaum Andrew S. Computer Networks. – Prentice Hall, 1996. – 428 p.*
6. *OSI – Open Systems Interconnection. ISO 7498.*

Поступила 24.07.2003

***КУЗНЕЦОВ Александр Александрович**, канд. техн. наук, начальник научно-исследовательской лаборатории Харьковского военного университета. В 1996 году окончил Харьковский военный университет. Область научных интересов – теория аутентификации, алгебраическая теория кодов. E - mail : kuznetsov@ sky.net.ua*

***ЧЕВАРДИН Владислав Евгеньевич**, адъюнкт Полтавского института связи. В 2001 году окончил Харьковский военный университет. Область научных интересов – теория аутентификации, алгебраическая теория кодов.*

***КУЧЕРЯВЕНКО Игорь Вячеславович**, начальник группы вычислительной лаборатории Сумского научного центра РВ и А. В 1999 году окончил Харьковский военный университет. Область научных интересов – теория аутентификации, алгебраическая теория кодов.*