ПРОГРАММНЫЕ МЕТОДЫ - КАК ЭФФЕКТИВНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Баранова Жанна Михайловна,
г. Смоленск, Россия, Gosha_v_a@mail.ru

Зайцев Владислав Геннадиевич,
г. Смоленск, Россия, Nemezida6969@mail.ru

Аннотация. Надежно защитить сообщения и данные от подглядывания и перехвата может только полное их шифрование. Поэтому начальный этап развития компьютерной безопасности прочно связан с криптографией.
В настоящее время защита информации не ограничивается только программными методами. Проблема значительно шире. Основной недостаток защиты – люди, и поэтому надежность системы безопасности зависит в основном от отношения к ней служащих компании. Помимо этого, защита должна постоянно совершенствоваться вместе с развитием компьютерной сети. Не стоит забывать, что мешает работе не система безопасности, а ее отсутствие.

Ключевые слова: шифрование, криптопротоколы, конфиденциальность и целостность информации, система безопасности, возникновения нештатных ситуаций.

Сведения об авторах: Баранова Ж.М., к.т.н., доцент кафедры автоматизированных систем боевого управления Военной академии войсковой противовоздушной обороны Вооруженных Сил Российской Федерации имени Маршала Советского Союза А. М. Василевского;
Зайцев В.Г., начальник лаборатории кафедры автоматизированных систем боевого управления Военной академии войсковой противовоздушной обороны Вооруженных Сил Российской Федерации имени Маршала Советского Союза А. М. Василевского.

С самого начала своего развития системы информационной безопасности разрабатывались для военных ведомств. Разглашение такой информации могло привести к огромным жертвам, в том числе и человеческим. Поэтому конфиденциальности (то есть неразглашению информации) в первых системах безопасности уделялось особое внимание. Очевидно, что надежно защитить сообщения и данные от подглядывания и перехвата может только полное их шифрование. Поэтому начальный этап развития компьютерной безопасности прочно связан с криптографией.

К программным методам защиты в сети Internet могут быть отнесены защищенные криптопротоколы, которые позволяют надежно защищать соединения. В процессе развития Internet были созданы различные защищенные сетевые протоколы, использующие как симметричную криптографию с закрытым ключом, так и асимметричную криптографию с открытым ключом. К основным на сегодняшний день подходам и протоколам, обеспечивающим защиту соединений, относятся SKIP-технология и протокол защиты соединения SSL.

SKIP (Secure Key Internet Protocol) технологией называется стандарт защиты графика IP-пакетов, позволяющий на сетевом уровне обеспечить защиту соединения и передаваемых по нему данных.

Возможны два способа реализации SKIP-защиты трафика IP-пакетов:

шифрование блока данных IP-пакета;

инкапсуляция IP-пакета в SKIP-пакет.

Шифрование блока данных IP-пакета иллюстрируется рисунком 1.

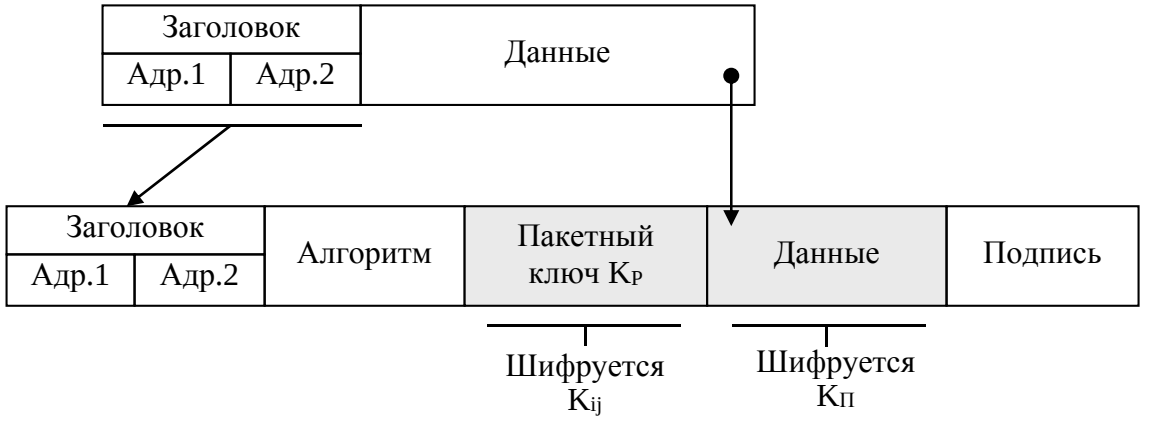

Рис. 1. Схема шифрования блока данных IP-пакетов

В этом случае шифруются методом симметричной криптографии, только данные IP-пакета, а его заголовок, содержащий помимо прочего адреса отправителя и получателя, остается открытым, и пакет маршрутизируется в соответствии с истинными адресами.

Закрытый ключ K_{ij}, разделяемый парой узлов сети I и J, вычисляется по схеме Диффи-Хеллмана.

Инкапсуляция IP-пакета в SKIP-пакет показана на рисунке 2. SKIP-пакет внешне похож на обычный IP-пакет. В поле данных SKIP-пакета полностью размещается в зашифрованном виде исходный IP-пакет. В этом случае в новом заголовке вместо истинных адресов могут быть помещены некоторые другие адреса. Такая структура SKIP-пакета позволяет беспрепятственно направлять его любому хост-компьютеру в сети Internet, при этом межсетевая адресация осуществляется по обычному IP-заголовку в SKIP-пакете. Конечный получатель SKIP-пакета по заранее определенному разработчиками алгоритму расшифровывает криптограмму и формирует обычный TCP- или UDP-пакет, который и передает соответствующему модулю (TCP или UDP) ядра операционной системы.

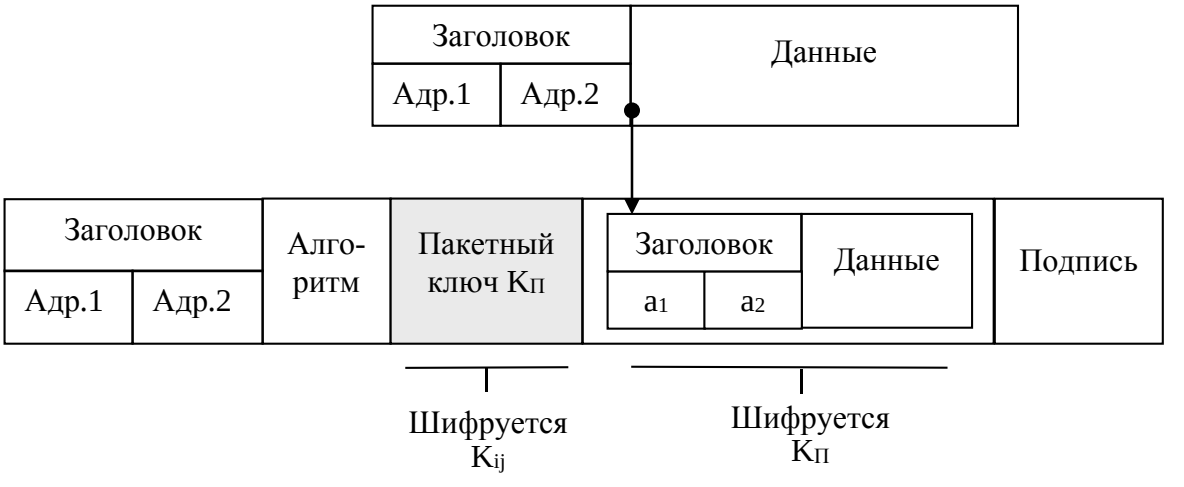

Рис. 2. Схема инкапсуляции IP-пакетов

Универсальный протокол защиты соединения SSL (Secure Socket Layer) функционирует на сеансовом уровне эталонной модели OSI. Протокол SSL, разработанный компанией Netscape, использует криптографию с открытым ключом. Этот протокол является действительно универсальным средством, позволяющим динамически защищать соединение при использовании любого прикладного протокола

(FTP, TELNET, SMTP, DNS и т.д.). Протокол SSL поддерживают такие ведущие компании, как IBM, Digital Equipment Corporation, Microsoft Corporation, Motorola, Novell Inc., Sun Microsystems, Mastercard International Inc. и др.

Следует отметить также функционально законченный отечественный криптографический комплекс «Шифратор IP потоков», разработанный московским отделением Пензенского научно-исследовательского электротехнического института. Криптографический комплекс «Шифратор IP потоков» представляет собой распределенную систему криптографических шифраторов, средств управления криптографическими шифраторами, средств хранения, распространения и передачи криптографической информации, а также средств оперативного мониторинга и регистрации происходящих событий.

Криптографический комплекс «Шифратор IP потоков» предназначен для выполнения следующих функций:

обеспечения конфиденциальности и целостности информации, передаваемой в сетях общего пользования (Internet), построенных на основе протоколов IP;

создания защищенных подсетей передачи конфиденциальной информации;

объединения локальных сетей в единую защищенную сеть;

закрытия доступа к ресурсам локальной сети или отдельным компьютерам из сети общего доступа;

организации единого центра управления защищенной под сетью.

Комплекс обеспечивает:

закрытие передаваемых данных на основе использования функций шифрования в соответствии с отечественным стандартом ГОСТ 28147-89;

контроль целостности передаваемой информации;

аутентификацию абонентов (узлов сети);

защиту доступа к локальной сети и сокрытие IP адресов подсети;

передачу контрольной информации в Центр управления ключевой системой защищенной IP сети;

поддержку протоколов маршрутизации PIP II, OSPF, BGP;

фильтрацию IP, ICMP и TCP-соединений на этапе маршрутизации и при приеме/передаче в канал связи;

поддержку инкапсуляции IPX в IP (в соответствии с RFC-1234);

поддержку инкапсуляции IP в X.25 и Frame Relay;

защиту от НСД ресурсов самого шифратора.

Криптографический комплекс «Шифратор IP потоков» имеет модульную структуру и состоит из распределенной сети шифраторов IP потоков и единого центра управления ключевой системой.

Шифратор IP протоколов (ШИП) состоит из:

криптографического модуля, непосредственно встроенного в ядро опе-рационной системы;

модуля поддержки клиентской части ключевой системы;

модуля записи протоколов работы криптографической системы;

модуля проверки целостности системы при загрузке.

ШИП содержит также плату с интерфейсом ISA, используемую для за-щиты от НСД при загрузке системы и для получения от сертифицированного физического датчика случайных чисел, необходимых для реализации процедуры шифрования.

Центр управления ключевой системой (ЦУКС) состоит из:

автоматизированного рабочего места управления ключевой системой, работающего в среде X Windows;

модуля серверной части ключевой системы;

сервисной программы просмотра протоколов работы криптографического комплекса «Шифратор IP потоков».

Управление ключами выполняется при помощи ЦУКС и заключается в следующем:

периодическая (плановая) смена парных ключей шифрования зареги-стрированных узлов защищенной сети;

формирование и рассылка по сети справочников соответствия, опреде-ляющих возможность абонентов работать друг с другом;

сбор и хранение в базе данных информации о всех критичных событиях в сети, возникающих как при аутентификации абонентов, так и при передаче между ними зашифрованной информации.

В случае возникновения нештатных ситуаций, создающих угрозу нарушения защиты информации, администратор ЦУКС предпринимает действия, направленные на восстановление целостности системы защиты информации.

Схема организации виртуальной корпоративной сети с применением криптографического комплекса «Шифратор IP потомков» показана на рисунке 3.

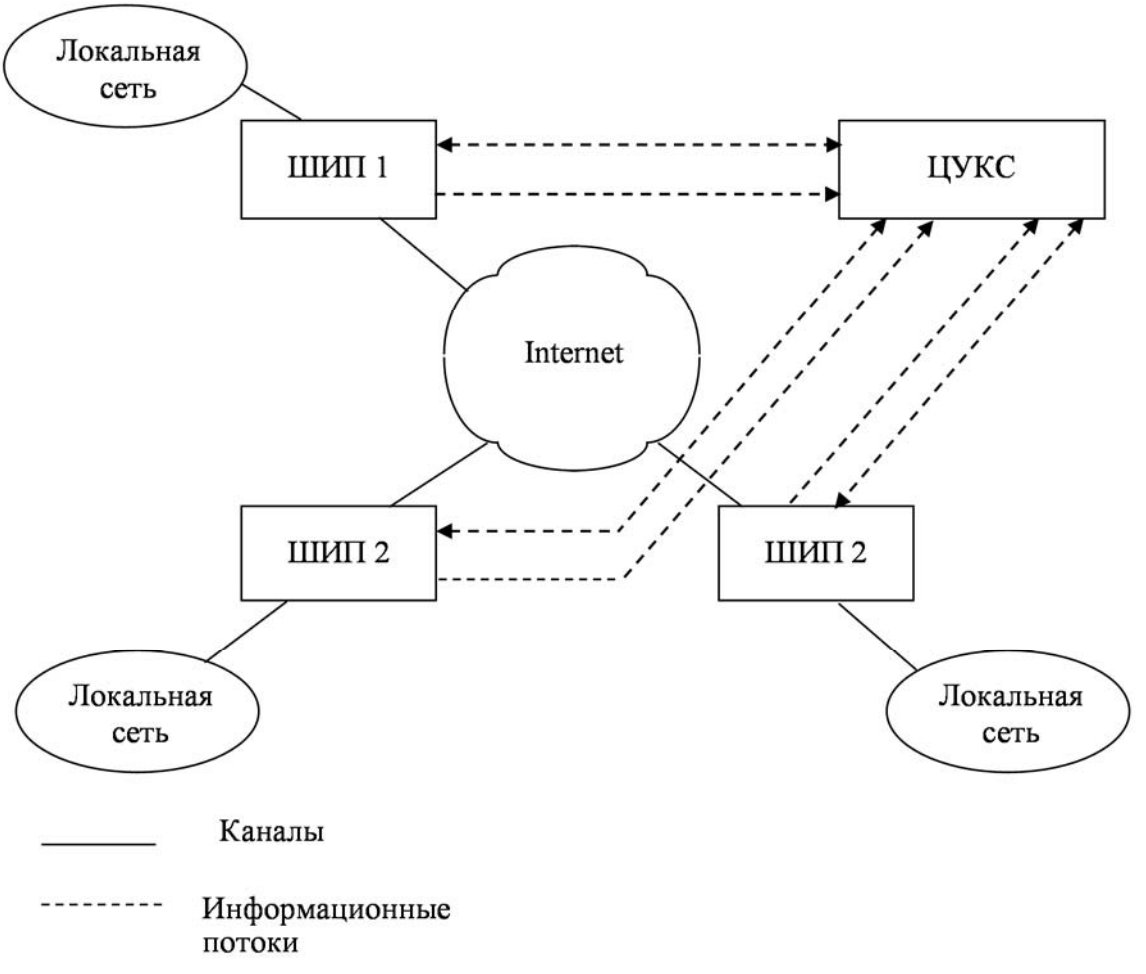

Рис. 3. Виртуальная корпоративная сеть с применением криптографического комплекса «Шифратор IP потоков»

При организации виртуальной корпоративной сети небольшого размера без жестких требований к времени оповещения абонентов о компрометации какого-либо абонента и без жестких требований к полноте собираемых протоколов об ошибках доступа возможно использование одного ЦУКС. При организации виртуальной корпоративной сети среднего размера или с жесткими требованиями к времени оповещения абонентов о компрометации какого-либо абонента и к полноте собираемых протоколов об ошибках доступа следует использовать несколько ЦУКС. При этом желательно, чтобы ЦУКС имели независимые друг от друга каналы подключения к глобальной сети.

В настоящее время защита информации не ограничивается только программными методами. Проблема значительно шире. Основной недостаток защиты – люди, и поэтому надежность системы безопасности зависит в основном от отношения к ней служащих компании. Помимо этого, защита должна

постоянно совершенствоваться вместе с развитием компьютерной сети. Не стоит забывать, что мешает работе не система безопасности, а ее отсутствие.

Из всего предшествующего следует, что действительно эффективное обеспечение защиты информации в автоматизированных системах возможно только на основе комплексного использования всех известных методов и подходов к решению данной проблемы.

Литература

1. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоиздат, 1994, – 400 с.

2. Мельников В.В. «Защита информации в компьютерных системах». – М.: «Финансы и статистика», 1997, – 368 с.

3. Алексенцев А.И. История и современные системы защиты информации в России: учеб.-метод. комплекс / А.И. Алексенцев, В.И. Еремеева, И.А.Комочкова. - М.:РГГУ, 2002, –102 с.

4. Бузов Г.А. Практическое руководство по выявлению специальных технических средств несанкционированного получения информации / Г.А. Бузов. - М.: Горячая линия-Телеком, 2010, – 237 с.

5. Варакута С.А. Связи с общественностью: учеб. пособие / С.А. Варакута, Ю.Н. Егоров. - М.: ИНФРА-М, 2003, – 246 с.

6. Гашков С.Б. Криптографические методы защиты информации: учеб. пособие для студентов вузов / С.Б. Гашков, Э.А. Применко, М.А. Черепнев. - М.: Академия, 2010, – 297 с.

PROGRAM METHODS – AS EFFECTIVE ENSURING INFORMATION SECURITY IN THE AUTOMATED SYSTEMS

Baranova Zhanna Mihajlovna,
Smolensk, Russian , Gosha_v_a@mail.ru

Zajcev Vladislav Gennadievich,
Smolensk, Russian, Nemezida6969@mail.ru

ABSTRACT

It is reliable to protect messages and data from peeping and interception only their full enciphering can. Therefore the initial stage of development of computer safety is strongly connected with cryptography.

Now information security isn't limited only to program methods. The problem is much wider. The main lack of protection – people and therefore reliability of a security system depends generally on the attitude of employees of the company towards her. In addition, protection has to be improved constantly together with development of a computer network. You shouldn't forget that work is disturbed by not a security system, but its absence.

Keywords: enciphering, cryptoprotocols, confidentiality and integrity of information, security system, emergence of emergency situations.

References

1. Gerasimenko V.A. Protection of information in automated data processing systems. – M.: Energoizdat, 1994, – p. 400.

2. Melnikov V.V. "the Protection of information in computer systems". – M.: "finances and statistics", 1997, – p. 368.

3. Alexencev A.I. History and modern systems of information protection in Russia: textbook.-method. complex / A. I. Alexencev, I. V. Eremeev, I. A. Komachkova. - Moscow: RGGU, 2002, – p. 102.

4. Buzov G.A. Practical guide on the identification of special technical means of unauthorized information / G. A. Buzov. - M.: hotline-Telecom, 2010, – p. 237.

5. Varakuta S. A. Public relations: textbook. the grant / S.A. Varakuta, Y.U. Egorov. - M.: INFRA-M, 2003, – p. 246.
6. Gashkov S.B. Cryptographic methods of information security: studies. a Handbook for University students / S.B. Gashkov, A.E. Primenko, M.A. Cherepnyov. - M.: Academy, 2010, – p. 297.

Information about authors:
Baranova Z.M., Candidate of Technical Sciences, the associate professor of the automated systems of fighting management of Military academy of army antiaircraft defense of Armed Forces of the Russian Federation of Marshall of the Soviet Union A. M. Vasilevsky;
Zajcev V.G., the chief of laboratory of chair of the automated systems of fighting management of Military academy of army antiaircraft defense of Armed Forces of the Russian Federation of Marshall of the Soviet Union A. M. Vasilevsky.