УДК 681. 322

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В КОРПОРАТИВНЫХ СИСТЕМАХ

САДАТ КХУДИР, ГАВРИШ Т.В.

Предлагаются средства защиты информации для распределенных корпоративных систем (КС) коммерческих предприятий, выполнены процедуры аутентификации пользователей рабочих станций, обеспечения конфиденциальности информаци и контроля ее целостности. Для реализации защиты использованы стандартные криптоалгоритмы простой замены.

Широкое распространение сетевых технологий в распределенных КС обуславливает актуальность задачи обеспечения их инфорационной безопасности. Последнее предполагает организацию достаточно эффективного противодействия любому несанкционированному вторжению в процесс функционирования КС, а также попыткам модификации, хищения или разрушения ее компонентов. Использование локальных и корпоративных сетей в коммерческих целях и, в частности, для передачи информации, содержащей сведения конфиденциального характера, обуславливает необходимость разработки средств защиты информации (СЗИ).

Разработку СЗИ, реализующих разумный компромисс между требуемым уровнем безопасности информации и стоимостью их создания и эксплуатации, следует начинать с анализа возможных угроз, способов их осуществления и рисков [1]. Типы угроз зависят от специфики системы и обрабатываемой в ней информации. В рассматриваемых КС конфиденциальная информация передается по незащищенным каналам связи от удаленных рабочих станций, а затем обрабатывается на сервере головной организации. В подобных ситуациях основным фактором риска является распределенность компонентов сети в пространстве, а наиболее уязвимым с точки зрения возможности несанкционированного доступа (НСД) выступает процесс прохождения информации по каналам связи. В таких случаях основные средства защиты компонентов сети (как правило, компьютеры) следует направлять на исключение НСД и разграничение доступа к ресурсам ПК со стороны сети. Этот подход не исключает возможности угрозы безопасности компьютеров со стороны консоли.

С учетом изложенного выше основными нарушениями информационной безопасности для рассматриваемых КС являются: получение НСД к конфиденциальным данным; незаконное копирование или искажение информации; перехват паролей пользователей КС; проникновение в КС предприятия под именем зарегистрированного пользователя. С помощью полученной неавторизированным лицом информации может быть подорвана конкурентоспособность предприятия и доверие его клиентов.

Для исключения возможных потерь предлагаются следующие способы защиты: идентификация и аутентификация пользователей КС; обеспечение конфиденциальности данных; контроль целостности данных. Эти способы реализуются криптографическими методами защиты по следующей схеме.

Каждый пользователь КС имеет индивидуальный идентификатор ID и пароль P. В начале любого сеанса связи каждого пользователя рабочей станции необходимо однозначно идентифицировать, а затем средства защиты информации должны подтвердить его подлинность и наделить его соответствующими полномочиями. После завершения процедуры идентификации пользователь получает статус законного. Подтверждение его подлинности (аутентификация) состоит в сравнении переданного пользователем пароля P’ с его исходным значением P. Если значения P и P’ совпадают, то операция аутентификации считается успешной и пользователь получает полномочия на передачу данных. Для исключения перехвата пароля в сети его следует передавать в зашифрованном виде с использованием симметричного криптоалгоритма, вычислительная блок-схема которого приведена ниже.

С целью повысить криптостойкость процедуры аутентификации предложено шифровать идентификационный номер пользователя рабочей станции, а в качестве ключа использовать результат побитового сложения по модулю 2 значений пароля пользователя и ключа криптоалгоритма K. Тогда аутентификационный шифротекст A(P) определяется по правилу:

$$A(P) = E_{P \oplus K}(ID),$$

где E – криптографическое преобразование.

Ключи для шифрования ID, равно как и сеансовые ключи, генерируются в головной организации и передаются при личном контакте.

Схема процедуры авторизации удаленного пользователя представлена на рис. 1.

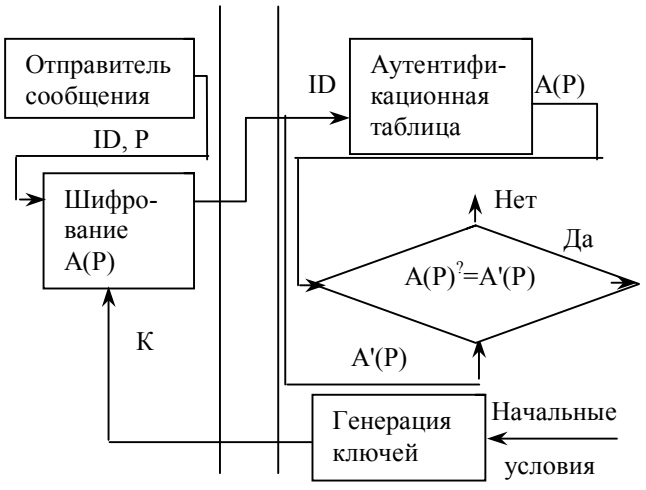

Рис. 1

Таким образом, реализованная процедура авторизации с вероятностью нераскрытия в канале $A(P)$ подтверждает подлинность источника данных и может служить гарантом подотчетности поступающей документации.

Основные функции разработанных СЗИ, состоящие в обеспечении конфиденциальности и целостности передаваемой информации, реализованы криптографическими методами информационной защиты. Они основаны на технологии "прозрачного" шифрования по алгоритму простой замены ГОСТ 28147−89 [2].

Контроль целостности данных осуществляется с помощью имитовставки, которая вырабатывается из блоков открытых данных либо перед шифрованием всего сообщения, либо параллельно с шифрованием по блокам. В связи с этим целесообразно рассмотреть математическую модель криптоалгоритма, имея в виду его применение как для шифрования, так и для имитозащиты передаваемых по каналу сообщений.

Алгоритм шифрования данных представляет собой 64-битовый блочный алгоритм с 256-битовым ключом, заданным в виде матрицы, состоящей из восьми 32-битовых векторов K_i:

$$K = K_7K_6K_5K_4K_3K_2K_1K_0.$$

Для записи K предусмотрено ключевое запоминающее устройство (КЗУ), состоящее из восьми 32-разрядных накопителей $X_0, X_1, X_2, ..., X_7$.

Исходные данные для шифрования разбиваются на 64-разрядные блоки $T_0^{(1)}, T_0^{(2)}, ..., T_0^{(m)}$. Процедура шифрования каждого блока T_0 включает 32 цикла $(j = 1,..,32)$. Последовательность битов T_0 разбивается на 2 части по 32 бита в каждой:

$$T_0 = (a_1(0), a_2(0), \ldots, a_{32}(0), b_1(0), b_2(0), \ , b_{32}(0)),$$

которая помещается в накопители N_1 и N_2. Первый цикл $(j = 1)$ описывается следующим уравнением:

$$\begin{cases} a(1) = f(a(0) \otimes K_0) \oplus b(0), \\ b(1) = a(0). \end{cases} \qquad (1)$$

Здесь f − функция шифрования, $a(1)$ и $b(1)$ − заполнение соответственно накопителей N_1 и N_2 после первого цикла шифрования. Аргументом f является сумма по модулю 2^{32} чисел $a(0)$ и K_0, а сама функция f состоит из двух операций над полученной 32-разрядной суммой $(a(0) \otimes K_0)$.

Первая операция сводится к замене каждого из восьми 4-разрядных векторов, на которые разбивается ранее вычисленная сумма, таким же по разрядности выходным вектором из таблиц−перестановок. Последние являются долговременными ключами криптоалгоритма. Вторая операция состоит в циклическом сдвиге на 11 разрядов влево 32-разрядного вектора, полученного с выхода блока замены.

Затем $(f(a(0) \otimes K_0))$ суммируются по модулю 2 с $b(0)$ и результат записывается в N_1 как $a(1)$, а содержимое N_1 переписывается в N_2, причем $b(1) = a(0)$. После завершения первого цикла аналогично выполняются остальные 31 цикл. Однако порядок использования подключей K_i в уравнении (1) может быть описан следующим образом:

$$\begin{cases} a(j) = f(a(j-1) \otimes K_{i-1(\mathrm{mod}\,8)}) \oplus b(j-1), \\ b(j) = a(j-1), \quad j = 1, ..., 24. \end{cases} \qquad (2)$$

$$\begin{cases} a(j) = f(a(j-1) \otimes K_{32-j}) \oplus b(j-1), \\ b(j) = a(j-1), \quad j = 25, ..., 31. \end{cases} \qquad (3)$$

$$\begin{cases} a(32) = a(31), \\ b(32) = f(a(31) \otimes K_0) \oplus b(31), \quad j = 32. \end{cases} \qquad (4)$$

Здесь $a(j)$ − битовая последовательность, заполняющая накопитель N_1 после j-го цикла шифрования; $b(j)$ − заполнение накопителя N_2 после j-го цикла шифрования. По окончании 32 циклов блок зашифрованного текста $T_ш$, соответствующий исходному T_0, поразрядно выводится из накопителей N_1 и N_2. В канал связи поступает последовательность $T_ш^{(1)}, T_ш^{(2)}, ..., T_ш^{(M)}$, где M − число 64-разрядных блоков, на которые разбивается исходное сообщение.

Для расшифрования принятой последовательности используется аналогичный криптоалгоритм с тем изменением, что заполнение накопителей $X_0, X_1, ..., X_7$ считывается из КЗУ в другом порядке. Уравнения расшифрования при этом имеют вид

$$\begin{cases} a(32-j) = f(a(32-j+1) \otimes Kj-1) \oplus b(32-j+1), \\ b(32-j) = a(32-j+1), \quad j = 1, ..., 8, \end{cases} \qquad (5)$$

$$\begin{cases} a(32-j) = f(a(32-j+1) \otimes K_{32-j(\mathrm{mod}\,8)}) \oplus b(32-j+1), \\ b(32-j) = a(32-j+1), \quad j = 9, ..., 31. \end{cases} \qquad (6)$$

$$\begin{cases} a(0) = a(1), \\ b(0) = f(a(1) \otimes K0) \oplus b(1), \quad j = 32. \end{cases} \qquad (7)$$

Для обнаружения возможных изменений в передаваемом по каналу шифротексте была использована имитозащита согласно рекомендациям ГОСТ 28147-98. Число двоичных разрядов имитовставки вычислялось из условия непревышения вероятности преднамеренного искажения данных, равной 10^{-4}, и составило $p = 12$.

Имитовставка формируется из блоков открытых данных $T_0^{(l)}, l = 1, 2, ..., m$ с помощью функции $\varphi(T_0^{(l)})$, суть которой состоит в реализации следующих операций. Первый блок $T_0^{(1)}$ подвергается 16 циклам шифрования согласно уравнению (2). Ре-

зультат этой операции суммируется по модулю 2 с $T_0^{(2)}$ и $\varphi(T_0^{(1)})$, и $\varphi(T_0^{(2)})$ снова преобразуется в режиме защиты согласно уравнению (2). Данные процедуры повторяются m раз.

Из последовательности $a^m{}_{(16)}$ полученного 64-битового числа следует сформировать имитовставку (отрезок из p бит), равную

$$И_p = [a^{(m)}_{32-p+2}(16),\ a^{(m)}_{32-p+2}(16),...,a^{(m)}_{32}(16), a^{(m)}_{32}(16)],$$

$$32 - p + 1 \le i \le 32.$$

Для рассматриваемой КС с $p = 12$ выражение для имитовставки $И_p$ примет вид

$$И_{12} = [a_{21}, a_{22}, \ldots, a_{32}].$$

Имитовставка формируется пользователем рабочей станции и передается по каналу связи в конце зашифрованных данных $T^{(1)}_{ш}, T^{(2)}_{ш}, \ldots, T^{(ь)}_{ш}, И_{12}$. Поступившее на сервер сообщение расшифровывается и из блоков $T_0^{(1)}, T_0^{(2)}, \ldots, T_0^{(M)}$, аналогичным образом вырабатывается имитовставка $И'_p$, сравнение величин $И_p$ и $И'_p$ позволяет сделать вывод о целостности полученной информации.

Структурная схема вычислительных процедур обеспечения конфиденциальности и целостности приведена на рис. 2.

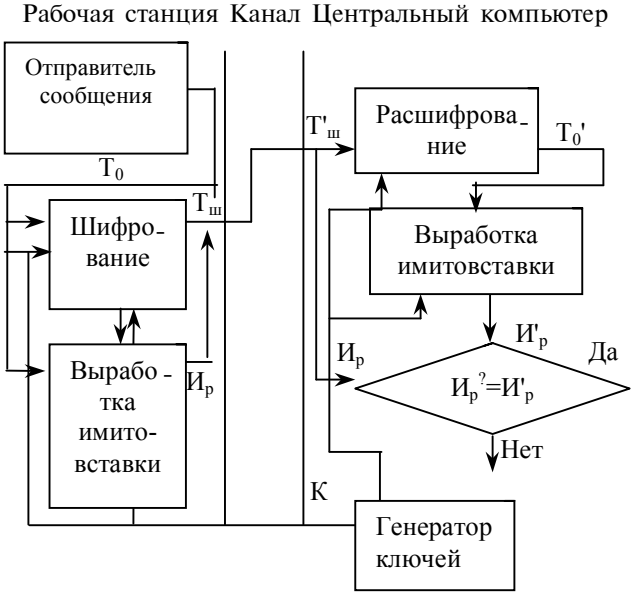

Рис. 2

Рассмотренные функции шифрования и дешифрования программно реализованы в виде Windows-приложения Kanaris, разработанного в среде Borland Delphi 4.0. Приложение рассчитано на работу с несколькими пользователями, каждый из которых должен иметь дискету, содержащую доступные ему ключи, защищенные индивидуальным паролем. Для организации избирательного управления доступом субъектов предусмотрено независимое приложение KeyCreator. Данное приложние генерирует для каждого пользователя файл с указанием его прав доступа на все виды информации. Доступ к содержимому файлов осуществляется после идентификации субъекта.

Приложение Kanaris имеет модульную структуру. Функции отдельных модулей и образующие их файлы приведены в таблице.

Имя файла	Функция модуля
Kanaris.dpr	Главный связующий модуль программы
Form1.pas,Form1.dfm	Главное окно приложения
Form2.pas,Form2.dfm	Диалог смены ключей шифрования
Form3.pas,Form3.dfm	Диалог шифрования файла
Form4.pas,Form4.dfm	Диалог дешифрования файла
Form5.pas,Form5.dfm	Диалог смены паролей
Form6.pas,Form6.dfm	Диалог ввода пароля

Главное окно приложения представляет собой панель с кнопками, активизирующими функции защиты и сопутствующие действия: Шифровать файл, Дешифровать файл, Сменить ключи, Сменить пароли, Помощь, Выход. Каждой кнопке соответствует пиктограмма и оперативная подсказка (Hint), разъясняющая ее действие. Достоинством пользовательского интерфейса следует считать минимум занимаемого им пространства на Рабочем Столе Windows. Это весьма существенно с учетом необходимости его постоянного размещения на экране ПК, что исключает помехи при работе пользователя с другими приложениями.

Апробация разработанного программного продукта подтвердила его работоспособность.

Литература: 1. *Мафтик С.* Механизмы защиты в сетях ЭВМ. М.: Мир, 1993. 216 с. 2. *ГОСТ* 28197–89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

Поступила в редколлегию 25.05.2000

Рецензент: д-р техн. наук, проф. Авраменко В.П.

Садат Кхудир, аспирант кафедры ИУС факультета КН ХТУРЭ. Научные интересы: управление потоками информации в компьютерных сетях, теория телетрафика. Увлечения: французская лингвистика, путешествия по странам Европы и Ближнего Востока. Адрес: 61154, Украина, Харьков, пр. Героев Труда, 24, кв.22, раб. тел. 40-94-51.

Гавриш Татьяна Валентиновна, канд. техн. наук, доцент кафедры ИУС факультета КН ХТУРЭ. Научные интересы: прикладная теория надежности, методы защиты информации, геоинформационные системы. Увлечения: бег с препятствиями, купание в ледяной воде. Адрес: Украина, 61024, Харьков, ул. Мироносицкая, 99, кв. 30, дом. тел. 43-69-33.