УДК 621.3+681.326

Разработка защищенных приложений в рамках ИПИ-технологий

А. В. Трищенков, А. А. Мартынов, В. Л. Ведерников

Все разрабатываемые принципиальные электрические схемы и проекты печатных плат содержат коммерческую информацию, поэтому возникает необходимость обеспечения их сохранности. Для решения этой задачи была создана прикладная программа, позволяющая преобразовывать исходные данные с использованием криптографического алгоритма преобразования данных DES. Данная программа реализована как самостоятельный блок, который интегрирован в оболочку системы P-CAD.

Результаты разработки являются важным этапом во внедрении ИПИ-технологий в реально действующий производственный процесс и позволяют оперативно и надежно осуществлять взаимодействие между структурными подразделениями предприятия любого вида деятельности.

В настоящее время на предприятиях активно ведутся работы по сквозному проектированию односторонних, двусторонних и многослойных, а также рельефных, печатных плат аналоговых, цифровых и аналого-цифровых устройств на базе сквозной системы автоматизированного проектирования P-CAD 2004 [1].

Система проектирования радиоэлектронной аппаратуры P-CAD, разработанная первоначально фирмой ALTIUM, на сегодняшний день является одной из самых мощных, полных и последовательных систем автоматизированного проектирования для персональных компьютеров. Изначально P-CAD представлял собой пакет специализированных модулей, тесно связанных друг с другом и охватывающих все этапы разработки и изготовления печатных плат. Начиная с версии P-CAD 2001, в состав пакета включен модуль схемотехнического моделирования электронных устройств, позволяющий проектировать аналоговые, логические и смешанные, аналого-цифровые устройства и идеально вписывающийся в концепцию развития и внедрения ИПИ-технологий.

Программные средства системы позволяют автоматизировать весь процесс проектирования электронных средств, начиная с ввода принципиальной схемы, ее моделирования, упаковки схемы на печатную плату, интерактивного размещения радиоэлектронных компонентов на печатную плату и ее автоматической трассировки, вплоть до получения конструкторской документации и подготовки информации для производства плат на технологическом оборудовании.

Система P-CAD 2004 предназначена для проектирования многослойных печатных плат аналоговых, цифровых и аналого-цифровых устройств. Она состоит из четырех основных модулей и ряда вспомогательных программ, показанных на рис. 1 [1, 2].

Редактор схем – Schematic. Графический редактор для ввода электрических принципиальных схем изделий. Легко позволяет создавать сложные многолистовые схемы, в том числе с иерархической структурой. Обладает средствами проверки схем. Позволяет создавать и помещать в библиотеки символы новых компонентов и редактировать существующие.

Редактор печатных плат – PCB. Графический редактор для работы с односторонними, двухсторонними и многослойными печатными платами. Позволяет в ручном режиме создавать контур

печатной платы, проводить размещение компонентов. В ручном и интерактивном режимах может быть осуществлена трассировка и редактирование проводников. Осуществляет контроль за соблюдением установленных технологических норм и правил. Позволяет выделять на плате отдельные участки с различными проектными нормами.

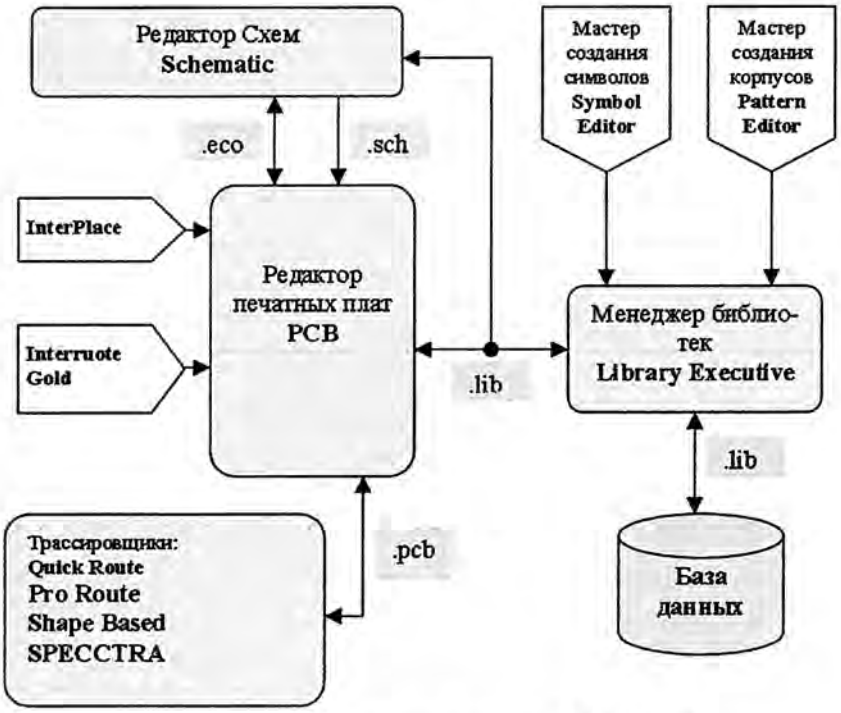

Рис. 1. Структурная схема системы P-CAD 2004

Library Executive – менеджер библиотек с расширенными возможностями. Предназначен для работы с интегрированными библиотеками, которые содержат графическую информацию о символах и типовых корпусах компонентов и текстовую упаковочную информацию.

Interrout Gold – дополнительная утилита для PCB, позволяющая в интерактивном режиме прокладывать проводники, автоматически раздвигая мешающие. Существенно облегчает и ускоряет процесс ручной и интерактивной трассировки проводников.

Система P-CAD 2004 выполняет полный цикл проектирования печатных плат, а именно:

– графический ввод электрических схем;
– смешанное аналого-цифровое моделирование на основе ядра SPICE3;
– упаковку схемы на печатную плату;
– интерактивное размещение компонентов;
– ручную, интерактивную и автоматическую трассировку проводников;
– контроль ошибок в схеме и печатной плате;
– подготовку к выпуску конструкторской документации;
– анализ целостности сигналов и перекрестных искажений;
– подготовку файлов управляющих программ для производства печатных плат;
– подготовку библиотек символов, топологических посадочных мест и моделей компонентов.

В связи с тем, что данный программный продукт является зарубежным, то возникает вопрос о создании библиотек отечественных радиоэлементов. Все библиотеки элементов создаются сред-

ствами системы P-CAD на производстве и представляют собой коммерческую информацию, но становится актуальным другой вопрос – это вопрос об обеспечении надежного хранения и передачи данных. Все разрабатываемые принципиальные электрические схемы и проекты уже готовых печатных плат также содержат коммерческую информацию, поэтому возникает необходимость обеспечения их сохранности. Таким образом, был реализован программный комплекс, позволяющий преобразовывать исходные данные (будь то библиотеки элементов, электрические схемы, проекты печатных плат либо управляющие программы для станков с числовым программным управлением) с использованием стандарта преобразования данных Data Encryption Standard (DES) [3, 4]. Данный программный комплекс выделен в самостоятельный блок, который был интегрирован в оболочку системы P-CAD. Общий вид редактора PCB со встроенным модулем шифрования приведен на рис. 2.

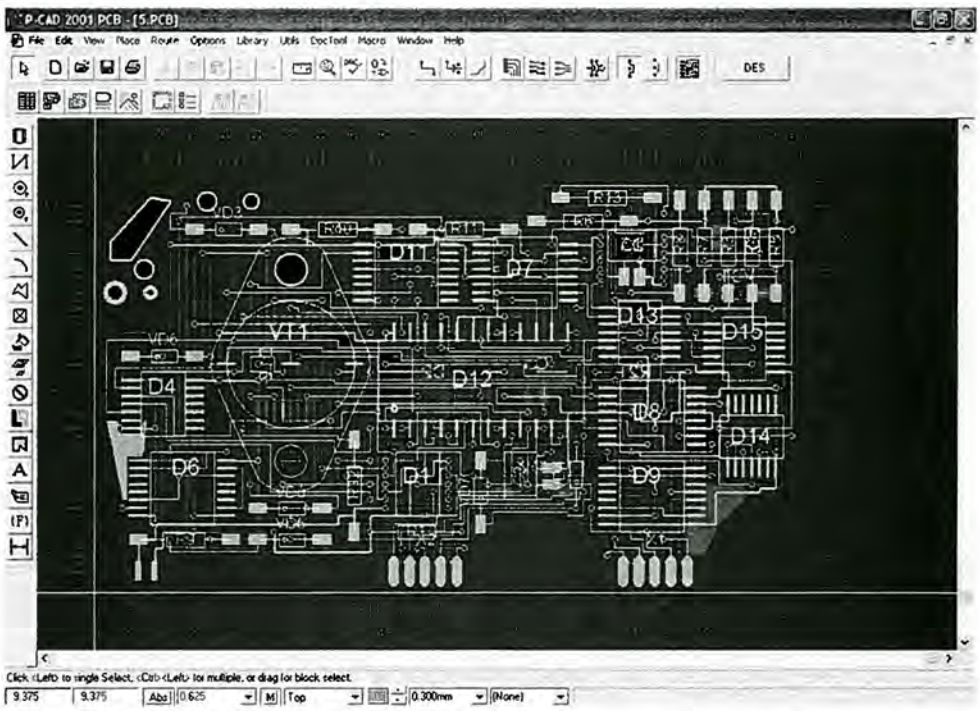

Рис. 2. Общий вид редактора PCB со встроенным модулем шифрования данных Data Encryption Standard

Криптографический алгоритм DES осуществляет шифрование 64-битовых блоков данных с помощью 56-битового ключа. Дешифрование в DES является операцией обратной шифрованию и выполняется путем повторения операций шифрования в обратной последовательности (несмотря на кажущуюся очевидность, так делается далеко не всегда).

Процесс шифрования заключается в начальной перестановке битов 64-битового блока, шестнадцати циклах шифрования и обратной перестановке битов, что показано на рис. 3.

Необходимо сразу же отметить, что все таблицы, приведенные в данной статье, являются стандартными, а следовательно, включены в данную реализацию алгоритма в неизменном виде. Все перестановки и коды в таблицах подобраны разработчиками таким образом, чтобы максимально затруднить процесс расшифровки путем подбора ключа.

Пусть из файла считан очередной 8-байтовый блок T, который преобразуется с помощью матрицы IP (табл. 1) начальной перестановки.

Рис. 3. Общая схема стандарта шифрования DES

Таблица 1

Матрица начальной перестановки *IP*

T0 = IP(T)							
58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

Затем шестнадцать раз повторяется процедура шифрования этого блока с помощью функции *f*.

Пусть T_i обозначает результат i-й итерации. Тогда предположим, что $L_i = t_1 \ldots t_{32}$, (первые 32 бита) и $R_i = t_{33} \ldots t_{64}$ (последние 32 бита), т. е. $T_i = L_i R_i$.

Тогда результатом i-й итерации будет

$$L_i = R_{i-1} R_i = L_{i-1} + f\left(R_{i-1}, K_i\right),$$

где + – операция "исключающее или"; K_i – i-е преобразование ключа шифрования.

Функция f выполняет операции над значением R_{i-1} (результатом предыдущей операции) и текущим значением 48-битового ключа K_i (с отсечением лишних битов). После шестнадцатой итерации левая и правая половины блока местами не меняются, что показано на рис. 4.

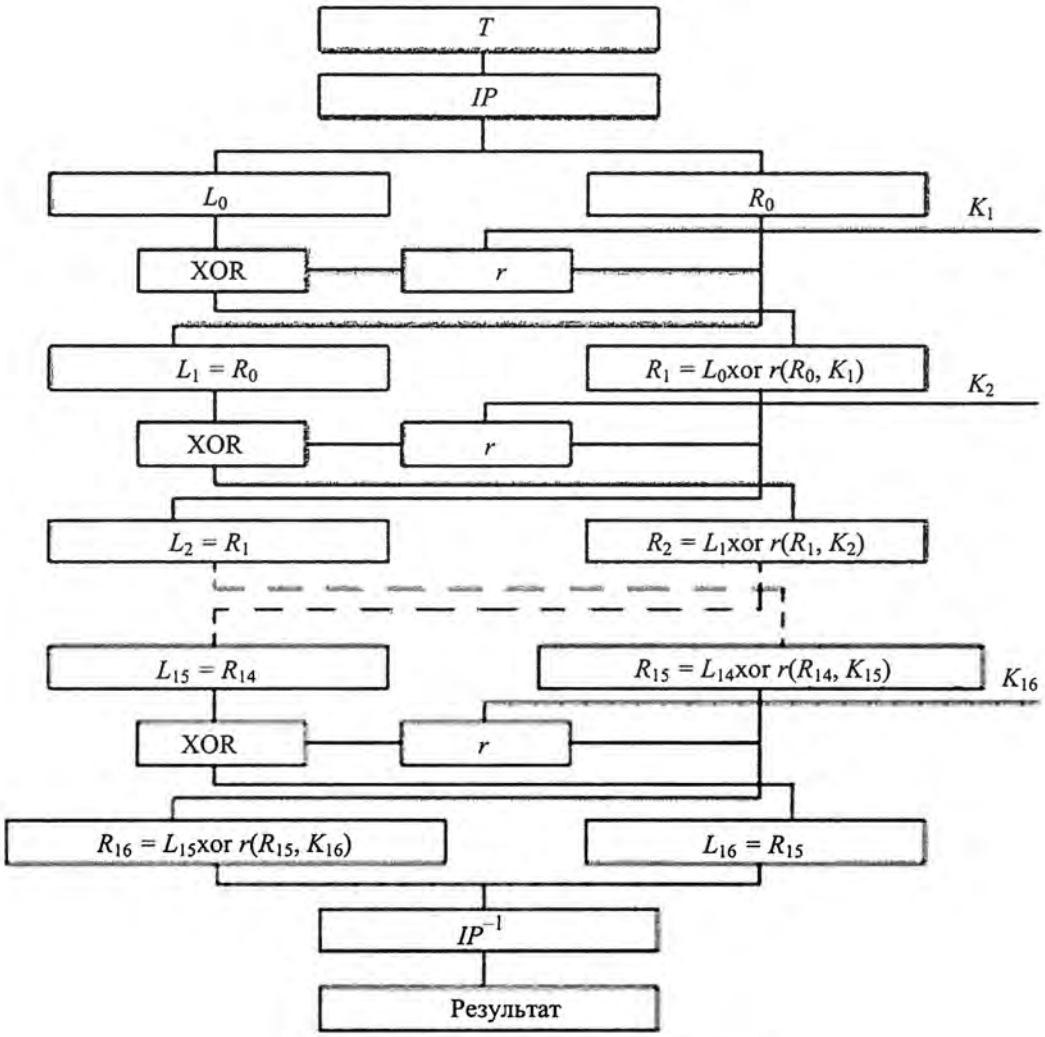

Рис. 4. Общая блок-схема стандарта DES

По окончании шифрования осуществляется восстановление позиций битов с помощью матрицы перестановок IP^{-1} (табл. 2).

Таблица 2

Матрица обратной перестановки IP^{-1}

$T0 = IP^{-1}(T)$							
40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	09	49	17	57	25

Теперь рассмотрим, что же скрывается под преобразованием, скрытым функцией *f*.

На каждой итерации массив R_{i-1} с помощью таблицы распределения *E* (табл. 3) расширяется до 48 битов.

Таблица 3

Матрица распределения битов *E*

32	01	02	03	04	05
04	05	06	07	08	09
08	09	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	01

Полученный результат (обозначим его $E(R_{i-1})$) складывается по модулю 2 (операция XOR) с текущим значением ключа K_i и затем разбивается на восемь 6-битовых блоков $B_1 \ldots B_8$. То есть $E(R_{i-1}) + K_i = B_1 B_2 \ldots B_8$. Далее каждый элемент из этих блоков используется как номер элемента в матрицах $S_1 \ldots S_8$, содержащих 4-битовые значения (табл. 4).

Таблица 4

Матрица преобразования 6*4 $S_1 \ldots S_8$

Номер строки	Номер столбца																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	S_1
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	S_2
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	S_3
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	S_4
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	
2	10	6	9	0	12	11	7	13	15	1	3	14	4	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	S_5
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	

Окончание таблицы 4

Номер строки	Номер столбца																
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	S_6
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	S_7
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	S_8
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

В результате, применив операцию выбора к каждому из блоков, получаем $S_1(B_1)S_2(B_2)S_3(B_3)...S_8(B_8)$.

Полученный 32-битовый блок (матрицы S_j содержат 4-битовые значения) преобразуем с помощью матрицы перестановки P (табл. 5).

Таблица 5

Матрица перестановки битов P

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

Таким образом, $f(R_{i-1}, K_i) = P(S_1(B_1),...S_8(B_8))$.

Общая схема данного участка алгоритма представлена на рис. 5.

Следует отметить, что выбор элемента в матрице S_j осуществляется достаточно оригинальным образом. Пусть на вход поступает 6-битовый блок $B_j = b_1b_2b_3b_4b_5b_6$, тогда 2-битовое число b_1b_6 выбирает строку матрицы, а $b_2b_3b_4b_5$ – номер столбца. Результатом $S_j(B_j)$ будет 4-битовое число, расположенное по указанному адресу.

На каждой итерации используется новое значение ключа K_i, которое вычисляется из начального ключа K. Ключ K представляет собой 64-битовый блок с восемью битами контроля четности, расположенными в позициях 8, 16, 24, 32, 40, 48, 56, 64.

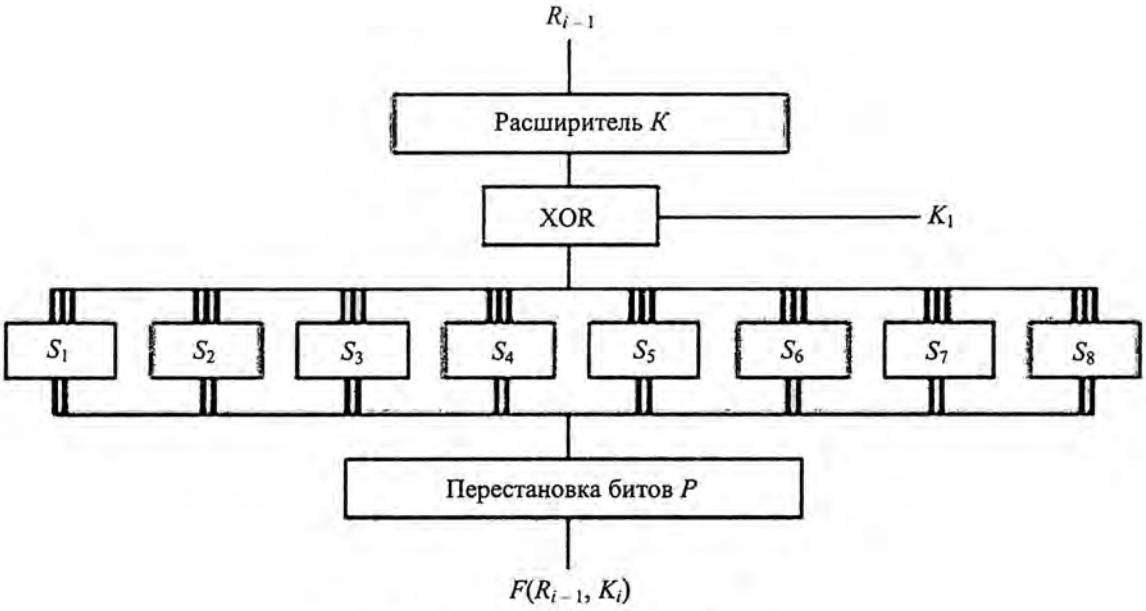

Рис. 5. Вычисление функции $F(R_i, K_i)$

Для удаления контрольных битов и подготовки ключа к работе используется матрица PC^{-1} (табл. 6).

Таблица 6

Матрица первоначальной подготовки ключа

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Результат преобразования PC^{-1} (K) разбивается на две половины C_0 и D_0 по 28 битов каждая. После этого блоки C_0 и D_0 на каждой итерации последовательно сдвигаются влево. Пусть C_j и D_j обозначают значения, полученные на i-й операции:

$$C_i = LS_i(C_{i-1}) \text{ и } D = LS_i(D_{i-1}),$$

где LS_i представляет собой i-й элемент матрицы сдвига LS (табл. 7).

Полученное значение вновь перемешивается в соответствии с матрицей PC^{-2} (табл. 8).

Таблица 7

Таблица сдвигов для вычисления ключа

Номер итерации	Сдвиг (бит)
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Таблица 8

Матрица завершающей обработки ключа

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Таким образом, $K_i = PC^{-1}(C_i D_i)$.

Блок-схема алгоритма вычисления *i*-й итерации ключа приведена на рис. 6.

Восстановление исходного текста осуществляется по этому алгоритму, но вначале используется ключ K_{16}, затем – K_{15} и т. д.

Для установки программы шифрования/дешифрования по алгоритму DES необходимо запустить программу SETUP из установочного пакета, и выполнив стандартную установку под Windows, установить программный продукт, следуя подсказкам системы.

Для выполнения операции шифрования либо дешифрования по алгоритму DES необходимо запустить программу DES Crypt. После этого появится окно, показанное на рис. 7.

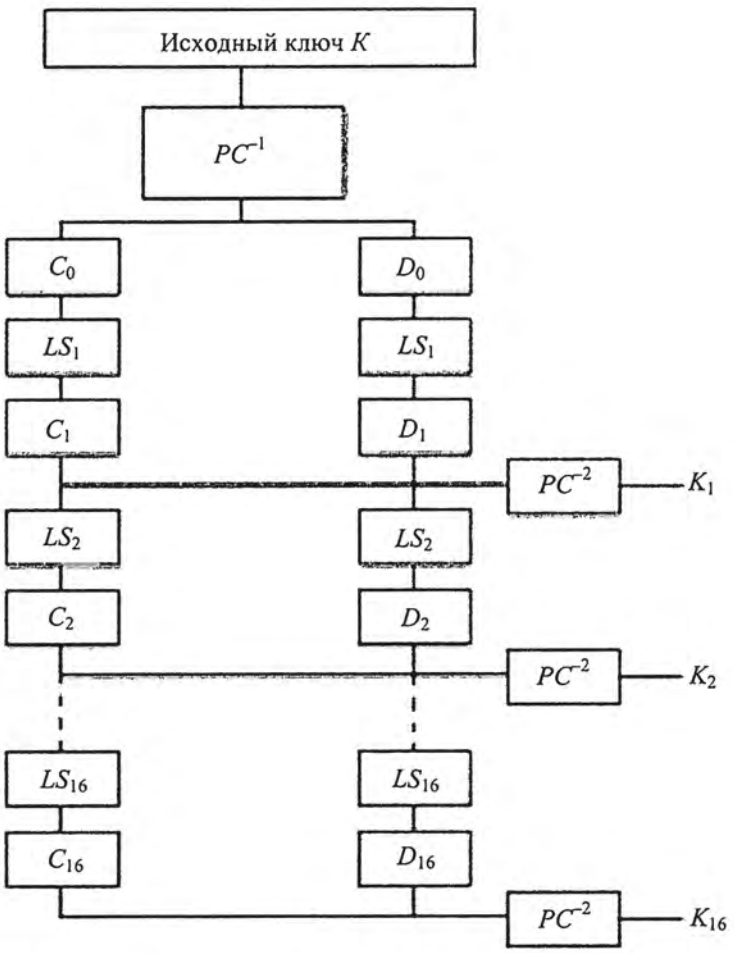

Рис. 6. Блок-схема алгоритма вычисления ключа

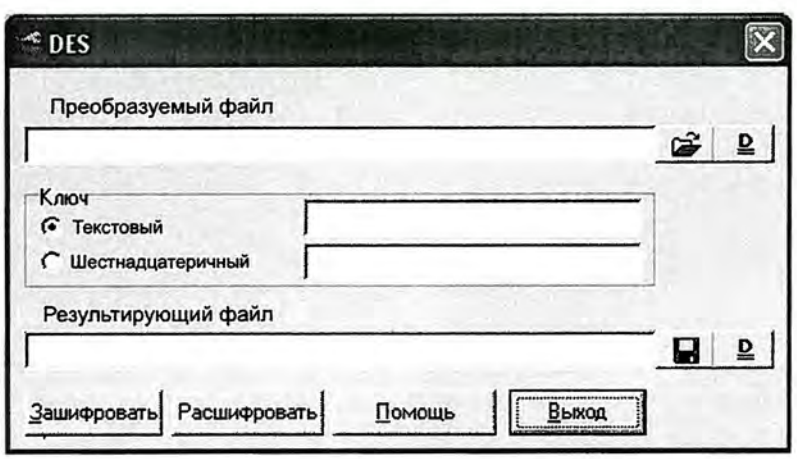

Рис. 7. Рабочее окно программного модуля DES

В строкс "Преобразуемый файл" указывается путь к файлу, который необходимо зашифровать. В строке "Результирующий файл" указывается путь к файлу, в который будут помещены зашифрованные данные. Если такого файла нет, то программа DES Crypt выдаст окно, в котором сообщит об отсутствии данного файла и предложит создать его.

Пути к файлам можно указать напрямую в строке или воспользоваться кнопкой открытия/сохранения файла. Для просмотра файлов необходимо нажать кнопку просмотра.

В программе DES Crypt предусмотрено два варианта задания ключа:

– в текстовом (символьном) виде;

– в шестнадцатеричном виде.

Когда выполнены все эти указания, необходимо нажать кнопку "Зашифровать" либо "Расшифровать". После этого программа выдаст сообщение “Файл преобразован” и информация будет зашифрована либо расшифрована.

Для получения справочной информации о программе DES Crypt необходимо нажать правую кнопку мыши.

Для получения информации о стандарте DES и руководства пользователя программой DES Crypt необходимо нажать кнопку "Помощь".

Список литературы

1. Разевиг В. Д. Система P-CAD 2000. Справочник команд. М.: Горячая линия – Телеком, 2000.

2. Сучков Д. И. Адаптация САПР P-CAD к отечественному технологическому оборудованию. М.: Призма, 1993.

3. Диев С. А., Шаваев А. Г. Организация и современные методы защиты информации. М.: Концерн "Банковский Деловой Центр", 1998.

4. Галатенко В. А. Информационная безопасность. НН.: Открытые системы, 1995.

Development of Protected Applications in the Framework of IPI-Technologies

A. V. Trischenkov, A. A. Martynov, V. L. Vedernikov

All basic electric circuits and designs of printed circuit boards contain commercial information. Thus the necessity to provide their safety arises. An application program making possible to transform initial data using cryptographic algorithm for translating DES data has been developed to solve this problem. The program has been accomplished as a self-contained unit integrated in the P-CAD system shell.

The results of development are of great importance when commissioning IPI technologies in a real industrial process. They provide efficient and reliable interaction between subdivisions of enterprise engaged in any kind of activity.