УДК 621.372

А.П. Пеньков, В.В.Герасимов

СИСТЕМНЫЕ АСПЕКТЫ РАЗРАБОТКИ КРИПТОСИСТЕМ

Аннотация. Рассмотрены методологические аспекты поведения разработчика и заказчика криптосистем, которые позволяют разработчику быть уверенным, инициативным, отслеживать процесс разработки, находить общий язык с заказчиком.

Ключевые слова: инженер, система, модель, триединство, информатика, разработчик, заказчик, предмет труда, средство труда.

Актуальность. Современные криптосистемы являются классом развивающихся встроенных систем в компьютерных и коммуникационных системах. Это требует подготовки соответствующих инженеров системотехников для рыночных условий.

Анализ источников. В [1] исследована методология подготовки инженеров-системотехников, их эволюции. Такой специалист является "исследователем, конструктором и администратором", должен "уметь объединить разных специалистов для совместной работы, понимать их..., быть универсалом..."

Согласно [2]разработчик и заказчик должны согласовать свои точки зрения и совместно разработать техническое задание (ТЗ) на разработку. Следует обратить внимание на специфику разработки криптосистемы.

Очевидна особенность формирования инженеров-системотехников в вузе. В [1] предлагается специально готовить универсалов. А как готовить специалистовпо разработке криптосистем?

Постановка задачи. Необходимо использовать комплекс системных моделей деятельности инженера, разработать подход к проектированию криптосистем.

Решение задачи. В [3] при разработке сложных систем рекомендовано использовать "триединство информатики" (модель — алгоритм — программа), предложенное академиками А.И. Самарским и А.А. Дородницыным в качестве общей модели информатики в 1984

 ISSN 1562-9945

г.Очевиден приоритет модели и необходимость её правильного выбора. В проведенном представлении уже очевидны этапы учебный (изготовление разработчика) и проектный (разработка технической системы). Представим это в виде цепи Маркова (рис. 1):

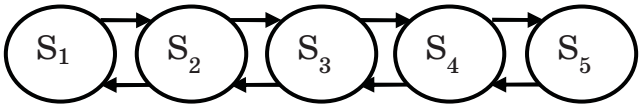

Рисунок1 — Цепь Маркова учебного и проектного этапов

где:S_1 — первичный источник полной информации; S_2 — преобразователь сообщений от S_1; S_3 — потребитель сообщений от S_2, будущий разработчик; S_4 — заказчик на разработку конкретной системы; S_5 — разработанная система.

Рассмотрим особенности $\overline{S_1, S_5}$ в применении к криптосистемам. В интернете S_1 по криптосистемам представлен описанием отдельных систем и математических моделей в объеме, не возможном для признания в качестве конкретных методических рекомендаций. Случайный авторский характер известных криптосистем зафиксирован в их названиях по фамилиям авторов. Нет обобщения опыта деятельности инженера при разработке секретной технической системы (разработка — производство — испытания — применение) с формированием необходимой секретной сопроводительной документации всех этапов в обычном и специальном виде.

На этапе S_2 источники S_1 сжаты до [4-6], где источник 4 — самая читаемая в мире книга энциклопедия по криптографии, источники 5 и 6 — учебные пособия, основанные на 4. Энциклопедический характер и объем источника 4 ухудшает её читаемость. Терминологическая неупорядоченность привела к случайному распределению конкретного материала источника 4 практического характера. Пособия 5 и 6 сокращены примерно в 5 раз по отношению к источнику 4. Но, как и в источнике 4, в последних используется жаргон, терминологическая неточность (на одном уровне используются понятия "алгоритм", "криптосистема" и т.д.).

Очевидно, что использование методического обеспечения S_2 для S_3 приведет к профессиональной неопределенности практической разработки, к трудностям отношений с разработчиком S_3. Необходимо предложить общую модель мышления для S_3 и S_4. Такая модель получена одним из авторов в 1984 г. для проектной модели дисплея и в

1999 г. обнаружена в [7] в качестве системы охраны труда $S_{тр}$. Эта модель $S_{тр}$ использована для построения обобщенной системы труда "шифрования — передачи — дешифрования" $S_{ш/дш}$ (рис. 2) и проверена на методах шифрования с закрытым ключом (см. примеры).

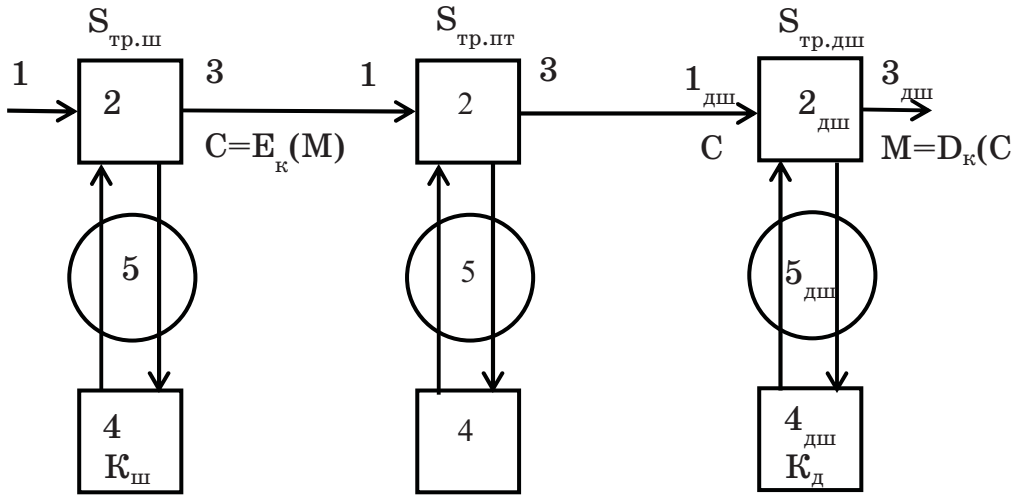

Рисунок 2 —Структурно-функциональная модель формирования и обработки секретных сообщений

На рис. 2 использованы следующие обозначения:$1_ш$ — исходный текст, документ; $2_ш$ — обрабатываемый текст; $3_ш$ — зашифрованный текст, шифротекст; $4_ш$ — средства шифрования; $5_ш$ — алгоритм шифрации; $1_{дш} \equiv 3$; $2_{дш}$ — обрабатываемый исходный текст; $3_{дш} \equiv 1_ш$; $4_{дш}$ — средства дешифрации; $5_{дш}$ — алгоритм дешифрации; $1 \equiv 3_ш$, исходное сообщение на входе линии связи; 2 — сообщение на линии связи с шумами; 3 — очищенное от шумов сообщение; 4 — средства борьбы с шумами; 5 — алгоритм очищения от шумов; C — шифротекст; M — открытый текст; E — функция шифрования; D — функция дешифрования; $К_ш$ — ключ шифрования; $К_{дш}$ — ключ дешифрования.

Элементы $S_{ш/дш}$:

- подсистема $1 \equiv M = \sum i_M = \sum i_1$, где i_M, i_1 — знак исходного документа;

- подсистема $2 \equiv \sum i_2 = \sum i_1'$, где i_1' — текущее значение i_1;

- подсистема $3 \equiv C = \sum i_C = \sum i_3 = \sum i_4'$, где i_3, i_C— знаки шифротекста, i_4' — выбранные текущие элементы средства 4;

- подсистема $4 \equiv \sum i_4$, где i_4 — знаковые элементы;

- подсистема 5 — алгоритм шифрования/дешифрования.

Общий алгоритм создания криптосистемы $S_{ш/дш}$:

 ISSN 1562-9945

1. Признать деятельность по структурно-функциональной модели $S_{ш/дш}$.

2. Обратить внимание на цели и связи элементов $S_{ш/дш}$.

3. Построить модель 2 текстового сообщения 1.

4. Построить модель средства шифрования 4.

5. Построить модель получения элементов 3.

6. Реализовать преобразование.

На текущий момент существуют такие известные методы шифрования с закрытым ключом:

1. Методы замены (подстановки):одноалфавитная, многоалфавитная.

2. Методы перестановки:простая (с фиксированным периодом), табличная, усложненная по маршрутам.

3. Комбинированные методы: блочные шифры, поточные шифры.

4. Другие методы: смысловые, сжатие/расширение.

Рассмотрим алгоритм одноалфавитной подстановки на примере шифра Цезаря. Шаги 1, 2 общего алгоритма шифрования сохраняются. Каждая буква сообщения заменяется на знак алфавита, который от соответствующего знака сообщения отстоит (сдвинут) на *n*позиций дальше. Например, сообщение (1) — "замена". Его модель (2):

Подсистема (4) — русский алфавит. Его модель

$$\frac{\text{абвгдеёжзийклмнопрстуфхцчшщъыьэюя}}{12345678901234567890123456789012 3} = i_4\big|_{1\ldots 33}.$$

Модель получения элементов шифротекстаi_3 (шифрования):

$$i_3|_{1\ldots 6} \equiv (i_1|_{1\ldots 6} = i_4|_{1\ldots 6} / "+"" - " n_{1\ldots 33}),$$

где n_{var} — задаваемая связь $i_1|_j c i_3|_j$, может быть признана "секретным ключом".

Пусть n=3. Тогда $i_3\big|_1 = з * \frac{ийк}{123} \to к$; $i_3\big|_2 = а * \frac{бвг}{123} \to г$; $i_3\big|_3 = м * \frac{ноп}{123} \to п$; $i_3\big|_4 = е * \frac{ёжз}{123} \to э$; $i_3\big|_5 = н * \frac{опр}{123} \to р$;. Шифротекст С=(3)="кгпзрг". При расшифровке вместо "+n" в примере используется "-n" (-3).

Далее рассмотрим пример одноалфавитной подстановки с использованием таблиц замены. Шаги 1 и 2 общего алгоритма $S_{ш/дш}$ сохраняются. Исходное сообщение (3) не меняется. Средством шифрования (4) является таблица строчного соответствия элементов i_1 алфа-

вита исходного текста (1) и элементов i_3 алфавитов шифров $1_ш \cup 2_ш$, являющаяся закрытым ключом. Это можно представить моделью, представленной в табл. 1.

Дешифрация осуществляется по модели шифрации в обратном порядке.

Криптоаналитикииспользуют статистические закономерности естественных языков в исходных текстах (1) (частоты встречаемости символов, их сочетания и т.д.). Эти характеристики маскируются применением сжатия открытого текста компьютерными программами-архиваторами.

Таблица 1

Связь i_1 с i_3 по строкам

Таблица алфавита (1)	Таблица 1 алфавита (3), буквенный шифр 1	Таблица 2 алфавита (3), знаковый шифр 1
А	В	^
Б	И	@
В	О	)
Г	А	+
Д	Щ	<
Е	П	>
...	...	...

Выводы. Представленные системные модели деятельности разработчика криптосистем позволяют ему быть уверенным, инициативным, отслеживать процесс разработки, достигнуть общего языка мышления с заказчиком, сделать его соавтором разработки, заставить его уточнить понимание требований заказчика к разработке, её оптимизации.

ЛИТЕРАТУРА

1. Горохов В. Г. Методологический анализ системотехники. — М.: Радио и связь, 1982. — 240 с.
2. Захаров В. Н., Поспелов Д. А., Хазацкий В. Е. Системы управления. Задание. Проектирование. Реализация. — М.: Энергия, 1977. — 424 с.
3. Краснощеков П. С., Петров А. А., Федоров В. В. Информатика и проектирование. — М.: Знание, 1986. — 48 с.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. — М.: ТРИУМФ, 2002. — 816 с.
5. Емец В., Мельник А., Попович Р. Сучасна криптографія. Основні поняття. — Львів, Бак, 2003. — 44 с.
6. Басалова Г. В. Основы криптографии. Уч. пособие. — Тула: Тульский госуниверситет, 2009. — 145 с.
7. Мардахаев А. А. Охрана труда. История, теория, практика. — Львов: "Вища школа", 1984. — 240 с.

 ISSN 1562-9945