УДК 681.327.8:519.81
В.К. Маригодов, проф., д-р техн. наук
Севастопольский национальный технический университет
Студгородок, г. Севастополь, Украина, 99053
root@sevgtu.sebastopol.ua

ОЦЕНКА ПРАКТИЧЕСКОЙ СТОЙКОСТИ ШИФРА В СИСТЕМАХ ПЕРЕДАЧИ ИНФОРМАЦИИ

На основе расчета трудоемкости алгоритмов зашифрования и криптоанализа определена практическая стойкость шифра, которая количественно выражается проигрышем во времени криптоаналитика по сравнению с шифровальщиком.

В качестве оценки практической стойкости шифра обычно используются трудозатраты, которые необходимы криптоаналитику для дешифрования при наличии зашифрованного текста. Предполагается, что зашифрованный текст может быть получен в результате несанкционированного доступа к каналу связи. Под дешифрованием понимается либо получение открытого текста, либо вскрытие ключей шифра. Мерой трудоемкости может служить количество элементарных операций, которые нужно выполнить для дешифрования, а также время, необходимое для реализации алгоритма дешифрования на основе применения вычислительной техники.

Предположим, что для зашифрования информации, передаваемой по каналу системы передачи информации, применяется алгоритм информации зашифрования ГОСТ 28147-89 [1]. Схема такого алгоритма изображена на рисунке 1. Здесь $x_0, x_1, \dots x_7, N_1, N_2, R$ - 32-разрядные регистры; CM_1 - сумматор по модулю 2^{32}; CM_2 - сумматор по модулю 2; T_0 - 64-разрядный блок открытого текста; $T_ш$ - шифрованный текст.

Регистр $x_0, \dots, x_7$ представляет ключевое запоминающее устройство (КЗУ), в которое записывается 256 битов ключа. Зашифрование очередного блока выполняется за 32 цикла. В первом цикле содержимое регистра N_1 суммируется по модулю 2^{32} в сумматоре CM_1 с x_0, при этом заполнение N_1 сохраняется. В блоке подстановок K осуществляется моноалфавитная подстановка, которая выбирается из 8 возможных, содержащихся в блоке. В регистре R осуществляется циклический сдвиг на 11 битов в сторону старших разрядов. В сумматоре CM_2 выполняется покоординатное сложение по модулю 2 содержимого регистров R и N_2. Полученный на выходе сумматора CM_2 результат записывается в регистр N_1, при этом старое заполнение N_1 перезаписывается в регистр N_2. Последующие циклы выполняются аналогично.

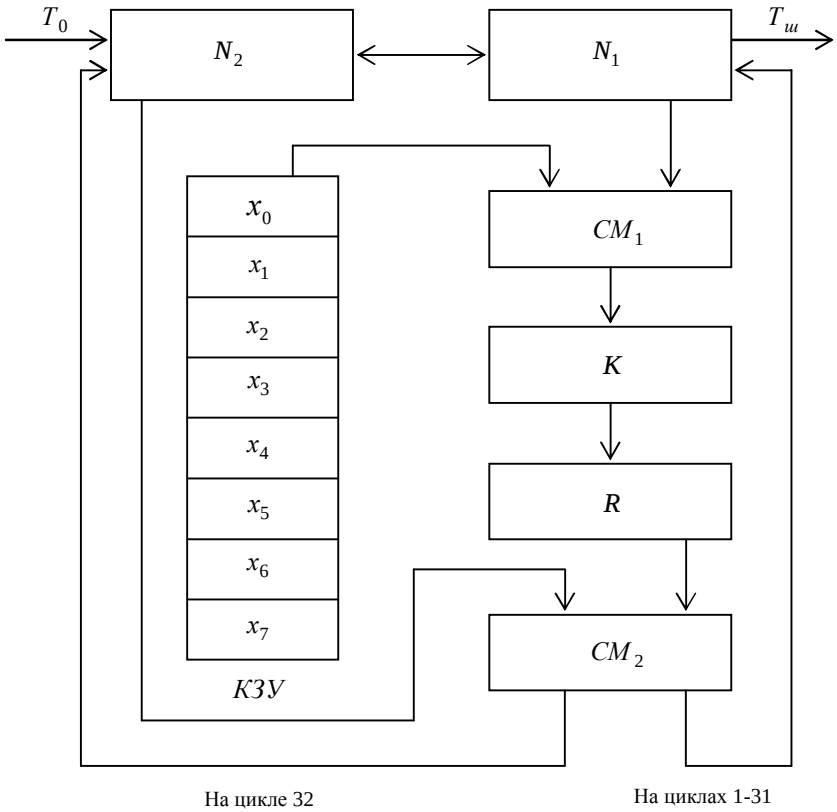

Рисунок 1 – Алгоритм зашифрования

Порядок считывания из КЗУ в режиме зашифрования следующий:

$$x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7;\ x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7;$$
$$x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0;\ x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0;$$
$$x_7, x_6, x_5, x_4, x_3, x_2, x_1, x_0.$$

После 32-го цикла результат из CM_2 вводится в регистр N_2, а в регистре N_1 сохраняется старое значение. Заполнение N_1 и N_2 после 32-го цикла работы схемы является блоком шифрованного текста $Tш$.

Для определения трудоемкостиалгоритма зашифрования обратимся к рисунку2, на которомизображен граф этого алгоритма. Вершинами этого графа являются блоки алгоритма зашифрования (рисунок1), а дуги интерпретируютсвязи между блоками.

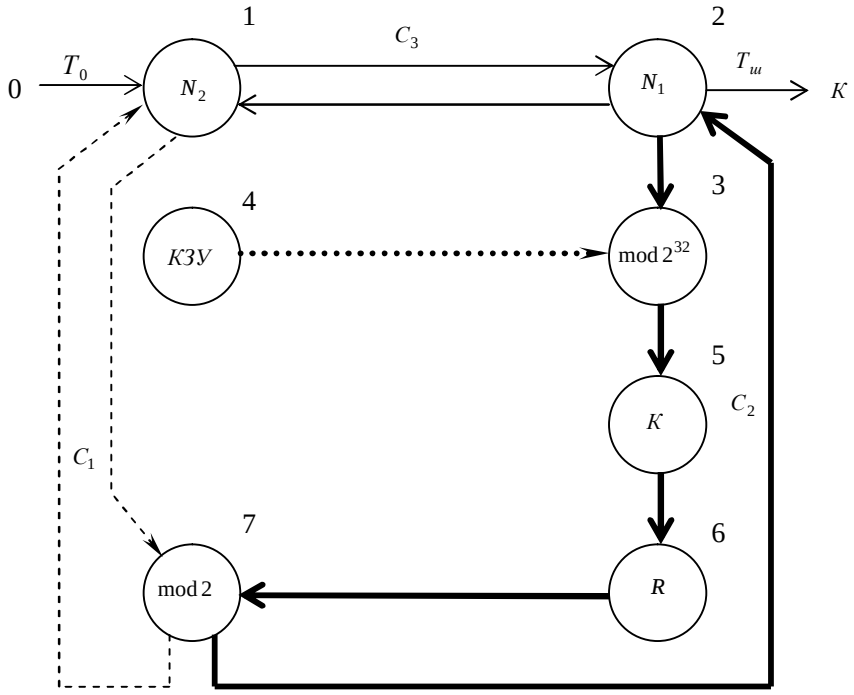

Рисунок 2 – Граф алгоритма зашифрования

Граф алгоритма зашифрования содержит три цикла: C_1 - штриховые линии дуг; C_2 - жирные линии; C_3 - тонкие линии. Предположим, что все операторы каждого из циклов *однотипные* и *основные*. Вероятности переходов между вершинами графа P_{ij}, где i, j – номера соответствующих вершин, обозначенные на рисунке 2 цифрами. Их целесообразно выбрать следующим образом: $P_{1,2}$=0,5; $P_{2,1}$=0,5; $P_{2,3}$=0,3; $P_{2,K}$=0,2; $P_{3,5}$=1; $P_{5,6}$=1; $P_{6,7}$=1; $P_{1,7}$=0,5; $P_{7,1}$=0,1; $P_{7,2}$=0,9; $P_{4,3}$=1. Выбор производится по правилу: P_{ij}=1, если из вершины исходит только одна дуга; если имеется несколько исходящих дуг, то результирующаявероятность равна единице.

Находим среднее количество повторений циклов[2]

$$n_{ci} = 1/(1 - P_{K,l}), \qquad (1)$$

где $P_{K,l}$ - вероятность перехода по дуге, замыкающей цикл; i – номер цикла.

Для циклов графа (рисунок2) из (1) получаем:

$$n_{c1} = \frac{1}{1 - P_{7,1}} = 1{,}1;\ n_{c2} = \frac{1}{1 - P_{7,2}} = 10;\ n_{c3} = \frac{1}{1 - P_{2,1}} = 2.$$

Определяем среднюю трудоемкость тел циклов C_1, C_2, C_3. Для этого полагаем, что трудоемкость каждого из основных операторов равна 10. Если такое же значение трудоемкости принять для основных операторов графа алгоритма дешифрования, то на относительной величине проигрыша криптоаналитика во времени по сравнению с шифровальщиком это допущение не повлияет. Зададим количество операций K_i порождаемых каждым оператором (по числу разрядов, числу подстановок, сдвигов и циклов). Номер индекса i соответствует номеру вершины графа (рисунок 2). Тогда получаем: K_1=32; K_2=32; K_3=32; K_4=7*32=224; K_5=8; K_6=1; K_7=32. Зададим также среднее число обращений к операторам n_i где индекс i

соответствует номеру вершины графа. Для упрощения примем, что в начальных вершинах графа (начинающих цикл) n_i =10.

С учетом этого трудоемкость тела каждого цикла определяется по формуле [2]

$$\theta_{ci} = \sum_{V_j \in C_i} n_i K_i , \qquad (2)$$

где V_j - количество вершин графа , входящих в тело цикла; n_i, K_i - упомянутые выше параметры.

Для тела цикла C_1 находим : n_1=10; $n_7 = P_{1,7} \cdot n_1 = 5$. Тогда в соответствии с (2) получаем $\theta_{c1} = n_1 \cdot K_1 + n_7 \cdot K_1 = 480$ операций.

Аналогично для тела цикла C_2 находим его трудоемкость $\theta_{c2} = n_2 K_2 + n_3 K_3 + n_5 K_5 + n_6 K_6 + n_7 K_7$, где n_2 =10, $n_3 = P_{2,3} \cdot n_2 = 3$, $n_5 = P_{3,5} \cdot n_2 = 10$, $n_6 = P_{5,6} \cdot n_2 = 10$, $n_7 = P_{6,7} \cdot n_2 = 10$.

Подставляя эти значения параметров в выражение для θ_{c2}, получаем θ_{c2} =794 операции.

Для тела цикла C_3 находим $\theta_{c3} = n_1 K_1 + n_2 K_2 = 640$ операций.

Определяем средние трудоемкости для каждого из циклов графа зашифрования как

$$K_{ci} = n_{ci} \theta_{ci} . \qquad (3)$$

Используя (2) и (3), получаем: K_{c1} =528, K_{c2} =7940, K_{c3} =1280.

Заменим циклы графа (рисунок 2) эквивалентными по трудоемкости операторами. В результате такого преобразования получаем граф без циклов (рисунок 3).

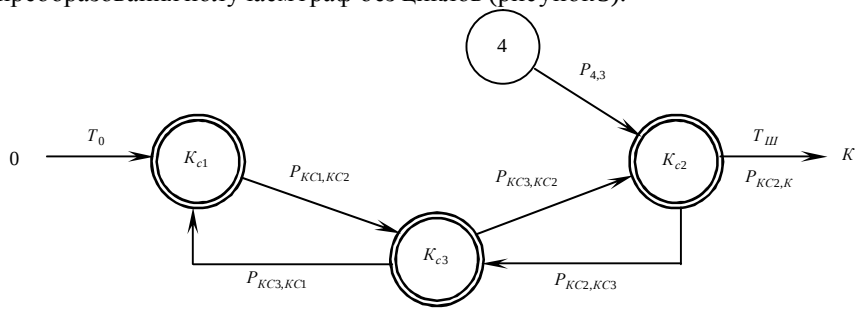

Рисунок 3 – Приведенный граф алгоритма зашифрования

Вероятности переходов для графа (рисунка 3) определяются следующим образом:

$$P_{KC1,KC2} = 1;\ P_{\mathrm{KC3,KC2}} = 0{,}9;\ P_{KC3,KC1} = 0{,}1;\ P_{\mathrm{KC2,KC3}} = 0{,}8;\ P_{\mathrm{KC2,K}} = 0{,}2.$$

Трудоемкость алгоритма приведенного графа равна $\theta_{\sum заш} = K_4 + K_{c2} + 0{,}8K_{c2} + 0{,}1K_{c3} + K_{c1} + + 0{,}9K_{c3} =$ 16384 операции.

Рассмотрим теперь алгоритм дешифрования, который необходим криптоаналитику для получения открытого текста. При этом предполагается, что зашифрованный текст получен в результате несанкционированного доступа к каналу связи. Если криптоаналитику известен алгоритм зашифрования, то дешифровка производится в обратном порядке. Даже при известном типе шифра криптоаналитик не знает порядка считывания информации из КЗУ, модулей суммирования содержимого регистров, количества подстановок и циклов обработки блоков открытого текста. В связи с этим в процессе дешифрования возникает необходимость многократного повторения почти всех операций (десятки и сотни раз).

На рисунке 4 изображен граф алгоритма дешифрования, который может применяться в случае использования ГОСТа 28147-89.

Граф (рисунок 4) содержит три цикла: C_1 - штриховые линии; C_2 - жирные линии; C_3 - тонкие линии. Считаем, что операторы каждого цикла *однотипные* и *основные*. Символы $R^{-1}, \underline{\mathrm{mod}}, K^{-1}$ означают соответственно обратный сдвиг в сторону младших разрядов, вычитание по модулю и обратную моноалфавитную подстановку.

Вероятности переходов между вершинами графа дешифрования выберем следующим образом:
$P_{1,2}$ =0,9; $P_{2,1}$ =0,5; $P_{2,K}$ =0,2; $P_{2,3}$ =0,3; $P_{3,1}$ =0,9; $P_{3,2}$ =0,3; $P_{5,3}$ =1; $P_{6,5}$ =1; $P_{7,6}$ =1; $P_{4,7}$ =1; $P_{1,7}$ =0,1.

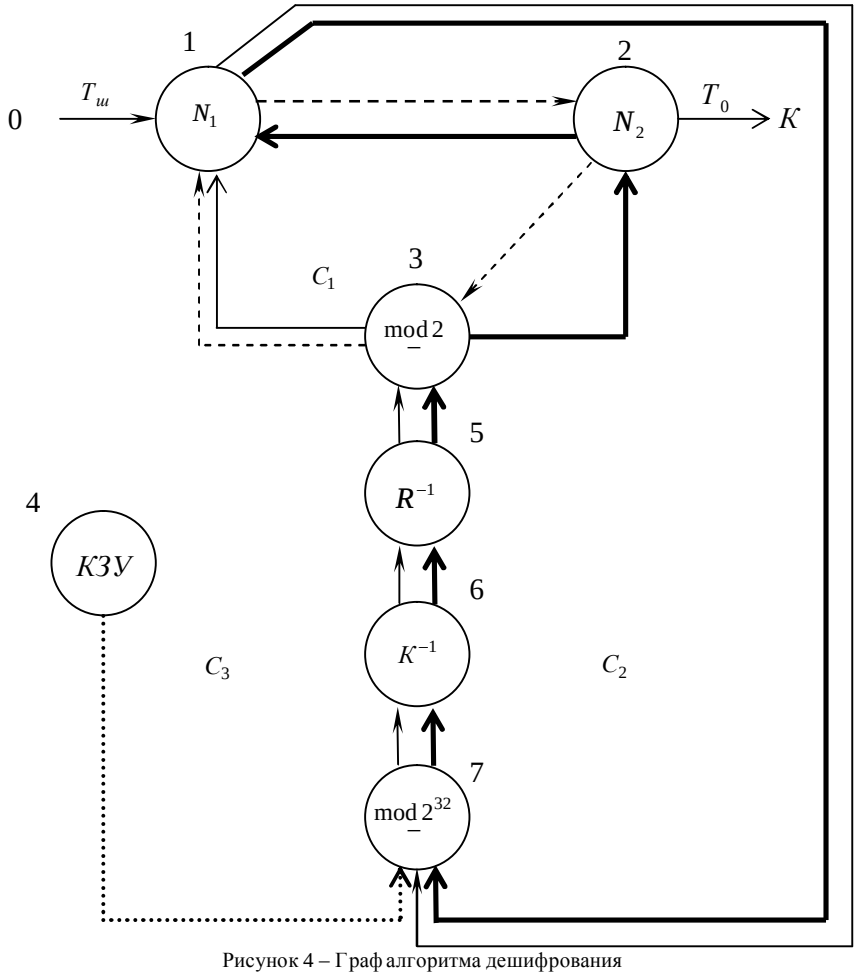

Рисунок 4 – Граф алгоритма дешифрования

Согласно (1) определяем количество повторений циклов:

$$n_{c1} = \frac{1}{1-P_{3,1}} = 10; \quad n_{c2} = \frac{1}{1-P_{2,1}} = 2; \quad n_{c3} = \frac{1}{1-P_{1,7}} = 1{,}1.$$

Определяем по формуле (2) трудоемкости тел каждого цикла, полагается, что в вершинах графа, начинающих цикл, число обращений к операторам $n_i = 10$. Количество операций K_i, порождаемых каждым оператором, выбирается, исходя из того, что при дешифровке криптоаналитику потребуется многократное повторение многих операций, а именно:

$$K_1 = 10,\ K_2 = 10,\ K_3 = 32,\ K_4 = 224,\ K_5 = 1,\ K_6 = 20,\ K_7 = 32.$$

По аналогии с алгоритмом зашифрования получаем следующие значения средней трудоемкости тел циклов:

$\theta_{c1} = n_1K_1 + n_2K_2 + n_3K_3 = 198$ операций;

$\theta_{c2} = n_7K_7 + n_6K_6 + n_5K_5 + n_3K_3 + n_2K_2 + n_1K_1 = 35076$ операций;

$\theta_{c3} = n_4K_4 + n_7K_7 + n_6K_6 + n_5K_5 + n_3K_3 + n_1K_1 = 42142$ операции.

Находим по формуле (3) средние трудоемкостикаждого цикла:

$K_{C1} = n_{C1} \cdot \theta_{C1} = 1980$ операций;

$K_{C2} = n_{C2} \cdot \theta_{C2} = 70152$ операции;

$K_{C3} = n_{C3} \cdot \theta_{C3} = 46356$ операций.

Заменяем циклы графа (рисунок 4) эквивалентными по трудоемкости операторами $K_{C1,}\ K_{C2}$ и K_{C3}. Такой приведенный граф алгоритма дешифрования показан на рисунке 5.

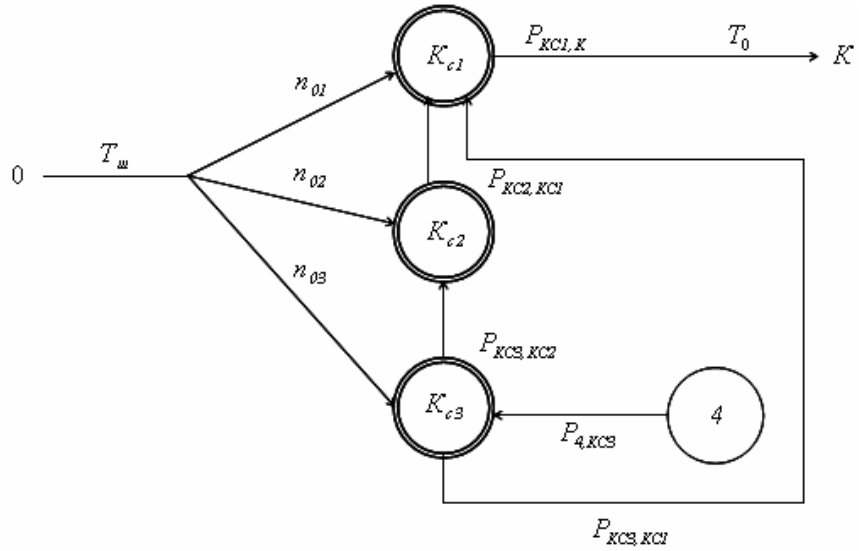

Рисунок 5 – Приведенный граф алгоритма дешифрования

Вероятности переходов между вершинами приведенного графа выбираются следующим образом:

$$P_{KC1,K}=1;\ P_{KC2,KC1}=1;\ P_{KC3,KC2}=0{,}5;\ P_{KC3,KC1}=0{,}5;\ P_{4,KC3}=1.$$

Если считать, как и раньше, что число обращений к операторам, начинающих цикл $n_1=10$, то для вершин приведенного графа имеем $n_{01}=10,\ n_{02}=10,\ n_{03}=10,\ n_{04}=32$. При этом получаем:

$$n_{KC1}=n_{01}\cdot P_{KC1,K}=10;$$

$$n_{KC2}=n_{02}\cdot P_{KC2,KC1}=10;$$

$$n_{KC3}=n_{03}\cdot P_{KC3,KC1}+n_{03}\cdot P_{RC3,KC2}+n_4\cdot P_{4,KC3}=42.$$

Трудоемкость алгоритма дешифрования определяется как:

$$\theta_{\sum деш}=\alpha(n_4\cdot K_4+n_{KC3}\cdot K_{C3}+n_{KC2}\cdot K_{C2}+n_{KC1}\cdot K_{C1}),\qquad (4)$$

где α - числовой коэффициент, учитывающий многократное повторение операций при поиске алгоритма дешифрования.

Подставляя в (4) найденные ранее параметры при α=32, получаем $\theta_{\sum деш}$=85.607680.

Проигрыш криптоаналитика во времени по сравнению с временными затратами шифровальщика составляет

$$p=\frac{\theta_{\sum деш}}{\theta_{\sum заш}}=5237.$$

Таким образом, если для зашифрования открытого текста потребуется 1 минута машинного времени, то для дешифровки криптоаналитику необходимо затратить 5237 минут, т.е. 87 часов или более 3 суток.

Задачами дальнейших исследований в этом направлении могут быть оценки совершенной и практической стойкости шифра с позиции теории игр, что предусматривает наличие конфликтной ситуации между шифровальщиком и криптоаналитиком.

Библиографический список

1. Банкет В.Л. Защита информации в системах телекоммуникации Учеб. пособие для вузов /В.Л. Банкет, Н.В. Захарченко, А.В. Дырда; Под ред. В.Л. Банкета. —Одесса: Изд-во Укр. госуд.акад.связи им. А.С.Попова, 1997. — 95 с.

2. Бертсекас Д. Сети передачи данных / Д. Бертсекас, Р. Галлагер: Пер.с англ. — М.: Мир, 1989. — 544 с.

Поступила в редакцию 01.03.2005 г.