стійкість зазначених шифрів може бути значно менше, ніж стверджують їх розробники. На відміну від підходу до аналізу стійкості, що використовується у попередніх роботах, запропоновано більш прості аналітичні методи, які дозволяють з'ясувати теоретико-кодовий сенс параметрів, що визначають обчислювальну стійкість цих шифрів. Запропоновано один із можливих альтернативних способів (на основі нелінійного випадкового кодування) побудови рандомізованих потокових шифрів із підвищеною стійкістю.
Ключові слова: симетрична криптографія, рандомізоване шифрування, потоковий шифр, випадкове кодування, відвідний канал, задача LPN, кореляційна атака.

Олексійчук Антон Миколайович, доктор технічних наук, професор Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ».
E-mail: alex-dtn@ukr.net.
Алексейчук Антон Николаевич, доктор технических наук, профессор Института специальной связи и защиты информации НТУУ «КПИ».
Alekseychuk Anton, Doctor of Technical Science, Professor of Institute of Special Communication and Information Security of NTUU «KPI».

Гришаков Сергій Володимирович, здобувач Інституту спеціального зв'язку та захисту інформації НТУУ «КПІ».
E-mail: gsv-crypto@mail.ru.
Гришаков Сергей Владимирович, соискатель Института специальной связи и защиты информации НТУУ «КПИ».
Gryshakov Sergey, applicant of Institute of Special Communication and Information Security of NTUU «KPI».

УДК 004.056.2:004.421.5

МЕТОД ФОРМИРОВАНИЯ ИМИТОВСТАВКИ НА ОСНОВЕ ПЕРЕСТАНОВОК

Эмиль Фауре, Валерий Швыдкий, Валентина Щерба

Для построения защищенных телекоммуникационных систем актуальной является задача контроля целостности передаваемых сообщений, который обеспечивается за счет использования процедуры имитозащиты данных. С учетом роста производительности вычислительных средств, а также совершенствования методов взлома систем защиты информации, в том числе защиты от навязывания ложных данных, возрастают требования к стойкости методов и средств имитозащиты. В работе разработана и представлена структурная схема устройства формирования случайной последовательности перестановок. На основе принципов построения данного устройства предложен метод формирования имитовставки и устройство, его реализующее. Сущность метода заключается в том, что в качестве имитовставки используется выбранная в некотором порядке часть символов перестановки большой размерности. Указанная перестановка формируется из последовательности символов сообщения, преобразованных в последовательность взаимосвязанных чисел, представленных в факториальной системе счисления. Для скрытия закона формирования имитовставки используется сменяемый ключ преобразования. Определена стойкость перестановки и сформированной из нее имитовставки при попытке взлома ключа методом «грубой силы».
Ключевые слова: *генератор перестановок, имитозащита, имитовставка, факториальная система счисления, преобразование факториального числа в перестановку, ключ преобразования.*

Введение. Непрерывное совершенствование средств вычислительной техники, их эффективное применение для взлома систем защиты информации приводит к непрерывному процессу совершенствования методов и средств защиты, включая средства и методы имитозащиты [2]. Естественным ответом на непрерывный рост производительности ЭВМ, используемых для взлома систем защиты информации, является требование столь же быстрого роста крипто- и имитостойкости систем защиты. Это обстоятельство обуславливает актуальность разработки новых методов и средств имитозащиты данных с повышенной стойкостью.

Выделение нерешенных задач. Несмотря на несомненные успехи в области разработки технологий повышения стойкости имитозащиты, любые работы, проводимые в этом направлении, представляют значительный интерес. В частности, представляют интерес работы, связанные с разработкой и исследованием новых методов и средств синтеза (случайных) последовательностей перестановок, упрощения алгоритмов их формирования (уменьшение числа и сложности операций, уменьшение объема требуемой памяти и т.п.), в том числе на основе использования факториальной системы счисления [1, 3, 4].

Использование факториальной системы счисления предусматривает представление каж-

дой из $M!$ перестановок (где M – размерность перестановки) точкой отрезка $[0, M!-1]$ числовой оси, по существу, определяющей ее порядковый номер. В соответствии с этим подходом, порядковый номер перестановки в дискретный момент времени n, может быть представлен в виде:

$$B(n)=\sum_{i=0}^{M-1} b_i(n)\cdot w_i, \qquad (1)$$

где $b_i(n)$ – слово (символ), размещенное на i-той позиции, такое, что $0 \le b_i(n) \le i$;

$w_i = i!$ – вес слова, размещенного на i-той позиции.

Для формирования перестановки $P(n)=p_{M-1}(n),\ p_{M-2}(n),...,p_1(n),p_0(n)$ может быть использован синдром перестановки $S_F(n)$ – факториальная запись числа $B(n)$, а именно последовательность факториальных коэффициентов $b_i(n)$ при представлении числа $B(n)$ в факториальной системе счисления:

$$S_F(n)=b_{M-1}(n),b_{M-2}(n),...,b_1(n),b_0(n).$$

Последовательность действий для формирования перестановки может быть записана в виде $B(n)\to S_F(n)\to P(n)$, которая разбивается на две операции: $B(n)\to S_F(n)$ и $S_F(n)\to P(n)$.

Выполнение операции $B(n)\to S_F(n)$ приводит к необходимости обработки чисел очень большой размерности (размерность числа $B(n)$ $r(B(n))=\lceil \lg(M!)\rceil+1$, а при $M>100$ размерность $r(B(n))\ge 158$). В связи с этим, при формировании последовательности перестановок, где модификации подвергаются их номера $B(n)$, целесообразным является произведение операций только над синдромом $S_F(n)$. В соответствии с таким подходом, перестановка в дискретный момент времени «n» может быть сформирована в соответствии с математической моделью

$$\left(S_F(n)=f\left(S_F(n-1)\right)\oplus t_{10}(n)\right)\to P(n), \qquad (2)$$

где $f(S(n-1))$ – функция модификации синдрома (некоторая функция от синдрома в предыдущий «n-1» момент времени);

$t_{10}(n)$ – случайное число, представленное в десятичной системе счисления и обозначающее смещение порядкового номера формируемой перестановки относительно порядкового номера предшествующей перестановки.

В выражении (2) символ $\oplus$ обозначает сложение чисел различных систем счисления – факториальной $(S_F(n-1))$ и десятичной $(t_{10}(n))$.

Постановка задачи. Задачей исследования является разработка метода формирования имитовставки на основе использования перестановок, обладающего высокой эффективностью и стойкостью к взлому, а также устройства для его реализации.

Требования, предъявляемые к методу формирования имитовставки:

– метод формирования имитовставки должен обладать свойством рассеивания, т.е. каждый символ сообщения, с учетом его позиции в нем, должен оказывать влияние на формирование имитовставки;

– метод формирования имитовставки должен обеспечивать минимальный уровень коллизий – ситуаций, при которых имитовставки различных сообщений совпадают. Подобное свойство обеспечивается, когда все значения имитовставки (из полного множества возможных) встречаются с равными вероятностями и не зависят от сообщения или ключа преобразования по отдельности;

– длина имитовставки для любого количества символов сообщения должна быть фиксированной и постоянной;

– должно обеспечиваться отсутствие корреляции между имитовставками, вычисленными по целому сообщению и его части;

– имитовставка должна быть невоспроизводимой без знания ключа преобразования.

Решение задачи. Прежде всего, рассмотрим подходы к созданию технических средств, реализующих метод синтеза воспроизводимой непредсказуемой последовательности перестановок в соответствии с выражением (2).

В качестве аппаратной платформы реализации генератора перестановок будем рассматривать однокристальные ЭВМ (микропроцессоры) или персональные ЭВМ (при программной реализации генератора). Упрощенная структурная схема устройства формирования перестановок приведена на рис. 1.

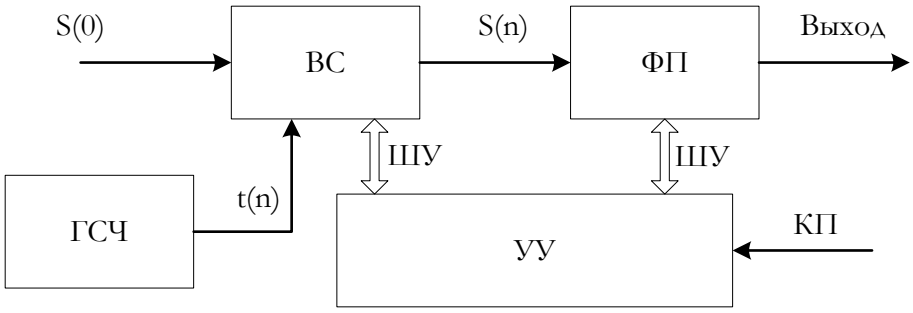

Рис. 1. Структурная схема устройства формирования перестановок

На рис. 1 приняты следующие обозначения: ВС – блок вычисления синдрома; ФП – блок формирования перестановки; УУ – устройство (процессор) управления; ГСЧ – генератор случайных чисел; КП – ключ преобразования.

При пуске устройства формирования перестановок в блок вычисления синдрома ВС загружается некоторый вектор начальной загрузки – синдром $S_F(0)$ и некоторое случайное число $t_{10}(1)$, по которым вычисляется синдром первой перестановки $S_F(1)$.

Полученный синдром поступает на вход блока формирования перестановки, в который при пуске вводится ключ преобразования (КП).

Преобразование синдрома в перестановку.

Блок формирования перестановки содержит ОЗУ, в которое по адресам 0, 1, 2, …, (*M*-2), (*M*-1) записывается ключевая последовательность – одна из *M*! возможных перестановок слов отрезка $[0, M-1]$, которая держится в секрете.

Пусть имеется синдром $S_F(n) = b_{M-1}(n), b_{M-2}(n), ..., b_1(n), b_0(n)$.

На *k*-ом шаге формирования перестановки (при вычислении *k*-ого символа перестановки) выполняются следующие действия:

1. выбирается *k*-ое слово синдрома b_{M-k};
2. из ОЗУ считывается слово по адресу b_{M-k}. Это слово является *k*-ым символом формируемой перестановки, т.е $p_k = R(b_{M-k})$ ($R(i)$ – содержимое ячейки ОЗУ по *i*-му адресу);
3. извлеченное слово удаляется из ОЗУ, а все остальные слова переписываются в соответствии со следующим правилом:

$$R_i \leftarrow R_i \text{ для } 0 \le i \le b_{M-k} - 1;$$
$$R_i \leftarrow R_{i+1} \text{ для } b_{M-k} \le i \le M - k - 1.$$

Формирователь перестановки, соответствующий модели лототрона, формирует перестановку $P(n)$ и выводит ее потребителю. Все последующие перестановки формируются аналогичным образом с учетом смены синдрома $S_F(n-1)$ и числа $t_{10}(n)$.

Дополнительным элементом ключа преобразования является ключ модификации синдрома, использующийся в процессе вычислении функции модификации синдрома $f(S_F(n-1))$ для формирования последующего синдрома.

Функция модификации синдрома. Функция модификации синдрома $f(S_F(n-1))$ может быть реализована, например, одним из двух способов:

1) путем выполнения перестановки символов предыдущей перестановки $P(n-1)$ по держащемуся в секрете ключу модификации синдрома с последующим преобразованием ее в синдром. В этом случае функция модификации синдрома $f(S_F(n-1))$ вырождается в функцию модификации перестановки $f(P(n-1))$, а процедура формирования перестановки может быть обозначена так: $(S_F(n) = f(P(n-1)) \oplus t_{10}(n)) \to P(n)$;

2) путем выполнения операции $(b_i \leftarrow (b_i + z_i) \bmod i)$ для каждого факториального коэффициента синдрома b_i и всех $i \in [0, M-1]$, где z_i – *i*-ый символ хранящегося в секрете ключа модификации синдрома $Z = z_{M-1}, z_{M-2}, ..., z_1, z_0$.

Стойкость генератора перестановок. Криптографическая стойкость генератора последовательности перестановок определяется следующими скрываемыми параметрами, образующими ключ преобразования:

– вектор начальной загрузки $S_F(0)$ с мощностью ключевого пространства *M*!;

– ключ преобразования синдрома в перестановку с мощностью ключевого пространства *M*!;

– ключ модификации синдрома с мощностью ключевого пространства *M*!.

Предложенное устройство формирования некоррелированной последовательности перестановок может быть использовано для решения

множества практических задач. Одна из таких задач – задача формирования имитовставки.

Устройство формирования имитовставки. Для выработки имитовставки может быть использован метод, реализованный в устройстве формирования последовательности перестановок, показанном на рис. 1. Для пояснения сущности метода формирования имитовставки незначительно изменим схему рис. 1 и приведем ее на рис. 2.

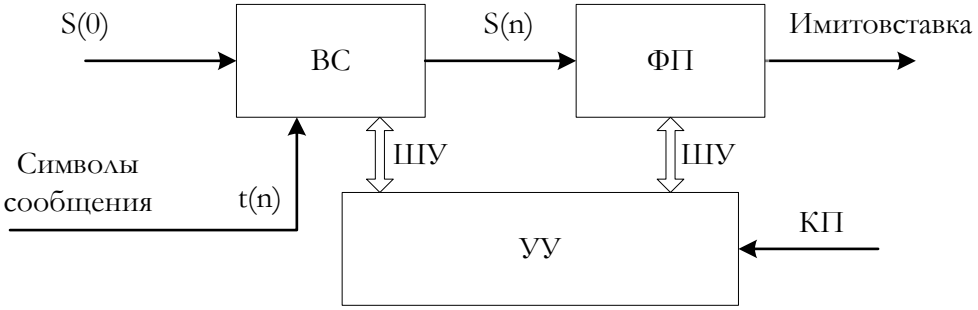

Рис. 2. Структурная схема устройства формирования имитовставки

Из рис. 2 следует, что устройство формирования имитовставки имеет структуру, подобную структуре устройства формирования перестановок, и, следовательно, формирование имитовставки может быть одним из режимов его работы.

Отметим, что режим выработки имитовставки характеризуется тем, что:

– работа ведется по секретному ключу;

– последовательность $t_{10}(n)$ образуют символы сообщения;

– имитовставка выводится потребителю однократно по окончании сообщения.

Для примера рассмотрим случай формирования имитовставки в персональном компьютере.

Известно, что в ПЭВМ каждый из символов (с которыми оперирует пользователь, работая с клавиатурой) кодируется комбинацией из 8 бит. Это значит, что мощность алфавита источника $M = 256$, а мощность множества перестановок $M! = 256! = 8{,}57\text{x}10^{506}$.

Все слова синдрома и все слова перестановки являются 8-битовыми словами.

Вектор начальной загрузки и ключ преобразования синдрома в перестановку (а также ключ модификации синдрома) содержат по 256 слов (по 8 бит каждый) и держатся в секрете. Первое слово сообщения и вектор начальной загрузки инициируют вычисление первого синдрома $S_F(1)$. Все последующие синдромы формируются на основе предшествующего. Так, синдром $S_F(1)$ и второй символ сообщения инициируют вычисление второго синдрома $S_F(2)$, при этом вычисление синдрома $S_F(2)$ производится с учетом модификации синдрома $S_F(1)$ в соответствии с секретным ключом модификации, чем и обеспечивается выполнение процедуры (2).

Так продолжается до момента завершения процесса формирования последнего синдрома, для которого по секретному ключу формируется перестановка.

В качестве имитовставки может быть использована группа k слов из 256 слов сформированной перестановки. Заметим, что использование k слов из M возможных в имитовставке увеличивает число коллизий за счет уменьшения числа возможных значений имитовставки со значения $M!$ до значения $\prod_{i=0}^{k-1}(M-i) = \frac{M!}{(M-k)!}$. Отметим также, что порядок выбора k слов (из M слов перестановки) держится в секрете.

Таким образом, ключом выработки имитовставки является:

– последовательность из $M = 256$ слов вектора начальной загрузки;

– последовательность из $M = 256$ слов ключа преобразования синдрома в перестановку;

– последовательность из $M = 256$ слов ключа модификации синдрома;

– последовательность из k слов, указывающих на номера выбираемых символов перестановки.

При выработке имитовставки существенным является достижение эффекта рассеивания за счет сцепления синдромов (взаимосвязи формируемого синдрома со всеми предшествующими словами сообщения). Сцепление синдромов достигается за счет обратной связи (связи выхода формирователя синдрома с его входом). Поэтому при попытке модификации текста сообщения происходит изменение всех последующих синдромов, начиная с

места модификации текста, и, как следствие, – изменение имитовставки в целом.

Заметим, что, в отличие от генератора перестановок, для формирования имитовставки не представляется возможным использование процедуры вида $S_F(n)=S_F(n-1)\oplus t_{10}(n)$ без предварительной модификации синдрома $S_F(n-1)$ в момент времени «n–1». Это связано с тем, что при использовании такой процедуры на одном и том же ключе преобразования (состоящем из вектора начальной загрузки, ключа преобразования синдрома в перестановку, а также последовательности из k слов, указывающих на номера выбираемых символов перестановки) имитовставки, вычисленные по двум сообщениям, состоящих из одинаковых символов и отличающихся только порядком их следования, совпадут. Поэтому обязательным является модификация синдрома $S_F(n-1)$, а формирование имитовставки должно выполняться с помощью процедуры $S_F(n)=f\left(S_F(n-1)\right)\oplus t_{10}(n)$, где $f\left(S_F(n-1)\right)\neq S_F(n-1)$, или, с учетом предложенной функции модификации синдрома, с помощью процедуры $S_F(n)=f\left(P(n-1)\right)\oplus t_{10}(n)$.

Оценка имитостойкости. Определим имитостойкость описанного метода выработки имитовставки как время, необходимое для его взлома методом «грубой силы». Будем считать, что криптоаналитик располагает:

– текстом сообщения и имитовставкой, выработанной по этому тексту;

– знанием (во всех деталях) алгоритма формирования имитовставки.

Это значит, что криптоаналитик знает число слов в сообщении, все значения параметра $t_{10}(n)$, число символов имитовставки k.

Чего не знает криптоаналитик:

– вектора начальной загрузки $S_F(0)$;

– ключа преобразования синдрома в перестановку;

– ключа модификации синдрома;

– правила выбора k символов имитовставки из M возможных.

Заметим, что вектор начальной загрузки, ключ преобразования синдрома в перестановку и ключ модификации синдрома являются последовательностями из M символов каждая. Это значит, что полная длина ключа выработки имитовставки равняется

$$l_{кл}=3M+k.$$

Будем считать, что имитозащита будет взломана, если криптоаналитик по имеющимся сообщениям и соответствующим им имитовставкам простым перебором всех возможных значений вектора начальной загрузки, ключа преобразования синдрома в перестановку, ключа модификации синдрома и всех сочетаний выбора k символов имитовставки сумеет подобрать ключ формирования имитовставки. Вероятность этих событий (обозначим их p_1, p_2, p_3, p_4) определится так: $p_1=p_2=p_3=(M!)^{-1}$, $p_4=(C_M^k)^{-1}$. Учитывая статистическую независимость каждого из этих событий, вероятность взлома имитовставки будет равна

$$p_0=p_1p_2p_3p_4=\left(M!\right)^{-3}\cdot\left(C_M^k\right)^{-1}.$$

Отсюда следует, что имитостойкость будет тем выше, чем больше M и чем ближе k к значению $0.5\cdot M$.

Зная вероятность взлома, можно определить среднее требуемое число попыток взлома таким образом:

$$N=0.5\cdot p_0^{-1}=0.5\cdot\left(M!\right)^3\cdot C_M^k.$$

Для определения времени взлома будем исходить из следующих предпосылок:

– производительность современных компьютеров порядка 10^{10} операций/сек;

– вычисление имитовставки требует не менее 1000 машинных операций;

– для взлома можно привлечь машинную группировку из 1000 компьютеров;

– год содержит 8760 часов, а час – 3600 сек.

Тогда такая компьютерная группировка за один год может выполнить $3{,}15\cdot10^{17}$ вычислений имитовставки, а за миллион лет $3{,}15\cdot10^{23}$ имитовставок. Отсюда имитостойкость (млн. лет) будет равна

$$T=\frac{0.5\cdot\left(M!\right)^3\cdot C_M^k}{3.15\cdot10^{23}}.$$

В частности для $M=256$ и $M!=8{,}57\text{x}10^{506}$ получим $T=\frac{0.5\cdot\left(M!\right)^3\cdot C_M^k}{3.15\cdot10^{23}}\approx C_M^k\cdot10^{1497}$ млн. лет.

Заметим, что если $f\left(S_F(n-1)\right)=S_F(n-1)$, имитостойкость составит

$$T=\frac{0.5\cdot\left(M!\right)^2\cdot C_M^k}{3.15\cdot10^{23}}.$$

Для обозначенных выше параметров $T=\frac{0.5\cdot\left(256!\right)^2\cdot C_M^k}{3.15\cdot10^{23}}\approx C_M^k\cdot10^{990}$ млн. лет.

Отсюда следует, что если не выполнять модификацию синдрома и не держать в секрете правило выбора k символов имитовставки (положить $C_M^k = 1$), имитостойкость составит 10^{990} млн. лет.

Заметим, что имитостойкость в первую очередь определяется размерностью перестановки и именно ее необходимо определить для заданной стойкости.

Изложенный алгоритм оценки имитостойкости может быть применен для оценки стойкости последовательности перестановок (стойкости генератора перестановок). Отличие состоит лишь в том, что криптоаналитик по имеющейся в его распоряжении последовательности перестановок подбирает вектор начальной загрузки, ключ преобразования синдрома в перестановку и ключ модификации синдрома. Все остальные параметры в секрете не держатся.

С учетом изложенного, стойкость генератора определится таким образом:

$$T = \frac{0.5 \cdot (M!)^3}{3.15 \cdot 10^{23}}.$$

При тех же параметрах получим $3.15 \cdot 10^{23} \cdot T = 0.5 \cdot (M!)^3$, откуда

$$M! \approx 8.7 \cdot 10^7 \cdot \sqrt[3]{T}.$$

Отсюда следует, что для обеспечения стойкости не менее, например, 10 млн. лет размерность перестановки $M \geq 12$.

При использовании режима формирования перестановок без модификации синдрома $M! \approx 7.9 \cdot 10^{11} \cdot \sqrt{T}$, для обеспечения стойкости не менее 10 млн. лет размерность перестановки составит $M \geq 16$.

Выводы. Выполненное исследование позволяет сформулировать следующие выводы:

– разработана структурная схема устройства формирования последовательности перестановок на основе использования факториальной системы счисления, позволяющая создать генератор перестановок в аппаратном или программном виде;

– определено, что длина ключа для формирования воспроизводимой случайной последовательности перестановок равняется $3M$, а теоретическая стойкость последовательности перестановок к взлому методом «грубой силы» составляет десятки миллионов лет при размерности перестановки $M \geq 12$;

– разработан метод формирования имитовставки, основанный на использовании перестановок и представлении синдрома формируемой перестановки в позиционной системе счисления с факториальным основанием, который за счет использования операции суммирования значения каждого символа сообщения с модифицированным синдромом перестановки на предыдущем этапе, а также формировании в соответствии с секретным ключом после обработки последнего символа сообщения перестановки и выборе из нее определенных секретным ключом символов, позволяет формировать имитовставку сообщения произвольной длины, обладающую высокой стойкостью к взлому, а также всеми свойствами, определенными в постановке задачи;

– определено, что длина ключа для формирования имитовставки равняется $3M + k$, где M – размерность перестановки, k – количество символов в имитовставке; размерность ключевого пространства составляет $(M!)^3 \cdot C_M^k$, что определяет высокую имитостойкость разработанного метода к взлому методом «грубой силы»;

– разработана структурная схема устройства формирования имитовставки на основе разработанного метода, позволяющая его реализовывать в аппаратном или программном виде.

ЛИТЕРАТУРА

[1]. Борисенко О.А. Електронна система генерації перестановок на базі факторіальних чисел / О.А. Борисенко, І.А. Кулик, О.Є. Горячев // Вісник СумДУ. Технічні науки. – 2007. – №1. – С. 183-188.

[2]. Диффи У. Защищенность и имитостойкость: введение в криптографию / У. Диффи, М. Хелльман // ТИИЭР. – 1979. – т.67., №3. – С. 71-109.

[3]. Кнут Дональд Э. Искусство программирования. В 7 т. Т.4. Выпуск 2. Генерация всех кортежей и перестановок. / Дональд Эрвин Кнут, Станфордский университет ; пер.с англ. Ю.Г. Гордиенко. – М.: ООО «И.Д. Вильямс», 2008. – 160 с.

[4]. Рейнгольд Э. Комбинаторные алгоритмы. Теория и практика / Э. Рейнгольд, Ю. Нивергельт, Н. Део; пер. с англ. Е.П. Липатова; под ред. В.Б. Алексеева. – М.: Мир, 1980. – 476 с.

REFERENCES

[1]. Borisenko, O.A., Kulik, I.A. and Goryachev O.E. (2007) 'Electronic System for Permutations Generating Based upon Factorial Numbers', *The Visnyk of the SSU. Technical sciences*, No.1, pp. 183-188.

[2]. W. Diffie and M. E. Hellman (1979) 'Privacy and Authentication: An Introduction to Cryptography', *Proceedings of the IEEE*, Vol. 67, No.3, March, pp. 71-109.

[3]. Donald E. Knuth (2008) *Art of Computer Programming, Volume 4, Fascicle 2, Generating All Tuples and Permutations*, Moscow: Williams Publishing House.

[4]. Reingold, E.M., Nievergelt, J. and Deo N. (ed.) (1980) *Combinatorial Algorithms: Theory and Practice*, Moscow: Mir.

МЕТОД ФОРМУВАННЯ ІМІТОВСТАВКИ НА ОСНОВІ ПЕРЕСТАНОВОК

Для побудови захищених телекомунікаційних систем актуальною є задача контролю цілісності переданих повідомлень, який забезпечується за рахунок використання процедури імітозахисту даних. З урахуванням зростання продуктивності обчислювальних засобів, а також вдосконалення методів злому систем захисту інформації, у тому числі захисту від нав'язування хибних даних, зростають вимоги до стійкості методів і засобів імітозахисту. У роботі розроблена і представлена структурна схема пристрою формування випадкової послідовності перестановок. На основі принципів побудови цього пристрою запропоновано метод формування імітовставки та пристрій, що його реалізує. Сутність методу полягає в тому, що в якості імітовставки використовується обрана в деякому порядку частина символів перестановки великої розмірності. Зазначена перестановка формується з послідовності символів повідомлення, перетворених в послідовність взаємопов'язаних чисел, представлених у факторіальній системі числення. Для приховування закону формування імітовставки використовується змінюваний ключ перетворення. Визначено стійкість перестановки і сформованої з неї імітовставки у випадку злому ключа методом «грубої сили».

Ключові слова: генератор перестановок, імітозахист, імітовставка, факторіальна система числення, перетворення факторіального числа в перестановку, ключ перетворення.

METHOD OF MESSAGE AUTHENTICATION CODE FORMATION BASED ON PERMUTATIONS

The task of controlling the integrity of transmitted messages which is provided by the use of message authentication is relevant for constructing of protected telecommunications systems. Given the growth of computing means productivity, and improving the methods of hacking of information protection systems including protection against false data imposing requirements for message authentication methods and means increase. In this paper the structural diagram of device of random permutations sequence formation is developed and shown. On the basis of this device construction principles the method and device of message authentication code formation is proposed. The essence of the method lies in the fact that as a message authentication code is used a part of large dimension permutation symbols in some chosen order. This permutation is formed from the sequence of characters of the message converted into a sequence of related numbers in factorial number system. To hide the law of formation of message authentication code a replaceable transformation key is used. The resistance of permutation and message authentication code generated from it when trying to break a key by "brute force" is determined.

Keywords: generator of permutations, message authentication, message authentication code, factorial number system, transformation of factorial number into permutation, transformation key.

Фауре Эмиль Витальевич, кандидат технических наук, доцент, докторант кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета.
E-mail: faureemil@gmail.com.
Фауре Еміль Віталійович, кандидат технічних наук, доцент, докторант кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету.
Faure Emil, PhD, Associate Professor, doctoral student of Department of Information Security and Computer Engineering of Cherkasy State Technological University.

Швыдкий Валерий Васильевич, кандидат технических наук, доцент, доцент кафедры информационной безопасности и компьютерной инженерии Черкасского государственного технологического университета.
E-mail: vvshv@uch.net
Швидкий Валерій Васильович, кандидат технічних наук, доцент, доцент кафедри інформаційної безпеки та комп'ютерної інженерії Черкаського державного технологічного університету.
Shvydkii Valerii, PhD, Associate Professor, Associate Professor of Department of Information Security and Computer Engineering of Cherkasy State Technological University.

Щерба Валентина Александровна, старший преподаватель кафедры прикладной математики Черкасского государственного технологического университета.
E-mail: shcherba_anatoly@mail.ru
Щерба Валентина Олександрівна, старший викладач кафедри прикладної математики Черкаського державного технологічного університету.
Shcherba Valentina, senior Lecturer of Department of Applied Mathematics of Cherkasy State Technological University.