РЕФЕРАТ

Магистерская аттестационная работа содержит 75 страниц, 7 рисунков, 16 таблиц, 57 формул, 28 источников, 4 приложения.

В данной работе рассмотрены методы формирования нелинейных узлов замен, широко используемых в блочных симметричных шифрах. Актуальной задачей является совершенствование симметричных средств защиты информации путем разработки новых подходов и способов построения нелинейных узлов замен с улучшенными свойствами.

Объект исследования — процесс построения нелинейных узлов замен блочных симметричных шифров.

Предмет исследования — метод имитации отжига для построения нелинейных узлов замен блочных симметричных шифров.

Цель — повышение криптографических свойств формируемых нелинейных узлов замен на основе совершенствования метода имитации отжига.

НЕЛИНЕЙНЫЙ УЗЕЛ ЗАМЕН, НЕЛИНЕЙНОСТЬ, АВТОКОРРЕЛЯЦИЯ, S-BOX, ВЕСОВЫЕ КОЭФФИЦИЕНТЫ, МЕТОД ИМИТАЦИИ ОТЖИГА

ABSTRACT

Master's thesis includes 75 pages, 7 pictures, 16 tables, 57 formulas, 28 sources, 4 appendixes.

In this work considered the methods for S-box construction, that are widely used in block symmetric ciphers. The urgent task is to improve the symmetric information security tools through the development new approaches and methods constructing S-boxes with improved properties.

Research object is the process of building S-boxes for block symmetric ciphers.

Research subject is the method of simulating annealing for S-box building for block symmetric ciphers.

The object is the enchancement of cryptographic properties of built S-boxes that are based on elaboration the simulation annealing method.

S-BOX, NONLINEARITY, AUTOCORRELATION, WEIGHT COEFFICIENTS, SIMULATED ANNEALING METHOD

РЕФЕРАТ

Магістерська атестаційна робота містить 75 сторінок, 7 рисунків, 16 таблиць, 57 формул, 28 джерел, 4 додатки.

В даній роботі розгянуто методи формування нелінійних вузлів замін, які широко використовуются у блочних симетричних шифрах. Актуальнім завданням є вдосконалення симетричних засобів інформаційної безпеки шляхом розробки нових методів та способів формування нелінійних вузлів замін з покращенними властивостями.

Об'єкт дослідження — процес побудови нелінійних вузлів замін блочних симетричних шифрів.

Предмет дослідження — метод імітації відпалу для побудови нелінійних вузлів замін блочних симетричних шифрів.

Мета — підвищення криптографічних властивостей нелінійних вузлів замін заснованих на вдосконаленні методу імітації відпалу.

НЕЛІНІЙНІ ВУЗЛИ ЗАМІН, НЕЛІНІЙНІСТЬ, АВТОКОРЕЛЯЦІЯ, S-BOX, ВАГОВІ КОЕФІЦІЄНТИ, МЕТОД ІМІТУВАННЯ ВІДПАЛУ

СОДЕРЖАНИЕ

СПИСОК СОКРАЩЕНИЙ, УСЛОВНЫХ ОБОЗНАЧЕНИЙ, СИМВОЛОВ, ЕДИНИЦ И ТЕРМИНОВ

AC — автокорреляция.

Cost функция — ценовая функция

NL — нелинейность.

S-box, S-блок — нелинейный узел замен.

WHT — преобразование Уолша-Адамара.

БСШ — блочный симметричный шифр.

ВВЕДЕНИЕ

Нелинейные узлы замен (S-блоки) являются ключевым элементом современных симметричных криптографических алгоритмов, среди которых наиболее известными являются стандарты блочного симметричного шифрования DES, ГОСТ-28147-89 и AES.

S-блок nxm представляет собой нелинейную функцию отображения n входных бит в m выходных. В случае, когда на выходе S-блока появляются все возможные m-битные значения и каждое выходное значение равновероятно, S-блок называют регулярным, что является обязательным условием для его использования в современных БСШ. Кроме того, для обеспечения устойчивости БСШ к атакам дифференциального и линейного криптоанализа используемые узлы замен должны удовлетворять требуемым показателям нелинейности и автокорреляции.

Вычислительным методам синтеза криптографически стойких регулярных узлов замен посвящено множество работ. Однако, как показал проведенный анализ, показатели формируемых S-блоков далеки от оптимальных, с увеличением их размерности некоторые методы становятся вычислительно нереализуемыми. Перспективным направлением исследований является использование математического аппарата недвоичных криптографических функций, что, как показано в данной работе, позволяет синтезировать регулярные нелинейные узлы замен с требуемыми показателями нелинейности и автокорреляции.

В данной работе исследуются новые критерии вычислительного поиска криптографически стойких S-блоков. На основе усовершенствованных весовых коэффициентов ценовых функций поиска предлагается дальнейшее развитие метода имитации отжига.

В разделе ”Охрана труда и безопасность в чрезвычайных ситуациях” будут исследованы вопросы условий труда, безопасности, производственной санитарии и пожарной безопасности в помещении научно-исследовательской лаборатории. Также будет произведён расчёт необходимой площади световых проёмов в помещении научно-исследовательской лаборатории.

1 КРИТЕРИИ И ПОКАЗАТЕЛИ СТОЙКОСТИ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ

Основным и наиболее эффективным механизмом криптографической защиты информации являются методы блочного симметричного криптографического преобразования. Наряду с высокой скоростью преобразований и простотой практической реализации симметричные криптоалгоритмы позволяют обеспечить высокую стойкость к различным методам криптографического анализа.

Основным элементом современных блочных симметричных криптографических средств защиты информации являются нелинейные узлы замен (нелинейные блоки подстановок), качество построения которых непосредственновлияет на эффективность разрабатываемых механизмов обеспечения безопасности информационных технологий.

На сегодняшний день в Украине нет национального алгоритма блочного симметричного криптографического преобразования информации. Правила формирования нелинейных узлов замен ныне действующего стандарта ГОСТ 28147-89 являются государственной тайной Российской Федерации и не доступны для использования в Украине. В этом смысле разработка математической модели и вычислительного метода формирования нелинейных узлов замен с высокими показателями стойкости является актуальной научно-технической задачей, непосредственно связанной с выполнением ряда важных государственных программ Украины и проводимым в недавнее время открытым конкурсом симметричных криптографических алгоритмов.

Нелинейные узлы замен блочных симметричных криптографических средств защиты информации эффективно описываются в математическом виде совокупностью криптографических булевых функций и накладываемой системой ограничений на отдельные показатели стойкости. Таким образом, использование математического аппарата булевой алгебры позволяет получить абстрактное аналитическое описание нелинейных узлов замен и адекватно оценивать их стойкость.

В данном разделе исследуется структура и основные функциональные

элементы алгоритмов блочного симметричного криптографического преобразования информации, обосновываются требования к перспективным методам блочного симметричного криптографического преобразования, исследуется математический аппарат булевой алгебры для построения нелинейных узлов замен блочных симметричных криптопреобразований, проводится анализ различных подходов к построению нелинейных узлов замен, исследуются основные показатели стойкости нелинейных узлов замен современных блочных симметричных шифров.

1.1 Сравнительный анализ методов блочного симметричного криптографического преобразования информации

Для защиты информации с ограниченным доступом в современных информационных системах применяются различные криптографические средства. Основным и наиболее эффективным механизмом криптографической защиты информации являются методы блочного симметричного криптографического преобразования. Наряду с высокой скоростью преобразований и простотой практической реализации симметричные криптоалгоритмы позволяют обеспечить высокую стойкость к различным методам криптографического анализа. Проведем анализ и сравнительное исследование методов блочного симметричного криптографического преобразования информации.

Как показывает анализ открытой литературы и результаты проводимых криптографических конкурсов, на сегодняшний день реализовано большое число различных блочных симметричных методов преобразования информации. При этом подавляющее большинство методов делится на две большие группы:

— методы, построенные на основе использования цепей Фейстеля;

— методы, построенные на основе чередования процедур перестановок и подстановок, т.н. SP-конструкций.

Приведём основные определения и обозначения блочных симметричных шифров и схем их построения.

Пусть T и K — пространства текстов и ключей соответственно

блочного симметричного шифра.

$$C = \{C_k : T \to T : k \in K\} \tag{1.1}$$

Пусть $r > 0$ — положительное целое и пусть $K_1, K_2, \ldots, K_r$ — r конечных множеств. Говорят, что C — r-раундовый итеративный блочный симметричный шифр (БСШ), если он может быть записан в виде:

$$C_k = R_{k_r}^{(r)} \circ R_{k_{r-1}}^{(r-1)} \circ \ldots \circ R_{k_1}^{1} \tag{1.2}$$

для всех $k \in K$, где

$$R^{(i)} = \{R_{k_i}^{(i)} : T \to T : k_i \in K_i\} \tag{1.3}$$

называется i-м раундом C.

Обычно i-й раунд блочного симметричного шифра состоит из трех слоев: слоя подстановочного преобразования с использованием нелинейных блоков замен или S-блоков, слоя линейного перестановочного преобразования и слоя функциональных преобразований, таких как сдвиг, сложение по модулю с ключом и пр.

Такой итеративный подстановочно-перестановочный подход к разработке стойких симметричных шифров был основан К. Шенноном и использует два общих принципа построения: перемешивание (confusion) и рассеивание (diffusion). Перемешивание осуществляет распространение влияния одного знака открытого текста на множество символов шифртекста, что обуславливает лавинный эффект (в случае блочных шифров — обеспечение распространения влияния каждого бита входного текста на все биты выходного текста). Рассеиванием называется шифрующее преобразование, нарушающее взаимосвязи статистических характеристик входного и выходного текста, т.е. маскировку статистических свойств исходного сообщения.

Ключи $k_1, k_2, \ldots, k_r$ называются раундовыми ключами блочного симметричного шифра и производятся из одного основного секретного ключа k посредством детерминистического алгоритма, называемого

алгоритмом распределения ключей.

Схема Фейстеля (см. рис. 1.1) является структурой, которая позволяет построить перестановку для $2n$-битных последовательностей, основываясь на функциях от n-битных последовательностей. Обозначим схему Фейстеля с $r > 0$ раундами преобразования, основанных на функциях $f_1, f_2, \ldots, f_r : \{0,1\}^n \to \{0,1\}^n$ как $\Phi(f_1, f_2, \ldots, f_r)$. Легко заметить, что $\Phi(f_1, f_2, \ldots, f_r)$ обратима, т.к.

$$\Phi^{-1}(f_1, f_2, \ldots, f_r) = \Phi(f_r, f_{r-1}, \ldots, f_1). \tag{1.4}$$

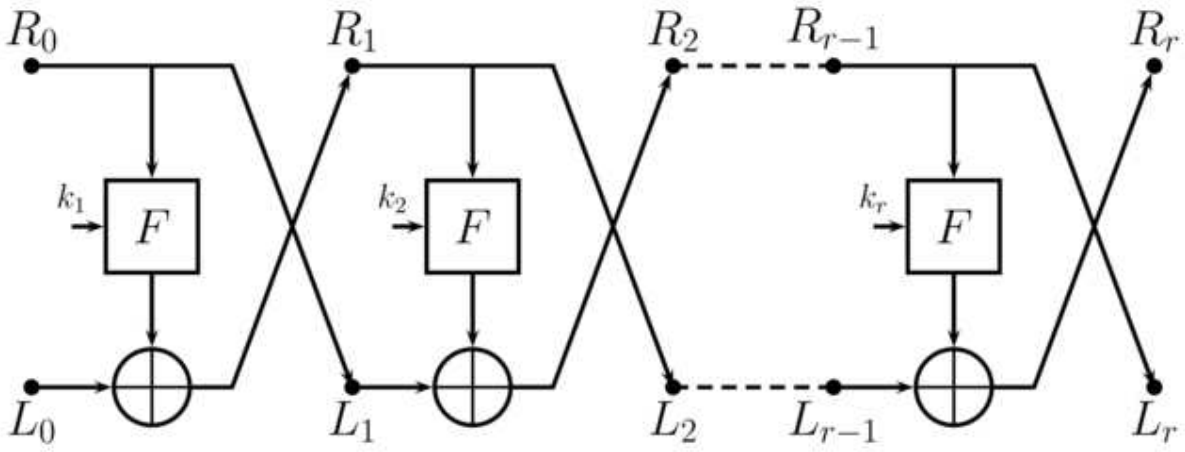

Рисунок 1.1 – r–раундовая схема Фейстеля $\Phi(f_1, f_2, \ldots, f_r)$

Подстановочно-перестановочная структура (SP-структура, Substitution Permutation) наиболее близка к принципам построения К. Шеннона и состоит из последовательности слоев, в которых подстановочный слой осуществляет перемешивание, за которым следует перестановочный слой, осуществляющий рассеивание. SP-схема проиллюстрирована на рисунке 1.2.

Все преобразования в SP-конструкциях должны быть обратимыми, так как расшифрование производится путем выполнения обратных преобразований в обратном порядке.

Оба вида конструкций имеют свои достоинства и недостатки. Так, преимуществом конструкции Фейстеля в сравнении с SP-конструкцией является значительное облегчение практической реализации на процес-

сорах малой разрядности, поскольку обрабатываемые итеративной процедурой данные разбиваются на 2 блока и обработка криптопримитивами производится над подблоками. Другим преимуществом является то, что конструкция Фейстеля позволяет использовать в шифрующей функции более широкий набор преобразований, так как к ним не предъявляется требование обратимости.

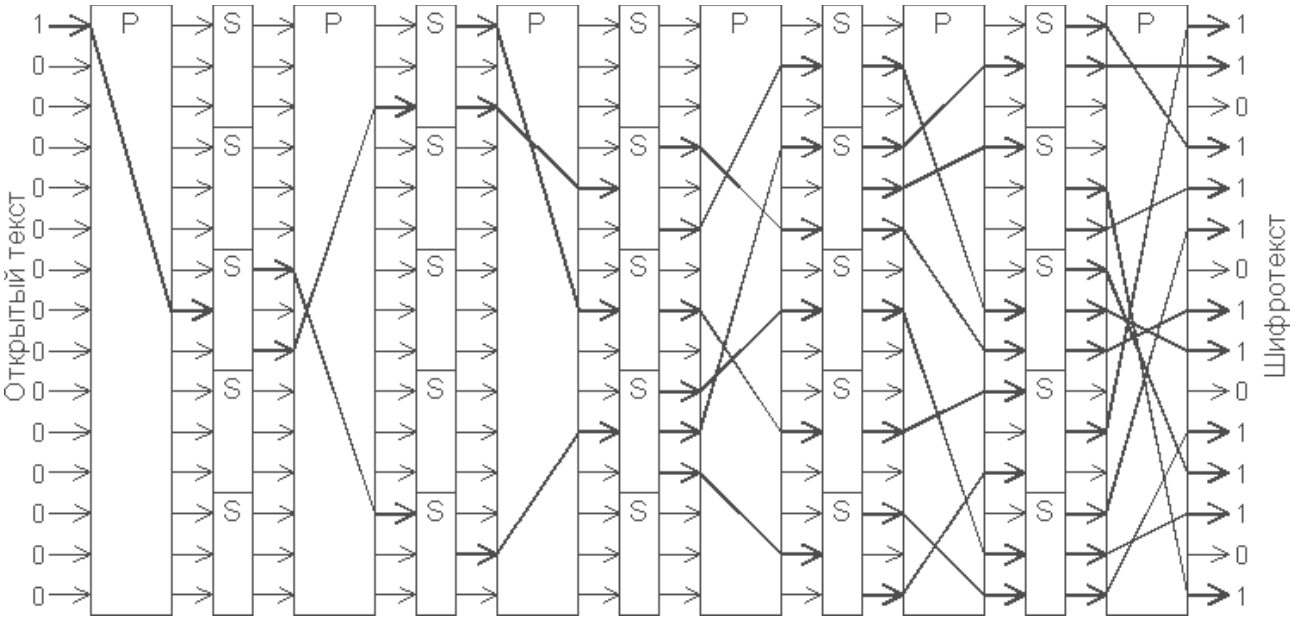

Рисунок 1.2 – SP-схема

В то же время блоки подстановок и перестановок, применяемые в конструкциях Фейстеля, имеют небольшой размер. Размерность же блоков нелинейного подстановочного и линейного перестановочного преобразования в SP-конструкциях значительно больше, что приводит к усилению устойчивости к различным методам криптоанализа. Другим преимуществом SP структуры является ее большая прозрачность и приближенность к принципам построения стойких симметричных шифров К. Шеннона.

В соответствии с приведенными определениями и обозначениями, ниже приведены результаты проведенного анализа современных БСШ (см. табл. 1.1 - 1.3). Рассматривались БСШ, поданные на конкурс NIST, на украинский конкурс, а также некоторые распространенные конструкции. Отметим, что в таблице 1.1 для шифров конкурса AES и украинского конкурса приводились данные только для блоков длины 128 бит.

В 1997 г. NIST (National Institute of Standards and Technology,

Национальный Институт Стандартов и Технологий) объявил открытый конкурс на разработку алгоритма блочного симметричного шифрования AES (Advanced Encryption Standard), который должен был прийти на замену DES (Data Encryption Standard) на несколько следующих десятилетий. Пятнадцать алгоритмов шифрования, приведенных в таблице 1.1, были поданы в качестве кандидатов на конкурс AES в 1998 г., затем пять алгоритмов были выбраны в качестве финалистов конкурса в 1999 г. Это MARS, RC6, Rijndael, Serpent и Twofish. Затем в 2001 г. в качестве шифра AES был выбран блочный симметричный алгоритм Rijndael.

В 2006 г. в Украине был объявлен конкурс блочных симметричных шифров. Были поданы пять алгоритмов шифрования: ADE, Лабиринт, Калина, Мухомор и RSB-32. Из-за особенностей своей структуры шифр RSB-32 нельзя отнести к блочным симметричным шифрам, поэтому он не приведен в таблицах 1.1 - 1.3.

Таблица 1.1 приводит общие параметры алгоритмов рассматриваемых БСШ. Увеличение/уменьшение значений данных параметров влияет как на стойкость блочных шифров, так и на скорость криптографического преобразования информации.

Таблица 1.1 – Параметры БСШ

Алгоритм	Размер блока (в битах)	Размер ключа (в битах)	Число раундов
Конкурс AES			
CAST 256	128	128, 160, 192, 224, 256	48
CRYPTON	128	До 256	12
DEAL	128	128, 192.256	6, 8 (256-битный ключ)
DFC	128	До 256	8
E2	128	128, 192, 256	12
FROG	8-128 байт	5-125 байт	8
HPC	Любой размер	512	8

Продолжение таблицы 1.1

Алгоритм	Размер блока (в битах)	Размер ключа (в битах)	Число раундов
LOKI97	128	128, 192, 256	16
MAGENTA	128	128, 192, 256	6-8
MARS	128	128-448	32
RC6	128	128, 192, 256	20
RIJNDAEL	128	128, 192, 256	10, 12, 14
SAFER+	128	128, 192, 256	8, 12, 16
SERPENT	128	128, 192, 256	32
TWOFISH	128	128, 192, 256	16
Распространённые шифры			
DES	64	64 (56)	16
BLOWFISH	64	32-448	16
CAST 128	64	40-128	12, 16
RC5	32, 64, 128	0-2040 (128)	0-255 (12)
SKIPJACK	64	80	32
IDEA	64	128	8
ГОСТ 28147-89	64	256	16, 32
Украинский конкурс			
ADE	128	128, 192, 256	10, 12, 14
Лабиринт	128	128, 192, 256	8
Калина	128	128, 256, 512	10, 14, 30
Мухомор	128	128, 256, 512	11

Таблица 1.2 классифицирует исследуемые блочные симметричные шифры по их структуре. Таблица 1.3 приводит математические операции, на которых основаны рассматриваемые БСШ: ”XOR” — исключающее побитовое ИЛИ w-битных слов, ”[+]” — сложение по модулю 2 ”>>>” —

циклический сдвиг вправо, ">>>" — циклический сдвиг влево. "[-]" — вычитание по модулю 2^w, "[·]" — умножение по модулю 2^w.

Таблица 1.2 показывает, что характерной особенностью конструкций блочного криптографического преобразования информации является использование в качестве шифрующих функций операций нелинейного перемешивания (нелинейных S-блоков, или нелинейных узлов замен). Современные БСШ, не использующие S-блоки, являются больше исключением из правил (RC6, RC5 и IDEA).

Таблица 1.2 – Структуры БСШ

Схема Фейстеля	Модифицированная схема Фейстеля	SP	Другая
DEAL	CAST 256	CRYPTON	FROG
DFC	MARS	RJINDAEL	HPC
E2	RC6	SAFER+	Мухомор
LOKI97	SKIPJACK	SERPENT	
MAGENTA		IDEA	
TWOFISH		ADE	
DES		Калина	
CAST 128			
RC5			
ГОСТ 28147-89			
Лабиринт			

Таблица 1.3 – Математические операции, используемые в БСШ

Алгоритм	Операции								
	XOR	[+]	[-]	[·]	>>>	<<<	S-блок	log_x	exp
Конкурс AES									
CAST 256	+	+	+			+	+		
CRYPTON	+						+		
DEAL	+						+		
DFC	+	+		+			+		

Продолжение таблицы 1.3

Алгоритм	Операции								
	XOR	[+]	[-]	[·]	>>>	<<<	S-блок	log_x	exp
E2	+						+		
FROG	+						+		
HPC	+	+	+	+	+	+	+		
LOKI97	+	+					+		
MAGENTA	+						+		
MARS	+	+	+	+	+	+	+		
RC6	+			+	+	+		+	
SAFER+	+	+		+		+	+		
SERPENT	+					+	+	+	+
TWOFISH	+	+				+	+		
Распространённые шифры									
DES	+						+		
BLOWFISH	+	+					+		
CAST 128	+	+	+			+	+		
RC5	+	+				+			
SKIPJACK	+						+		
IDEA	+	+		+					
ГОСТ 28147-89	+	+				+	+		
Украинский конкурс									
ADE	+			+		+	+		
Лабиринт	+	+	+	+	+	+	+		
Калина	+	+		+	+		+		
Мухомор	+	+		+		+	+		

Подход построения некоторых блочных шифров без использования S-блоков обусловлен накладываемыми ограничениями на память, необходимую для хранения больших S-блоков, не имеющих простого алгебраиче-

ского описания. Другими словами такой подход оправдан, когда большие S-блоки могут быть реализованы только через табличное представление. Например, IDEA достигает требуемого эффекта нелинейного перемешивания, смешивая операции из различных алгебраических групп (XOR, сложение по модулю 2^{16} и умножение по модулю $2^{16}+1$). Однако данный подход имеет ряд недостатков.

Операция умножения по модулю является наиболее нелинейной операцией из трех используемых операций и требует для своей аппаратной реализации большого количества логических элементов, а в программной реализации является относительно медленной операцией. Другим недостатком является проблема масштабирования — 64-битный размер блока шифра IDEA не может быть расширен к 128-битному размеру блока, поскольку число $2^{31}+1$ не является простым. В семействе шифров RC операция нелинейного перемешивания построена при помощи циклических сдвигов, зависящих от обрабатываемых данных. Недостатком такого подхода является то, что циклические сдвиги больших блоков данных (учитывая, что наиболее общий размер обрабатываемых блоков данных — 64 и 128 бит) являются неэффективными операциями на 8-битных платформах.

В целом же можно констатировать, что стойкость методов блочного криптографического преобразования информации базируется, прежде всего, на стойкости нелинейных узлов замен. Это объясняется проверенной временем теорией разработки и использования стойких S-блоков, как ключевой (иногда единственной) нелинейной операции блочного шифра, осуществляющей принцип перемешивания. Поэтому первостепенное значение для разработки стойких блочных симметричных криптографических средств защиты информации приобретает разработка математических моделей и вычислительных методов формирования стойких нелинейных узлов замен.

Проведем анализ и обоснование критериев и показателей стойкости нелинейных узлов замен для методов симметричного криптографического преобразования информации.

1.2 Анализ и обоснование критериев и показателей стойкости нелинейных узлов замен симметричных криптопреобразований

Блок замены (S-блок, S-бокс, S-box, Substitution Box, Векторная булева функция, Узел замены) — отображение n входных бит в m выходных бит, $S : \{0,1\}^n \to \{0,1\}^m$. Таким образом, S-блок является множеством m отдельных выходных булевых функций, объединенных в определенном (заданном) порядке. Для S-блока существует 2^n входов и 2^m возможных выходов. Часто S-блок представляется в виде таблицы.

Если все выходные значения S-блока различны, то S-блок называют инъективным. Если все возможные выходы представлены в S-блоке, то S-блок называют сюръективным. S-блок, который одновременно и инъективен, и сюръективен, называется биективным (сбалансированным). Биективные S-блоки существуют только, если $n = m$.

Регулярный S-блок — это S-блок, у которого все его 2^m возможных выхода появляются одинаковое число раз. Таким образом, каждое из возможных выходных значений появляется в S-блоке 2^{nm} раз. Регулярные S-блоки сбалансированы и существуют только при $n \geqslant m$. Биективные S-блоки являются частным случаем регулярных ($n = m$).

Актуальным направлением исследований являются биективные S-блоки, которые применяются в большинстве БСШ.

Анализ открытой литературы показал, что основными криптографическими показателями нелинейных узлов замен являются:

— сбалансированность;

— корреляционный иммунитет и эластичность (resilience) (для поточных шифров) / критерий распространения и строгий лавинный критерий (для блочных шифров);

— нелинейность;

— максимум таблицы линейных аппроксимаций;

— максимум дифференциальной таблицы;

— лавинность (avalanche): автокорреляция / показатель суммы квадратов (sum-of-square indicator);

— алгебраическая степень;

— линейная избыточность;

— отсутствие фиксированных точек;

— отсутствие линейных структур.

Существует также ряд других показателей, однако анализ открытой литературы показал, что при отборе S-блоков для использования в современных БСШ данные показатели не учитываются. Среди таких показателей, например, показатели, основанные на теории информации:

— независимость между входными и выходными данными;

— независимость между выходными и входными данными;

— независимость между выходными и выходными данными;

— динамическая независимость между входными и выходными данными;

— динамическая независимость между выходными и входными данными;

— динамическая независимость между выходными и выходными данными.

Данные показатели не будут приниматься во внимание в данной магистерской работе.

1.3 Теоретическая и практическая стойкость

Основным назначением криптосистем является обеспечение передачи секретных сообщений через несекретные каналы связи. Поэтому важнейшей характеристикой любой криптосистемы является ее стойкость, т.е. способность противостоять попыткам дешифровать перехваченный шифротекст или раскрыть ключи шифра.

К. Шеннон различал теоретическую и практическую стойкость криптосистем. Криптосистема называется теоретически стойкой, если криптоаналитик не может уточнять распределение вероятностей возможных открытых текстов по имеющемуся и у него шифротексту, даже если он обладает всеми необходимыми для этого средствами. При этом предполагается, что секретный ключ используется только один раз.

Криптосистемы называются практически стойкими если они не могут быть вскрыты в течение реального времени всеми общедоступными методами. На практике используют именно это понятие стойкости криптосистем. Из этого определения можно сделать вывод о том, что проблема создания практически стойких криптосистем или шифров может быть

сведена к проблеме нахождения наиболее сложных задач, удовлетворяющих определенным условием.

Можно составить шифр таким образом, чтобы раскрытие его было эквивалентно, или включало в себя, решение некоторой задачи, про которую известно, что для ее решения требуется определенный (желательно большой объем) работы. Поэтому стойкость криптосистемы можно определить вычислительной сложностью алгоритмов, применяемых криптоаналитиками для шифрования. Такой подход к определению стойкости криптосистем, основанный на понятии вычислительной сложности криптоаналитических алгоритмов основан не на вопросе о том возможно ли извлечь информацию об открытом тексте из анализа шифротекста, а на вопросе о том, осуществимо ли это в приемлемое время. Этот подход позволяет достичь свойства совершенной секретности криптосистемы даже для случаев, когда используется секретные ключи значительно меньше по размерам чем длина открытого шифруемого текста.

1.4 Основные криптографические показатели S-блоков

В терминах булевой алгебры применяются пять основных криптографических показателей нелинейных узлов замен:

1) сбалансированность — равенство числа нулей и единиц в выходной последовательности. Данный показатель связан со свойством биективности.

$$|\{x|f(x)=0\}| = |\{x|f(x)=1\}| = 2^{n-1}; \tag{1.5}$$

2) нелинейность — минимальное расстояние Хемминга между выходной последовательностью функции s и всеми последовательностями афинных функций ϕ:

$$N_s = min\{d(s,\phi)\}; \tag{1.6}$$

3) автокорреляция. Значение функции автокорелляции — макси-

мальное по модулю значение корреляции ко всем входным векторам:

$$AC(f) = \max_{s \neq 0} |\sum_{x} \hat{f}(x)\hat{f}(x \oplus s)| = \max_{s \neq 0} |\hat{r}(s)|; \quad (1.7)$$

4) алгебраическая степень — степень самого длинного слагаемого функции, представленной в алгебраической нормальной форме:

$$f(x_1, \ldots, x_n) = a_0 \oplus \bigoplus_{i=1}^{n} a_i x_i \oplus \bigoplus_{1 \leqslant i < j \leqslant n} a_{ij} x_i x_j \oplus \ldots \oplus a_{12..n} x_1 x_2 \ldots x_n; \quad (1.8)$$

5) критерий распространения КР относительно вектора α — сбалансированность функции:

$$f(x) \oplus f(x \oplus \alpha), x \in V_n, x = (x_1, x_2, \ldots, x_n). \quad (1.9)$$

1.5 Математическая модель регулярных нелинейных узлов замен с использованием недвоичных криптографических функций

Регулярные нелинейные криптографические функции (узлы замен) симметричных шифров реализуют отображение n-битных блоков входных данных в m-битные выходные блоки: $F : GF^n(2) \to GF^m(2)$. Традиционный подход к описанию, оцениванию и разработке методов синтеза регулярных нелинейных узлов замен состоит в представлении функции F с помощью ее координатных функций, которые задаются в терминах булевой алгебры. В то же время, как показано в [2; 7], построение нелинейных узлов замен с высокими показателями стойкости через итеративное формирование компонентных булевых функций является непрактичным уже при $n = 6$ и вычислительно недостижимым для $n > 6$. Это предполагает обоснование новых подходов к описанию криптографических узлов замен симметричных шифров, исследование математического аппарата оценивания основных показателей стойкости и построение вычислительно эффективных алгоритмов синтеза.

1.5.1 Традиционный подход к описанию нелинейных узлов замен через компонентные булевы функции

Введем основные понятия и определения математического аппарата булевой алгебры, используемые в дальнейшем при описании нелинейных узлов замен через компонентные булевы функции и оценке их криптографических свойств.

Булевой функцией $f(x_1, \ldots, x_n)$ от n переменных является функция, осуществляющая отображение из поля $GF(2^n)$ всех двоичных векторов $x = (x_1, \ldots, x_n)$ длины n в поле. Обычно булевы функции представляются в алгебраической нормальной форме (АНФ), т.е. рассматриваются как сумма произведений составляющих координат:

$$f(x_1, \ldots, x_n) = \lambda_0 + \lambda_1 x_1 + \ldots + \lambda_n x_n + \lambda_{12} x_1 x_2 + \ldots + \lambda_{12\ldots n} x_1 x_2 \ldots x_n, \quad (1.10)$$

где $\lambda_0, \lambda_1, \ldots, \lambda_{12\ldots n}$ — уникальные двоичные константы, а суммирование и умножение производится в двоичном поле GF(2).

Поле $GF(2^n)$ состоит из 2^n векторов $\alpha_i = (\alpha_1^i, \alpha_2^i, \ldots, \alpha_n^i), \alpha_j^i \in GF(2)$:

$$\alpha_0 = (0, 0, \ldots, 0), \alpha_1 = (0, 0, \ldots, 1), \alpha_{2^n-1} = (1, 1, \ldots, 1), \alpha_i \in V_n, \quad (1.11)$$

где V_n — векторное пространство над $GF(2)$.

Таблицей истинности функции f называется $(0,1)$-последовательность, определенная как:

$$(f(x)|x \in GF^n(2)) = (f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1})). \quad (1.12)$$

Последовательностью функции f, обозначаемой $\hat{f}$, называется $(1,-1)$-последовательность, определенная как:

$$((-1)^{f(x)}|x \in GF^n(2)) = ((-1)^{f(\alpha_1)}, (-1)^{f(\alpha_2)}, \ldots, (-1)^{f(\alpha_{2^n-1})}). \quad (1.13)$$

Рассмотрим криптографические свойства функций, реализующих отображения из $GF^n(2)$ в $GF^m(2)$, где $1 \leqslant m \leqslant n$. Пусть M_n^m есть

множество таких функций, а B_n есть множество булевых функций от n переменных, то есть функций, реализующих отображения из $GF^n(2)$ в $GF(2)$. Тогда любую функцию $F \in M_n^m$ можно рассматривать как состоящую из m булевых функций от n переменных, т.е. m-выходных координатных функций из B_n.

В более общем представлении, компонентная функция $F \in M_n^m$ является ненулевой линейной комбинацией ее координатных функций из B_n.

Таким образом, функцию $F : GF^n(2) \to GF^m(2)$ запишем через множество

$$F = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)), \tag{1.14}$$

где $f_i(x_1, \ldots, x_n) \in B_n$.

Алгебраическая степень f, обозначаемая $def(f)$, определяется как максимальная степень многочлена представленного в АНФ.

Важные свойства булевых функций изучаются с использованием преобразования Уолша-Адамара.

Преобразование Уолша-Адамара функции $f(x_1, \ldots, x_n) \in B_n$ есть вещественная функция $\bar{F}(\omega)$:

$$\bar{F}(\omega) = \sum_{x \in GF^n(2)} (-1)^{f(x)+\omega \cdot x}, \tag{1.15}$$

где скалярное произведение векторов x и ω определяется как $\omega \cdot x = \omega_1 x_1 + \ldots + \omega_n x_n$.

Булева функция f сбалансирована, если вероятности событий $f(x) = 1$ и $f(x) = 0$ равны. Используя преобразование Уолша-Адамара, условие сбалансированности функции f запишем в виде $\bar{F}(0) = 0$.

Расстояние по Хеммингу между двумя функциями f и g из B_n определяется как:

$$d_H(f, g) = card\{x | f(x) \neq g(x), x \in GF_n(2)\}. \tag{1.16}$$

Нелинейность $NL(f)$ функции определяется как:

$$NL(f) = \min_{g \in A_B} d_H(f, g), \tag{1.17}$$

где A_B — множество всех аффинных функций от n переменных,

$$A_n = \{a_0 + \sum_{i=1}^{n} a_i x_i | a_i \in GF(2), 0 \leqslant i \leqslant n\}. \tag{1.18}$$

С использованием преобразования Уолша-Адамара нелинейность функции f может быть получена следующим образом:

$$NL(f) = 2^{n-1} - \frac{1}{2} \max_{\omega \in GF^n(2)} \bar{F}(\omega). \tag{1.19}$$

Автокорреляционная функция, обозначаемая $r_{\hat{f}}(\alpha)$, вычисляется по формуле:

$$r_{\hat{f}}(\alpha) = \sum_{x \in GF^n(2)} \hat{f}(x)\hat{f}(x \oplus \alpha), \tag{1.20}$$

где $\alpha \in GF^n(2)$ и $r_{\hat{f}}(0) = 2^n$.

Автокорреляция АС функции f является максимальным абсолютным значением автокорреляционной функции:

$$AC = \max_{\alpha \in GF^n(2), \alpha \neq 0} |r(\alpha)|. \tag{1.21}$$

Таким образом, математический аппарат булевых функций является удобным инструментом для описания регулярных нелинейных узлов замен, а использование преобразования Уолша-Адамара дает адекватный механизм оценки основных криптографических показателей стойкости, в частности, нелинейности компонентных булевых функций.

1.5.2 Предлагаемый подход к описанию нелинейных узлов замен через недвоичные функции отображения

Введем основные понятия и определения предлагаемого математического аппарата для описания нелинейных узлов замен через недвоичные функции и оценки их криптографических свойств.

Недвоичной (над полем $GF(2^{n_1})$) функцией $F(X_1, \ldots, X_{n_2})$ от n_2 переменных является функция, осуществляющая отображение из поля $GF((2^{n_1})^{n_2})$ всех векторов длины n_2 с элементами из $GF(2^{n_1})$ в поле $GF(2^{n_1})$. Как и рассмотренные выше булевы функции, каждая недвоичная функция $F(X_1, \ldots, X_{n_2})$ может быть представлена в АНФ.

Корреляционным преобразованием недвоичной функции $F(X_1, \ldots, X_{n_2}) \in B_{n_2}$ есть вещественная функция $R(S)$:

$$R(S) = \sum_{X \in GF^{n_2}(2^{n_1})} \sum_{i=1}^{n_1} (-1)^{(F(X))_i + (F(X+S))_i}. \qquad (1.22)$$

Традиционный подход к описанию и оцениванию нелинейных узлов замен состоит в представлении функции S-блока с помощью ее координатных функций, которые задаются в терминах булевой алгебры. Основными криптографическими показателями нелинейных узлов замен в терминах булевой алгебры являются регулярность (сбалансированность компонентных булевых функций), алгебраическая степень, нелинейность и автокорреляция. Математическая модель представления S-блоков через недвоичные функции является новым направлением исследований в области формирования нелинейных узлов замен.

2 АНАЛИЗ МЕТОДОВ СИНТЕЗА РЕГУЛЯРНЫХ НЕЛИНЕЙНЫХ УЗЛОВ ЗАМЕН

Анализ открытой литературы показал, что на сегодняшний день существует ряд вычислительных методов синтеза регулярных нелинейных узлов замен, которые можно разделить на три основных класса [6–12]:

1) методы случайного поиска (побитовые методы (bit-by-bit methods), методы случайной генерации с фильтрацией (random generation))

2) методы алгебраического построения (степенное отображение в поле, инверсия в поле с афинным преобразованием)

3) методы эвристического поиска (метод градиентного подъема (hill climbing), генетические алгоритмы (genetic algorithms), метод имитации отжига (simulated annealing), метод дифференциальной эволюции (differential evolution), метод оптимизации роем частиц (particle swarm optimization))

В данной работе рассматривается метод эвристического поиска, метод имитации отжига, из соображений достаточно хороших характеристик синтезируемых S-блоков за небольшое время. Так, например, на основе проведенных в работах [10; 15] сравнений показано, что использование метода имитации отжига позволяет реализовать вычислительный поиск криптографических функций с лучшими на сегодняшний день показателями. Описание и алгоритм метода приведены в разделе 2.2.

2.1 Методы случайной генерации

Метод случайной генерации с фильтрацией.

Производится формирование нелинейного узла замен случайным образом, а затем оценивается криптографические показатели, которыми обладает сформированный S-блок. Если сформированный узел замен не удовлетворяет накладываемым критериям поиска (отбора), формируется следующий узел замен. Данный метод является крайне неэффективным.

Побитовый метод.

На вход алгоритма подается система ограничений на криптографические показатели отбираемых m булевых функций (и соответственно всех

их линейных комбинаций).

Некоторая функция j, $j \leqslant m$, фиксируется и считается отобранной для нелинейного узла замен, если функция и все ее линейные комбинации с уже отобранными функциями удовлетворяет заданной системе криптографических ограничений. Если функция не удовлетворяет наложенным криптографическим критериям отбора, она отбрасывается и формируется следующая. Алгоритм продолжает свое выполнение до тех пор, пока требуемый S-блок $n \times m$ не будет сформирован.

Выходными данными алгоритма являются m булевых функций с требуемыми криптографическими показателями, непосредственно представляющие собой нелинейный узел замен.

2.2 Метод имитации отжига

Метод имитации отжига заключается в вероятностном вычислительном поиске криптографических нелинейных узлов замен.

Поиск начинается с некоторого начального состояния $S = S_0$. Параметр T — некий контрольный параметр, известный как температура. T инициализируется высокой температурой T_0 и постепенно снижается. При каждом значении температуры, выполняется определенное число MIL (Moves in Inner Loop, шагов во внутреннем цикле) шагов к новым состояниям. Состояние-кандидата Y выбирается случайным образом из соседей $N(S)$ текущего состояния. Вычисляется изменение значения функции cost, $\delta = cost|Y| - cost(S)$. Если значение $cost(S)$ улучшается (т.е. $\delta < 0$ для задачи минимизации), тогда выполняется шаг относительно этого состояния ($S = Y$); в противном случае — он выполняется с некоторой вероятностью. Чем хуже шаг, тем меньше вероятность того, что он будет принят; чем ниже температура T, тем менее вероятно, что ухудшающий шаг будет принят. Вероятностное принятие решения определяется генерацией случайного числа U в интервале $(0..1)$ и выполнением указанного ниже сравнения.

Вначале температура высокая и принимается почти каждый шаг. Это сделано для того, чтобы поиск носил не локальный, а глобальный характер. По мере того как температура уменьшается, становится все более трудно принимать ухудшающие шаги. В конце концов, допускаются

только улучшающие шаги и процесс застывает. Алгоритм прерывается, когда встречается критерий остановки. Общий критерий остановки — остановка поиска при достижении заданного числа $MaxIL$ внутренних циклов, либо когда было выполнено некоторое максимальное число MUL последовательных непродуктивных внутренних циклов (т.е. без единого принятого шага). При этом лучшее достигнутое состояние сохраняется, поскольку поиск может выйти из него и впоследствии не найти состояние с подобными показателями. В конце каждого внутреннего цикла температура понижается. В исследуемом алгоритме использовалось геометрическое охлаждение — умножение на константу охлаждения α в интервале $(0..1)$.

Алгоритм имитации отжига SA:

$S \leftarrow S0$;
$T \leftarrow T0$;
repeat
    for $i \leftarrow 1$ to MIL do
        выбрать $Y \in N(S)$;
        $delta \leftarrow cost(Y) - cost(S)$;
        if *delta < 0* then
            $S \leftarrow Y$;
        else
            сгенерировать $U \leftarrow U(0,1)$;
        end
        if *U < exp(-delta/T)* then
            $S \leftarrow Y$;
        end
    end
    $T \leftarrow T * alpha$;
until *критерий остановки не достигнут*;

Соседей функции f можно определить следующим образом. Функция g находится по соседству с функцией f, если:

$$\exists x, y \in Z_2^n : \hat{f}(x) \neq \hat{f}(y), \hat{g}(x) = \hat{f}(y), \hat{g}(y) = \hat{f}(x),$$
$$\forall z \in Z_2^n \backslash x, y : \hat{g}(z) = \hat{f}(x). \tag{2.1}$$

Поиск начинался со сбалансированной, но при этом случайной

функции. Один шаг алгоритма меняет местами два отличных элемента таблицы истинности функции, сохраняя ее сбалансированность.

2.3 Стойкость блочных симметричных шифров относительно дифференциального криптоанализа

Метод дифференциального криптоанализа был основан Бихамом и Шамиром и применяется как атака с использованием выбранного открытого текста на блочные симметричные шифры. Дифференциальная атака на БСШ включает анализ переходов входных разностей открытого текста в соответствующие выходные разности шифртекста. Эти переходы используются с целью получения информации — биты ключа, что может снизить вычислительную сложность взлома шифра.

Пусть для блочного шифра с длиной блока B бит блоки $X = X_1X_2X_3 \dots X_B$ и $Y = Y_1Y_2Y_3 \dots Y_B$ представляют собой блоки открытого текста и шифртекста соответственно. Если X_i и X_j – два B-битных блока открытого текста, Y_i и Y_j — их соответствующие выходные блоки, то $\Delta X = X_i \oplus X_j$ и $\Delta Y = Y_i \oplus Y_j$ — их входные и выходные разности соответственно. Пара входных и выходных разностей называется дифференциалом. Каждому дифференциалу соответствует вероятность, что выходная разность появится определенное число раз при заданной входной разности, т.е. $P(\Delta Y|\Delta X)$. Чем ниже дифференциальная вероятность, тем менее вероятно, что выходная разность появится для определенной входной разности. Это желательно, поскольку мы стремимся минимизировать корреляцию между входными и выходными разностями с целью усложнения точного предсказания промежуточных бит на протяжении процесса шифрования. Серия дифференциалов для последовательности раундов в шифре, которые удовлетворяют $\Delta_Y^k = \Delta_X^{k+1}$ для раундов от 1 до l, называется l-раундовой дифференциальной характеристикой. Дифференциальные характеристики используются для определения общей дифференциальной вероятности шифра. Таким образом, вероятность дифференциальной характеристики может быть измерена вычислением произведения вероятностей дифференциала каждого отдельного раунда, предполагая при этом, что они независимы друг от друга.

Очевидно, что на значения дифференциальных вероятностей влияют

используемые компоненты шифра. Нелинейные узлы замен являются ключевым компонентом блочных шифров, поскольку являются основным и, зачастую, единственным источником нелинейности системы шифрования. Дифференциал S-блока — два значения, представляющие собой разность между двумя входными значениями и разность между их соответствующими выходными значениями. Для S-блока $n \times m$ существует всего $2^{2n-1} - 2^{n-1}$ возможных отдельных входных разностных пар. Таблица частот появления всех результирующих выходных разностей (для каждого значения входной разности возможны 2^m различных значений) является таблицей распределения дифференциалов S-блока. Таким образом, дифференциальная таблица — это матрица $2^n \times 2^m$, содержащая частоту появления всех возможных выходных разностей при каждой возможной заданной входной разности. Наибольшее значение в дифференциальной таблице S-блока называют Δ-равномерностью.

Сумма значений каждой строки в дифференциальной таблице должна равняться 2^n. Поэтому плоская дифференциальная таблица, т.е. таблица, в которой частота значений равномерно распределена, означает, что величина частот невелика. Узел замен, чья дифференциальная таблица является плоской, практически не дает никакой информации о выходных разностях, которая может быть применена для раскрытия промежуточных бит шифра. Большие же частотные значения в таблице дифференциалов могут быть использованы для формирования дифференциальной характеристики с высокой вероятностью.

В традиционном блочном шифре в раундах преобразования S-блоки осуществляют множество замен. Объединяя дифференциалы S-блоков, может быть получена дифференциальная характеристика для всего шифра. Для того чтобы шифр был стоек относительно дифференциального криптоанализа, вероятность его дифференциальной характеристики должна быть маленькой. Шифры, содержащие большее число раундов, более вероятно достигнут низкой вероятности дифференциальной характеристики. Величина дифференциалов S-блока также влияет на вероятность дифференциальной характеристики всего шифра. Отсутствие каких-либо больших значений в таблице распределения разностей S-блока приводит к маленьким дифференциальным вероятностям S-блока и, таким

образом, производит дифференциальную характеристику с малой вероятностью.

Пусть DDT_S (Difference Distribution Table) — матрица $2^n \times 2^m$, представляющая таблицу распределения разностей S-блока S $n \times m$. Пусть A_S — матрица $2^n \times 2^m$, представляющая автокорреляционную матрицу S-блока S. Нижняя граница дифференциальной Δ-равномерности, выражаемой через максимальное абсолютное значение автокорреляционной матрицы S-блока, задается следующим образом:

$$\Delta \geqslant 2^{n-m} + 2^{-m} AC(S_{n,m}), \tag{2.2}$$

где $AC(S_{n,m})$ — автокорреляция S-блока S.

Дальнейшее наблюдение, сделанное в [6], заключается в том, что маленькое значение Δ-равномерности подразумевает маленькое значение $AC(S_{n,m})$. Следовательно, минимизация автокорреляции S-блоков способствует повышению стойкости шифра относительно дифференциального криптоанализа через минимизацию их дифференциальной равномерности и, в свою очередь, сокращение вероятности дифференциальной характеристики шифра.

В [6] представлены две верхние границы для нелинейности S-блока $n \times m$, которые относятся к подсчету ненулевых ячеек в дифференциальной таблице S-блока и зависят от n и m. По существу, увеличение числа ненулевых ячеек в таблице соответствует S-блоку с потенциально высокой нелинейностью. Таким образом, использование высоко нелинейного S-блока повышает минимальное число ненулевых ячеек в дифференциальной таблице, сокращая восприимчивость шифра к дифференциальному криптоанализу. В 1990-х гг. было показано [5], что шифр DES (Data Encryption Standard) может быть взломан дифференциальным криптоанализом. Восприимчивость DES была обусловлена, в первую очередь, тем, что дифференциальные таблицы S-блоков DES обладают явной неравномерностью, в то время как стойкость относительно дифференциального криптоанализа характеризуется равномерностью дифференциальной таблицы.

Подводя итоги, можно сказать, что стойкость шифрующих систем

относительно дифференциального криптоанализа усиливается с использованием в них S-блоков с показателями высокой нелинейности и низкой автокорреляции.

2.4 Стойкость блочных симметричных шифров относительно линейного криптоанализа

Линейный криптоанализ, предложенный Мацуи [96] в 1993 г., является атакой по известному открытому тексту, которая стремится аппроксимировать отношения между битами открытого текста, шифртекста и ключа через построение линейного выражения и оценку вероятности этого выражения, точно отображающего это отношение. Таким образом, целью линейного криптоанализа является раскрытие битов ключа.

Пусть для блочного шифра с длиной блока B бит блоки $X = X_1X_2X_3 \dots X_B$ и $Y = Y_1Y_2Y_3 \dots Y_B$ представляют собой блоки открытого и закрытого текста соответственно. Линейный криптоанализ ищет линейное выражение для некоторой комбинации входных и выходных бит

$$\bigoplus_{i=1}^{B} X_i \cdot \alpha_i = \bigoplus_{j=1}^{B} Y_j \cdot \beta_j, \tag{2.3}$$

где $\alpha, \beta \in \{0, 1\}$. Лучшая линейная аппроксимация — это выражение с наивысшей вероятностью появления, а наилучшая аффинная аппроксимация — это выражение с наименьшей вероятностью появления. Пусть $P = P(X = Y)$ — вероятность, связанная с приведенным выше выражением 2.3. Если $P \approx \frac{1}{2}$, это указывает на то, что шифр имеет высокую стойкость к линейным и аффинным аппроксимациям. Смещение вероятности, задаваемое как $|P - \frac{1}{2}|$, является отклонением от ожидаемой вероятности для случайного процесса.

Любое линейное выражение, которое связывает биты открытого, закрытого текста и ключа, должно учитывать структуру шифра и его компонентов, включая используемые в раундах узлы замен. Для нахождения линейной аппроксимации S-блока $n \times m$, линейные отношения между входами и выходами S-блока должны быть посчитаны для всех пар входов

и выходов, что выражается через матрицу $2^n \times 2^m$, называемую таблицей линейных аппроксимаций LAT (Linear Approximation Table).

Каждое значение в ячейках таблицы линейных аппроксимаций $LAT_{X',Y'}$ S-блока может быть посчитано как

$$LAT_{X',Y'} = 2^{n-1} - d_H(X', Y'), \tag{2.4}$$

где d_H — расстояние по Хэммингу между двумя последовательностями. Это значение дает смещение знаковой вероятности $\frac{L_{X',Y'}}{2^n} = P(X' = Y') - \frac{1}{2}$ Смещение вероятности равное нулю указывает на то, что нет возможных линейных аппроксимаций, в то время как смещение, достигающее $\pm\frac{1}{2}$, указывает на то, что S-блок можно легко аппроксимировать с помощью линейной или аффинной функции. Таким образом, лучшая линейная аппроксимация к S-блоку $n \times m$ — это линейное выражение вида 2.3, чьи входные и выходные биты, X' и Y' соответственно, относятся к наибольшему значению таблицы линейных аппроксимаций S-блока.

Линейный криптоанализ блочных симметричных шифров включает нахождение линейной аппроксимации с большой знаковой вероятностью на каждом шаге шифрования, т.е. на каждом раунде. Объединение вероятностей линейных выражений, наилучшим образом аппроксимирующих различные шаги процесса шифрования, основывается на предположении о независимости линейных аппроксимаций на каждом шаге шифрования. Общая линейная аппроксимация шифра получается путем связывания множества линейных выражений вместе. Применение Леммы Мацуи (Piling-Up Lemma) [20] дает вероятность для линейной аппроксимации всего шифра. Чем выше рассчитанная вероятность, тем более вероятно, что с помощью аппроксимации удастся успешно получить биты ключа при достаточном количестве заданных пар открытого-закрытого текста. Чем выше величина смещения, достигаемая отдельными линейными выражениями на каждом шаге шифрования, тем выше общая вероятность линейной аппроксимации шифра. Смещение больших значений в таблице линейных аппроксимаций S-блока приводит к более успешной атаке на весь шифр.

Значения таблицы линейных аппроксимаций S-блока $n \times m$

тесно связаны со значениями матрицы преобразования Уолша-Адамара всех линейных комбинаций компонентных булевых функций S-блока. Смещение (bias) выражается через значения преобразования Уолша-Адамара следующим образом:

$$bias = L_{X',Y'} = \frac{\hat{F}(w)}{2}, \tag{2.5}$$

что напрямую связано с нелинейностью S-блока:

$$NL(S_{n,m}) = 2^{n-1} - |L_{X',Y'}|_{max}, \tag{2.6}$$

где $X' \neq 0$, $Y' \neq 0$ и $|L_{X',Y'}|_{max}$ представляет максимальное абсолютное значение в таблице линейных аппроксимаций.

Таким образом, использование высоконелинейных S-блоков в системах шифрования предпочтительно для того, чтобы шифр имел стойкость к атакам линейного криптоанализа. В 1993 г. в [20] показано, что DES также был взломан при помощи линейного криптоанализа. Успешность атаки была обусловлена наличием больших значений в таблицах линейных аппроксимаций S-блоков DES. Как упоминалось ранее, стойкость относительно линейного криптоанализа требует низких значений в таблице линейных аппроксимаций, которые получаются через использование высоко нелинейных S-блоков. Мы заключаем, что высокая нелинейность и низкая автокорреляция — важные свойства S-блоков, необходимые для обеспечения стойкости БСШ относительно дифференциального и линейного криптоанализа.

2.5 Эффективность блочных симметричных шифров относительно дифференциального и линейного криптоанализа

Задачу проектирования практического алгоритма БСШ следует рассматривать как задачу минимизации "затрат" на реализацию криптопреобразования, обеспечивающего необходимые показатели стойкости [4]. При этом можно утверждать, что шифр имеет стойкость относительно какого-либо вида криптоанализа, если для успешной реализации атаки

на шифр потребуется большее число вычислительных затрат, чем на реализацию атаки типа ”грубой силы”. Тогда можно утверждать, что исследуемый шифр достиг свойств случайной подстановки относительно данного вида атак.

Общим требованием к разрабатываемым вычислительным методам синтеза нелинейных узлов замен с улучшенными свойствами является улучшение показателей нелинейности и автокорреляции S-блоков, что значит максимизировать нелинейность и минимизировать актокорреляцию.

Общепринятыми показателями оценки стойкости алгоритмов БСШ относительно дифференциального и линейного криптоанализа являются оценки вероятностей дифференциальной и линейной характеристик шифра, которые необходимо минимизировать.

При этом эффективность БСШ относительно дифференциального и линейного криптоанализа определяется числом раундов зашифрования (либо вычислительных затрат на реализацию шифрования), необходимых для выхода шифра к дифференциальным и линейным свойствам случайных подстановок.

Очевидно, что чем меньше требуется вычислительных затрат на реализацию криптопреобразования для обеспечения требуемых показателей стойкости, тем выше эффективность шифра.

3 ИССЛЕДОВАНИЕ МЕТОДА ИМИТАЦИИ ОТЖИГА

В данном разделе представлены улучшения метода имитации отжига (simulated annealing) и экспериментальные результаты, полученные данным методом для шифров DES, MacGuffin и ГОСТ 28147-89. Исследнованы новые критерии вычислительного поиска криптографически стойких S-блоков. На основе усовершенствованных весовых коэффициентов ценовых функций поиска предлагается дальнейшее развитие метода имитации отжига. В основу предлагаемых функций стоимости положены спектральные и корреляционные свойства недвоичных криптографических функций, математический аппарат которых предложен в [3]. Проведены оценки быстродействия формирования нелинейных узлов замен методом имитации отжига для шифров MacGuffin и ГОСТ 28147-89 в сравнении с методом случайной генерации.

3.1 Ценовые функции и их улучшение

Метод имитации отжига, изложенный в разделе 2.2, основывается на постепенном улучшении текущего нелинейного узла замен оценивая эффект внесённых изменений на каждом шаге формирования при помощи cost (ценовой) функции.

Рассмотрим процедуры формирования функций стоимости ценовых функций, используемые для синтеза S-блоков через спектральные характеристики булевых функций, введем соответствующие функции стоимости для синтеза S-блоков через спектры недвоичных криптографических функций.

Пусть функция $F(x) : GF^n(2) \to GF^m(2)$ задает S-блок размерности $n \times m$. Пусть для $\beta \in GF^m(2)$, $F_\beta(x) = \beta_1 f_1(x) \oplus \ldots \oplus \beta_m f_m(x)$, — линейная комбинация m выходов S-блока F. Тогда $\hat{F}_\beta(\omega), r_\beta(s)$ — значения преобразования Уолша-Адамара и значения автокорреляции для каждой булевой функции f_β.

Поскольку нелинейность булевой функции

$$NL_f = \frac{1}{2}(2^n - \max_\omega |\hat{F}(\omega)|), \tag{3.1}$$

то задача повышения нелинейности может быть представлена как задача минимизации абсолютного максимального значения коэффициента Уолша-Адамара. Изначально в задачах синтеза S-блоков по критерию высокой нелинейности для метода имитации отжига использовалась следующая функция стоимости [10]:

$$cost(f) = WHT_{max}(f) = \max_{\omega} |\hat{F}(w)|. \tag{3.2}$$

Поскольку задача понижения автокорреляции представляется как задача минимизации максимального значения автокорреляционной функции, то cost функция в дальнейших исследованиях приняла следующий вид [10]:

$$cost(f) = AC(f) = \max_{s \neq 0} |\sum_{x} \hat{f}(x)\hat{f}(x \oplus s)| = \max_{s \neq 0} |\hat{r}(s)|. \tag{3.3}$$

Обычно в многокритериальных задачах применяется следующий подход: вычисляется сумма отдельных cost функций (по различным критериям), умноженных на весовые коэффициенты. Тогда cost функция в задаче синтеза S-блока с высокой нелинейностью и низкой автокорреляцией принимает вид [10]:

$$cost(f) = \alpha \cdot WHT_{max}(f) + \beta \cdot AC(f). \tag{3.4}$$

Далее были разработаны улучшенные функции, которые основывались на следующем положении.

Известно, что равенство Парсеваля

$$\sum (\hat{F}(\omega))^2 = 2^{2n} \tag{3.5}$$

ограничивает $WHT_{max}(f) = \max_{\omega} |\hat{F}(\omega)|$ значением равным как минимум $2^{n/2}$. Данная граница достигается тогда, когда выполняется равенство $\hat{F}(\omega) = 2^{n/2}$ для каждого ω. Когда значение некоторого коэффициента $|\hat{F}(\omega)|$ меньше этой идеальной границы, теорема Парсеваля утверждает,

что другие значения коэффициентов $|\hat{F}(\omega)|$ должны быть выше этой границы. Таким образом, попытка ограничить отдаленность абсолютных значений коэффициентов Уолша-Адамара от данной границы является возможным средством достижения высокой нелинейности. Спектры некоторых функций содержат все значения (по модулю), равные этой идеальной границы. Такие функции называются бент-функциями.

Помимо обладания наивысшей возможной нелинейностью эти функции имеют нулевую автокорреляцию. Следовательно, функция стоимости

$$cost(f) = \sum_{\omega \in GF^n(2)} ||\hat{F}(\omega)| - 2^{n/2}|^R \tag{3.6}$$

является возможным подходом к оптимизации нелинейности и автокорреляции. В виду несбалансированности бент-функций приведенная функция стоимости cost может быть улучшена для нахождения сбалансированных криптографических функций. В [10] было введено обобщение функции стоимости (3.6), которое приняло следующий вид

$$cost(f) = \sum_{\omega \in GF^n(2)} ||\hat{F}(\omega)| - X|^R. \tag{3.7}$$

Параметры X и R, называемые весовыми коэффициентами, обеспечивают свободу для экспериментирования и поиска оптимальных значений.

По аналогии с функциями стоимости относительно спектра Уолша-Адамара вида (3.7), функции стоимости относительно спектра автокорреляционной функции имеют следующий вид:

$$cost(f) = \sum_{s \in GF^n(2)} ||r(s)| - X|^R. \tag{3.8}$$

Традиционно, ценовые функции применяются для оптимизации отдельной булевой функции. Для всего же нелинейного узла замен cost функции, основанные на спектре Уолша-Адамара, можно обобщить

следующим образом [10]:

$$cost(f) = \sum_{\beta \in GF^m(2)} \sum_{\omega \in GF^n(2)} ||\hat{F}_\beta(\omega)| - X|^R \tag{3.9}$$

и аналогично для cost функций, основанных на автокорреляционном спектре:

$$cost(f) = \sum_{\beta \in GF^m(2)} \sum_{s \in GF^n(2)} ||r_\beta(s)| - X|^R. \tag{3.10}$$

Для оптимизации по критериям нелинейности и автокорреляции в [15] использовалась следующая функция стоимости:

$$\begin{aligned} cost(f) = & \sum_{\beta \in GF^m(2)} \sum_{\omega \in GF^n(2)} ||\hat{F}_\beta(\omega)| - X_1|^{R_1} \\ & + \sum_{\beta \in GF^m(2)} \sum_{s \in GF^n(2)} ||r_\beta(s)| - X_2|^{R_2}. \end{aligned} \tag{3.11}$$

Изначально в исследованиях использовались функции стоимости вида (3.8), (3.9), с заменой спектральных коэффициентов Уолша-Адамара и коэффициентов автокорреляционных спектров булевых функций на предложенные в [3] коэффициенты соответствующих спектров недвоичных функций.

Дальнейшие исследования состояли в совершенствовании функций стоимости (критерия поиска криптографических функций), которое основывается на следующем положении. Известно, что при оптимизации криптографической функции по нелинейности и автокорреляции она по своим спектральным характеристикам (спектру корреляции с линейными функциями и автокорреляционному спектру) стремится к спектральным характеристикам бент-функций, что и было использовано в предыдущих работах [10; 15] при разработке функций вида (3.6) - (3.11). В тоже время, очевидным недостатком такого подхода является использование одного (фиксированного) значения статического коэффициента, к которому стремятся все спектральные значения оптимизируемой криптографической

функции. При этом значения спектральных коэффициентов идеальной функции (или бент-функции) состоят из двух возможных значений для булевых функций, и из трех значений для введенных в [3] недвоичных функций. При введении же дополнительных ограничения на сбалансированность, количество возможных значений спектральных коэффициентов еще более возрастает.

При разработке новых функций стоимости предлагается в (3.7) - (3.11) заменить статический весовой коэффициент X на так называемые динамические весовые коэффициенты, т.е. весовые коэффициенты, принимающие различные значения для различных входных индексов спектра. В данной работе в качестве значений динамических весовых коэффициентов используются спектральные значения бент-функций. Предлагаемые функции стоимости имеют вид:

$$cost(f) = \sum_{\omega \in GF^n(2)} |\hat{F}_\beta(\omega)| - \hat{B}(\omega)|^R, \tag{3.12}$$

$$cost(f) = \sum_{s \in GF^n(2)} |r_F(s)| - r_B(s)|^R, \tag{3.13}$$

$$\begin{aligned} cost(f) = & \sum_{\omega \in GF^n(2)} |\hat{F}_\beta(\omega)| - \hat{B}(\omega)|^{R_1} \\ & + \sum_{s \in GF^n(2)} |r_F(s)| - r_B(s)|^{R_2}, \end{aligned} \tag{3.14}$$

где $\hat{B}(\omega), r_B(s)$ — спектральные значения нелинейности и автокорреляции случайной недвоичной бент-функции B.

Таким образом, в основе предлагаемого вычислительного метода синтеза регулярных нелинейных узлов замен симметричных криптоалгоритмов лежит применение математического аппарата недвоичных криптографических функций [3], методов корреляционного и спектрального анализа, а также предложенных в данной работе усовершенствованных ценовых функций (3.12) - (3.14), с использованием динамических весовых коэффициентов $\hat{B}(\omega), r_B(s)$. Усовершенствованный таким образом метод имитации отжига позволяет, как показано ниже, реализовать вычис-

лительный поиск регулярных узлов замен с требуемыми показателями нелинейности и автокорреляции.

3.2 Экспериментальных исследования формирования нелинейных узлов замен

Для подтверждения достоверности и обоснованности полученных теоретических результатов в данной работе проведены экспериментальные исследования эффективности предлагаемого вычислительного метода синтеза регулярных нелинейных узлов замен. Первая часть исследований была проведена с использованием спектров недвоичных функций со статическими весовыми коэффициентами в функциях стоимости (3.9) - (3.11) метода имитации отжига, вторая часть исследований — с использованием динамических коэффициентов в функциях стоимости (3.12) - (3.14).

Путём экспериментальных исследований были выбраны следующие параметры для всех последующих вычислединий:

— $\alpha = 0.95$ — параметр геометрического охлаждения;

— $MIL = 500$ — число шагов, предпринимаемых во внутреннем цикле;

— $MaxIL = 300$ — максимальное число внутренних циклов поиска;

— $MUL = 50$ — максимальное число последовательных непродуктивных внутренних циклов;

— количество пробегов алгоритма для каждого набора параметров равно 10.

В ходе экспериментов с функциями стоимости вида (3.9) - (3.11) использовались различные значения статических коэффициентов X и фиксированное значение $R = 3$.

Формировались S-блоки размерностей 8×2, 4×4, 6×4. Узлы замен выходной размерности 4 представлялись через одну недвоичную функцию над GF(24).

Полученные экспериментальные результаты для S-блоков 8×2 приведены в табл. 3.1. Лучший полученный результат выделен жирным шрифтом.

Как видно из полученных результатов использование функций

стоимости с динамическими весовыми коэффициентами позволило повысить показатели стойкости нелинейности и автокорреляции формируемых узлов замен.

В табл. 3.2 приведено сравнение полученных результатов с лучшими известными результатами, использующих традиционный подход описания S-блока в виде совокупности компонентных булевых функций [8–12]. Как видно из приведенной таблицы, полученные экспериментальные результаты предлагаемым методом с использованием функций стоимости на основе спектров недвоичных функций и статических весовых коэффициентов хорошо согласуются с экспериментальными результатами вычислительных методов традиционного подхода. Использование динамических весовых коэффициентов позволило получить лучшие известные на сегодняшний день результаты для S-блоков 8×2.

Таблица 3.1 – Криптографические свойства S-блоков 8×2

Способ построения спектров	Статические коэффициенты		Динамические коэффициенты	
	NL	AC	NL	AC
WHT, ср.	110	56	114	24
WHT, худш.	108	56	116	24
ACT, ср.	110	48	114	24
ACT, худш.	112	40	114	24
WHT+ACT, худш.	112	40	114	24
WHT+ACT, ср.	112	40	114	24

В табл. 3.3 приведены лучшие полученные результаты для S-блоков 4×4 и 6×4.

Как видно из приведенной таблицы, применение предлагаемого подхода позволяет повысить нелинейность формируемых S-блоков 6×4. Подобные S-блоки (размерности 6×4) применяются в DES-подобных шифрах.

Таблица 3.2 – Сравнение с результатами традиционного подхода, синтез S-блоков 8×2

Метод синтеза	NL	AC
Случайная генерация	108	56
Генетические алгоритмы	110	48
Имитация отжига (булевы функции)	114	32
Имитация отжига (недвоичные функции)	112	40
Имитация отжига (недвоичные функции, динамические весовые коэффициенты)	116	24

Таблица 3.3 – Криптографические свойства S-блоков 4×4, 6×4

S-блок	Метод имитации отжига	NL	AC
4×4	Булевы функции	4	8
4×4	Функции над GF(24)	4	8
6×4	Булевы функции	22	24
6×4	Функции над GF(24)	24	24

Как показал проведенный анализ S-блоки DES по своим криптографическим показателям нелинейности NL и автокорреляции AC далеки от оптимальных (см. данные для S1-S8 в табл. 3.4). Разработанный вычислительный метод предлагается использовать для синтеза DES-подобных S-блоков с улучшенными криптографическими показателями стойкости (в табл. 3.4 приведены характеристики формируемых узлов замен S1*-S8*).

Следует отметить, что для обеспечения стойкости DES-подобных шифров к дифференциальному и линейному криптоанализу сформированные S-блоки необходимо оценивать не только по показателям нелинейности и автокорреляции, но и с учетом других критериев, учитывающих саму структуру шифра [16]. В этом смысле оценка эффективности формируемых S-блоков с учетом ограничений, накладываемых особенностями основных преобразований БСШ, а также апробация полученных результатов являются перспективным направлением дальнейших исследований.

Таблица 3.4 – Исследование криптографических свойств регулярных узлов замен 6×4

S-блок	NL	AC	DDT_{max}
S1	14	48	16
S2	16	56	16
S3	16	48	16
S4	16	64	16
S5	12	**40**	**16**
S6	**18**	48	16
S7	14	52	16
S8	16	48	16
S1*-S8*	**24**	**24**	**10**

3.3 Критерии построения нелинейных узлов замен DES

В [19] описаны следующие критерии, которым должны соответствовать нелинейные узлы замен в шифре DES:

— (S-1) Каждый нелинейный узел замен имеет шесть входных и четыре выходных бит;

— (S-2) Ни один выходной бит узла замен не должен быть слишком близок к линейной функции входных бит, это значит, выбирая любое положение выходного бита и любое подмножество из шести бит на входе позиций, доля данных, для которых этот выходной бит равен XOR этих входных биты не должно быть близко к 0 или 1, а скорее должны быть около 1/2;

— (S-3) Если зафиксировать самый левый и правый входные биты, выходные биты должны быть различны для всех вохможных 4-хбитовых выходов;

— (S-4) Если два входа в нелинейный узел замен отличаются ровно на один бит, то выходные значения должны отличаться не менее, чем на два бита;

— (S-5) Если два входа в нелинейный узел замен отличаются ровно

в двух средних битах, то выходы должны отличаться не менее, чем в двух битах;

— (S-6) Если два входа в нелинейный узел замен отличаются в их первых двух битах и идентичны в их последних двух битах, то два выхода не должны совпадать.

Данные критерии были реализованы в утилите, описанной в разделе 4, и использовались для дальнейшей оценки формируемых нелинейных узлов замен в разделе 3.4.

3.4 Экспериментальные исследования DES-подобных шифров

В данном разделе будут рассмотрены экспериментальные результаты влияния нелинейных узлов замен на сложность дифференциального и линейного криптоанализа DES и MacGuffin шифров. Для сравнения будут использованы рекомендуемые к шифрам и сформированные методом имитации отжига нелинейные узлы замен.

Исследования нелинейных узлов замен размерностью 6×4, которые используются в DES, были представленны в разделе 3.2, однако в данном разделе к требованиям, выдвигаемым к формируемым нелинейным узлам замен, добавятся критерии, выдвигаемые непосредственно к узлам замен, применяемых в шифре DES. Данные критерии [19] были рассмотрены в разделе 3.3, также реализованы в утилите, описанной в разделе 4.

Однако, сформировать нелинейные узлы замен, отвечающие одновременно нашим критериям и критериям, выдвигаемыми авторами шифра DES, в отведённые сроки не удалось. Это может также свидетельствовать о необходимости замены полностью случайной генерации начального состояния и случайных перестановок на детерменированные методы, разработанные специально для нелинейных узлов замен DES.

Таким образом, для дальшейших исследований был взят шифр MacGuffin. Данный шифр интересен тем, что имеет такую же размерность S-блоков, 6×4, однако имеет не 2^4 различных выходов, а только 2^2. Также шифр MacGuffin изначально разрабатывался в исследовательских целях, что делает его привлекательным для изучения.

Шифр MacGuffin не выдвигает никаких требований к нелинейным узлам замен, кроме размерности 6×4 и выходным значениям из $GF(2^2)$.

В ходе исследований были получены и проанализированы такие показатели:

— нелинейность (NL);

— автокорреляция (AC);

— Δ-разность (максимум в таблице дифференциалов);

— лучшая линейная аппроксимация (максимальное абсолютное значение в таблице линейных аппроксимаций).

Для увеличения стойкости необходимо максимизировать нелинейность и минимизировать автокорреляцию, дифференциальную и линейнную характеристики.

Как можно убедиться из таблиц 3.5 и 3.6, метод имитации отжига дал оптимальные нелинейные узлы замен, которые по всем показателям дал значительное улучшение оцениваемых показателей.

Таблица 3.5 – Криптографические свойства исходных S-блоков шифра MacGuffin

S-блок	NL	AC	Δ-разность	Лучшая линейная аппроксимация
1	18	32	34	14
2	18	40	36	14
3	18	48	34	14
4	16	64	32	16
5	20	32	32	12
6	20	48	32	12
7	18	48	34	14
8	20	40	32	12

Отдельно стоит отметить скорость получения оптимальных нелинейных узлов замен. Для сравнения используем наиболее простой альтернативный метод получения узлов замен — метод случайной генерации.

Таблица 3.6 – Криптографические свойства S-блоков для шифра MacGuffin, сформированных методом имитации отжига

S-блок	NL	AC	Δ-разность	Лучшая линейная аппрок-симация
2, 2, 2, 1, 3, 3, 3, 3, 0, 3, 0, 2, 0, 0, 1, 0 0, 3, 2, 0, 3, 2, 0, 1, 1, 2, 3, 3, 2, 0, 3, 2 2, 2, 1, 3, 1, 1, 0, 2, 2, 0, 2, 3, 1, 3, 1, 0 1, 1, 3, 1, 1, 3, 2, 1, 0, 3, 2, 1, 0, 0, 0, 1	24	16	24	8
2, 1, 1, 2, 1, 2, 2, 2, 0, 0, 3, 0, 3, 1, 2, 0 3, 0, 3, 3, 3, 1, 1, 3, 0, 0, 2, 0, 0, 0, 2, 3 2, 3, 1, 3, 3, 1, 3, 2, 2, 2, 0, 3, 3, 1, 1, 1 2, 2, 3, 1, 0, 0, 0, 1, 0, 1, 0, 3, 2, 1, 2, 1	24	16	24	8
2, 0, 2, 0, 1, 3, 0, 3, 1, 0, 2, 0, 1, 1, 2, 2 2, 0, 3, 2, 3, 3, 3, 3, 2, 3, 0, 1, 1, 2, 3, 0 3, 0, 0, 2, 1, 0, 3, 1, 2, 2, 2, 1, 1, 1, 2, 0 1, 1, 0, 3, 3, 1, 0, 2, 3, 1, 0, 3, 2, 3, 1, 0	24	16	24	8
1, 1, 1, 0, 2, 0, 3, 2, 1, 0, 2, 2, 1, 2, 0, 1 3, 3, 3, 1, 2, 3, 3, 1, 3, 2, 3, 2, 3, 0, 1, 2 1, 0, 0, 0, 2, 2, 0, 2, 1, 0, 1, 3, 1, 3, 0, 2 0, 3, 0, 3, 3, 1, 0, 2, 0, 0, 2, 1, 3, 2, 1, 3	24	16	24	8
2, 1, 2, 2, 1, 2, 3, 1, 0, 2, 0, 0, 0, 0, 0, 1 1, 1, 3, 3, 0, 3, 2, 2, 2, 1, 1, 0, 0, 0, 3, 2 0, 2, 1, 3, 2, 2, 2, 1, 1, 0, 2, 3, 0, 2, 1, 3 3, 0, 1, 0, 3, 3, 1, 3, 3, 1, 3, 1, 2, 3, 0, 3	24	16	24	8
2, 3, 0, 3, 1, 3, 2, 2, 3, 1, 2, 0, 0, 3, 2, 0 0, 0, 2, 1, 1, 3, 0, 0, 3, 0, 1, 1, 3, 2, 3, 2 2, 1, 3, 0, 1, 2, 0, 1, 1, 3, 2, 0, 2, 0, 0, 2 2, 1, 1, 0, 2, 3, 1, 1, 3, 0, 1, 3, 3, 1, 2, 3	24	16	24	8
3, 1, 2, 1, 3, 2, 0, 3, 3, 2, 1, 2, 1, 1, 0, 1 3, 1, 0, 1, 2, 3, 1, 3, 3, 2, 2, 0, 2, 3, 0, 0 0, 2, 1, 0, 0, 1, 2, 2, 0, 0, 0, 0, 3, 3, 2, 0 2, 2, 3, 1, 3, 2, 3, 3, 3, 0, 2, 1, 0, 1, 1, 1	24	16	24	8
3, 1, 2, 1, 0, 3, 3, 2, 2, 0, 2, 0, 0, 0, 2, 1 1, 3, 2, 3, 0, 0, 0, 0, 3, 1, 2, 2, 1, 3, 2, 2 3, 0, 1, 2, 0, 1, 2, 2, 3, 1, 3, 0, 2, 2, 0, 1 0, 1, 1, 3, 3, 1, 2, 0, 3, 1, 3, 3, 1, 3, 1, 0	24	16	24	8

Оценка скорости формирования производилась следующим образом:

— устанавливались минимальные удовлетворяющие требования к критериям нелинейности, автокорреляции и дифферецниальным и линейным характеристикам;

— далее, в течение 48 часов (по 24 часа на каждый метод) на шести незадействованных серверах были запущены вышеописанные методы формирования узлов замен;

— по полученным результатам оценивалось количество нелинейных узлов замен, прощедших отбор по минимальным требованиям, нормированных на 1 процесс в сутки — K1;

— соотношение числа прошедших отбор нелинейных узлов замен к числу непрошедших — K2.

Минимальными удовлетворяющими требованиями были выбраны оптимальные показатели:

— нелинейность — 24;

— автокорреляция — 16;

— Δ-равномерность — 24;

— лучшая линейная аппроксимация — 8.

Данные тестирования эффективности метода имитации отжига относительно скорости формирования нелинейных узлов замен, предоставленные в таблице 3.7, свидетельствуют о значительном превосходстве метода имитации отжига в сравнении с методом случайной генерации. Так, формирование S-блоков методом имитации отжига на 3800% эффективнее метода случайной генерации по общему количеству оптимальных узлов замен, а также на 4900% эффективнее по общему числу проверок отбора.

Таблица 3.7 – Оценки скорости формирования нелинейных узлов замен MacGuffin

Метод	K1, S-блоков/сутки	K2
Метод имитации отжига	12.96	0.005
Метод случайной генерации	0.33	0.000001

3.5 Экспериментальные исследования ГОСТ 28147-89

Известные математические оценки верхней границы вероятности практической стойкости [17] дифференциального (3.17) и линейного (3.18) криптоанализа позволили дополнительно оценить криптографические свойства формируемых узлов замен. Стоит отметить, что данные оценки не являются оценкой доказуемой стойкости ГОСТ 28147-89, однако, это лучшая оценка, полученная точным математическим доказательством.

Данные оценки дают понимание о зависимости стойкости ГОСТ 28147-89 от характеристик нелинейных узлов замен в случае теоретического открытия дифференциального или линейного криптоанализа на данный шифр:

$$M_D(S) \leqslant max\{\Delta(S)^{r+1-2\lceil\frac{r}{3}\rceil} \cdot \Delta'(S)^{\lceil\frac{r}{3}\rceil}, \Delta(S)^{r-1}\}, \tag{3.15}$$

$$M_L(S) \leqslant \Lambda(S)^{[\frac{2r}{3}]}. \tag{3.16}$$

Так как в ГОСТ 28147-89 используется 32 раунда шифрования, то после подстановки $r = 32$ получим:

$$M_D(S) \leqslant max\{(\Delta(S) \cdot \Delta'(S))^{11}, \Delta(S)^{31}\}, \tag{3.17}$$

$$M_L(S) \leqslant \Lambda(S)^{21}, \tag{3.18}$$

где

$$\Delta(S) = max\{d(s) : \forall s \in S\}, \tag{3.19}$$

$$\Delta'(S) = max\{d'(s) : \forall s \in S\}, \tag{3.20}$$

$$d(s) = max\{2^{-t} \sum_{k \in V_t} \delta(s(k+\alpha) \oplus s(k), \beta) : \alpha, \beta \in V_t \backslash \{0\}\}, \tag{3.21}$$

$$d'(s) = max\{2^{-t} \times \sum_{\substack{k \in V_t \\ \nu(\alpha,k)=a}} \delta(s(k+\alpha) \oplus s(k), \beta) \tag{3.22}$$

$$: \alpha, \beta \in V_t \backslash \{0\}, a \in \{0,1\}\},$$

$$\Lambda(S) = max\{l(s) : \forall s \in S\}, \tag{3.23}$$

$$l(s) = max\{2^{-t} \sum_{k \in V_t} (2^{-t} \sum_{x \in V_t} (-1)^{\beta s(x+k) \oplus \alpha x})^2 : \alpha, \beta \in V_t \backslash \{0\}\}. \tag{3.24}$$

Заметим, что в 3.19 - 3.24 используется символ Кронекера 3.25 и t — размерность нелинейного узла замен, например, $t = 4$ для узлов замен 4×4. Также стоит отметить, что оператор сложения $(+)$ определён как сложение по модулю 2^t, а $\nu(\alpha, k)$ — бит переполнения суммы α и k в кольце $\mathbb{Z}$.

$$\delta(a,b) = \begin{cases} 1, & \text{если } a = b \\ 0, & \text{если } a \neq b \end{cases} \tag{3.25}$$

Для сравнения полученных результатов были взяты S-блоки, используемые в криптографических приложениях ЦБ РФ, и проанализированы их свойства, полученные результаты представлены в таблице 3.8.

Метод имитации отжига позволяет получить лучшие показатели нелинейности, автокорреляции, а также теоретической стойкости к дифференциальному и линейному криптоанализам. В результате расчётов было получено более 600 нелинейных узлов замен 4×4 с показателями равными лучшим теоретическим оценкам, некоторые из сформированных узлов замен представлены в таблице 3.9.

Для биективных 4×4 узлов замен лучшие теоретические оценки составляют:

— нелинейность [18] должна быть максимизирована:

$$NL_{max}(S) = 2^{n-1} - 2^{n/2} = 4;$$

— автокорреляция должна быть минимизирована: $AC_{min}(S) = 8$;

— для дифференциального и линейного криптоанализа верхняя граница вероятности должна быть минимизирована для максимизации практической стойкости шифра.

Как видно из таблицы 3.8, нелинейные узлы замен, используемые в ЦБ РФ не являются оптимальными по указанным выше критериям. Если сравнивать с S-блоками, полученными методом имитации отжига, представленными в таблице 3.9, то можно убедиться, что практическая стойкость ГОСТ 28147-89 по оценке верхней границы вероятности дифференциального криптоанализа может быть улучшена в 2^{22} раз и в 2^7 раз для линейного криптоанализа.

Таблица 3.8 – Оценка стойкости исходных S-блоков ГОСТ 28147-89

S-блок		NL	AC	M_D	M_L
S1	4, 10, 9, 2, 13, 8, 0, 14, 6, 11, 1, 12, 7, 15, 5, 3	4	16	$2^{-53.13}$	2^{-42}
S2	14, 11, 4, 12, 6, 13, 15, 10, 2, 3, 8, 1, 0, 7, 5, 9	2	16	$2^{-48.57}$	2^{-42}
S3	5, 8, 1, 13, 10, 3, 4, 2, 14, 15, 12, 7, 6, 0, 9, 11	2	16	$2^{-48.57}$	2^{-42}
S4	7, 13, 10, 1, 0, 8, 9, 15, 14, 4, 6, 12, 11, 2, 5, 3	2	16	$2^{-42.13}$	$2^{-38.43}$
S5	6, 12, 7, 1, 5, 15, 13, 8, 4, 10, 9, 14, 0, 3, 11, 2	2	16	$2^{-48.57}$	$2^{-35.24}$
S6	4, 11, 10, 0, 7, 2, 1, 13, 3, 6, 8, 5, 9, 12, 15, 14	2	16	$2^{-42.13}$	$2^{-37.6}$
S7	13, 11, 4, 1, 3, 15, 5, 9, 0, 10, 14, 7, 6, 8, 2, 12	2	16	$2^{-48.57}$	2^{-42}
S8	1, 15, 13, 0, 5, 7, 10, 4, 9, 2, 3, 14, 6, 11, 8, 12	2	16	$2^{-34.02}$	$2^{-37.6}$
S1-S8		2	16	$2^{-34.02}$	$2^{-35.24}$

Рассчитав сложность криптоанализа для каждого раунда, от 1 до 32, для нелинейных узлов замен, используемых в ЦБ РФ, и полученных методом имитации отжига, можем оценить эффективность использования

оптимальных узлов замен путём сравнения необходимого числа раундов для достижения того же уровня стойкости, что и исходные узлы замен.

Таблица 3.9 – Нелинейные узлы замен, сформированные методом имитации отжига для ГОСТ 28147-89

S-блок	NL	AC	M_D	M_L
9, 7, 14, 3, 6, 5, 13, 0, 4, 2, 8, 10, 1, 11, 15, 12	4	8	2^{-66}	2^{-42}
7, 3, 11, 9, 5, 4, 14, 2, 1, 12, 6, 8, 0, 15, 13, 10	4	8	2^{-66}	2^{-42}
2, 1, 7, 4, 6, 14, 0, 10, 15, 3, 11, 13, 9, 5, 8, 12	4	8	2^{-66}	2^{-42}
15, 3, 2, 10, 0, 5, 11, 4, 6, 1, 8, 14, 13, 9, 12, 7	4	8	2^{-66}	2^{-42}
7, 9, 4, 5, 13, 0, 15, 11, 1, 3, 10, 12, 6, 2, 14, 8	4	8	2^{-66}	2^{-42}
9, 1, 14, 7, 3, 0, 11, 12, 4, 2, 6, 13, 15, 5, 10, 8	4	8	2^{-66}	2^{-42}
6, 11, 14, 8, 1, 2, 7, 9, 5, 15, 12, 3, 4, 13, 10, 0	4	8	2^{-66}	2^{-42}
3, 13, 12, 9, 6, 11, 0, 1, 7, 14, 4, 2, 10, 5, 15, 8	4	8	2^{-66}	2^{-42}

На рисунках 3.1, 3.2 представлены графики, построенные по таблице 3.11, видно, что с использованием оптимальных нелинейных узлов замен уровень стойкости равный уровню стойкости с применением узлов замен ЦБ РФ достигается на 17 и 27 раундах относительно критериев стойкости к дифференциальному и линейному криптоанализу соответственно, что на 47% и 16% эффективнее.

Нельзя утверждать, что данное исследование свидетельствует о том, что необходимо сократить число раундов в шифре, однако, нужно отметить, что при одинаковом числе раундов, эффективность шифрования может быть увеличена лишь за счёт замены нелинейных узлов на оптимальные.

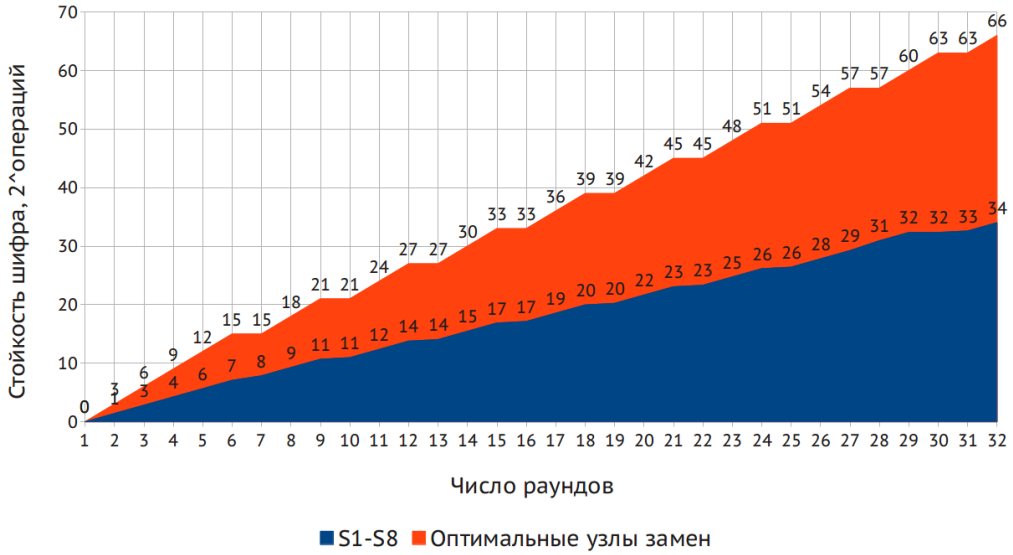

Рисунок 3.1 – Зависимость стойкости узлов замен к дифференциальному криптоанализу от числа раундов

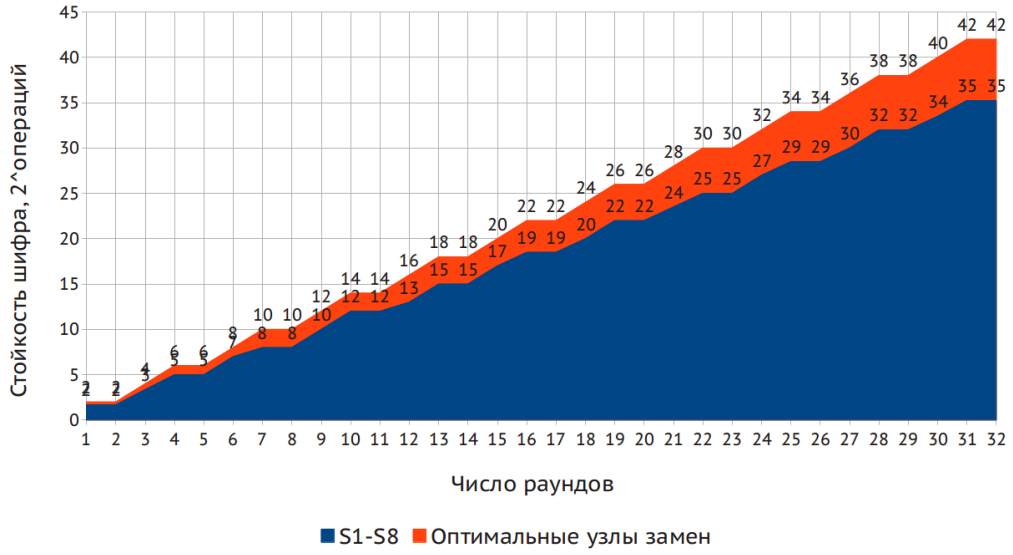

Рисунок 3.2 – Зависимость стойкости узлов замен к линейному криптоанализу от числа раундов

Также стоит отметить скорость получения оптимальных нелинейных узлов замен. Для сравнения используется наиболее простой альтернативный метод получения узлов замен — метод случайной генерации.

Оценка скорости формирования производилась следующим образом:

— устанавливались минимальные удовлетворяющие требования к критериям нелинейности, автокорреляции и дифферецниальным и

линейным характеристикам;

— далее, в течение 48 часов (по 24 часа на каждый метод) на четырёх незадействованных серверах были запущены вышеописанные методы формирования узлов замен;

— по полученным результатам оценивалось количество нелинейных узлов замен, прощедших отбор по минимальным требованиям, нормированных на 1 процесс в сутки — K1;

— соотношение числа прошедших отбор нелинейных узлов замен к числу непрошедших — K2.

Минимальными удовлетворяющими требованиями были выбраны оптимальные показатели:

— нелинейность — 4;

— автокорреляция — 8;

— верхняя граница вероятности дифференциального криптоанализа — 2^{-66};

— верхняя граница вероятности линейного криптоанализа — 2^{-42}.

Как видно из таблицы 3.10, метод имитации отжига на 200% эффективнее случайной генерации по абсолютному количеству формируемых оптимальных нелинейных узлов замен, а также на 3 порядка эффективнее с точки зрения операций проверки выдвинутых для тестирования минимальных требований. Так метод случайно генерации требует в среднем 10000 проверок финальных условий для получения одного S-блока, удовлетворяющего требованиям, в то время как метод имитации отжига формирует оптимальный нелинейный узел замен на каждый пятый выход.

Таблица 3.10 – Оценки скорости формирования нелинейных узлов замен ГОСТ 28147-89

Метод	K1, S-блоков/сутки	K2
Метод имитации отжига	172	0.2
Метод случайной генерации	53	0.0001

Таблица 3.11 – Сравнение вероятности криптоанализа оптимальных нелинейных узлов замен с используемыми в ЦБ РФ

№ раунда	$M_D(S1-S8)$	M_D(оптимальные)	$M_L(S1-S8)$	M_L(оптимальные)
1	2^{0}	2^{0}	$2^{-1.68}$	2^{-2}
2	$2^{-1.42}$	2^{-3}	$2^{-1.68}$	2^{-2}
3	$2^{-2.83}$	2^{-6}	$2^{-3.36}$	2^{-4}
4	$2^{-4.25}$	2^{-9}	$2^{-5.03}$	2^{-6}
5	$2^{-5.66}$	2^{-12}	$2^{-5.03}$	2^{-6}
6	$2^{-7.08}$	2^{-15}	$2^{-6.71}$	2^{-8}
7	$2^{-7.86}$	2^{-15}	$2^{-8.39}$	2^{-10}
8	$2^{-9.28}$	2^{-18}	$2^{-8.39}$	2^{-10}
9	$2^{-10.69}$	2^{-21}	$2^{-10.07}$	2^{-12}
10	$2^{-10.96}$	2^{-21}	$2^{-11.75}$	2^{-14}
11	$2^{-12.37}$	2^{-24}	$2^{-11.75}$	2^{-14}
12	$2^{-13.79}$	2^{-27}	$2^{-13.42}$	2^{-16}
13	$2^{-14.05}$	2^{-27}	$2^{-15.10}$	2^{-18}
14	$2^{-15.47}$	2^{-30}	$2^{-15.10}$	2^{-18}
15	$2^{-16.88}$	2^{-33}	$2^{-16.78}$	2^{-20}
16	$2^{-17.14}$	2^{-33}	$2^{-18.46}$	2^{-22}
17	$2^{-18.56}$	2^{-36}	$2^{-18.46}$	2^{-22}
18	$2^{-19.97}$	2^{-39}	$2^{-20.14}$	2^{-24}
19	$2^{-20.24}$	2^{-39}	$2^{-21.81}$	2^{-26}
20	$2^{-21.65}$	2^{-42}	$2^{-21.81}$	2^{-26}
21	$2^{-23.07}$	2^{-45}	$2^{-23.49}$	2^{-28}
22	$2^{-23.33}$	2^{-45}	$2^{-25.17}$	2^{-30}
23	$2^{-24.74}$	2^{-48}	$2^{-25.17}$	2^{-30}
24	$2^{-26.16}$	2^{-51}	$2^{-26.85}$	2^{-32}
25	$2^{-26.42}$	2^{-51}	$2^{-28.53}$	2^{-34}
26	$2^{-27.84}$	2^{-54}	$2^{-28.53}$	2^{-34}
27	$2^{-29.25}$	2^{-57}	$2^{-30.21}$	2^{-36}
28	$2^{-30.93}$	2^{-57}	$2^{-31.88}$	2^{-38}
29	$2^{-32.35}$	2^{-60}	$2^{-31.88}$	2^{-38}
30	$2^{-32.35}$	2^{-63}	$2^{-33.56}$	2^{-40}
31	$2^{-32.61}$	2^{-63}	$2^{-35.24}$	2^{-42}
32	$2^{-34.02}$	2^{-66}	$2^{-35.24}$	2^{-42}

4 ОПИСАНИЕ ПРОГРАММЫ

В данном разделе описывается функциональные возможности программы.

4.1 Общие сведения

Данная утилита была разработана в исследовательских академических целях, для практической проверки работоспособности теоретических методов, описанных в разделе 3.

Программа является кроссплатформенной, так как реализована на языке C++, компилятор и набор библиотек, которого имеет широкую распространённость на различных операционных системах.

Данная реализация может в дальнейшем развиваться и агрегировать в себе другие методы формирования и оценки S-блоков.

4.2 Функциональное назначение

Данная программа реализует работу с S-блоками, базовый математический аппарат для исследовения характеристик S-блоков, тестирование нелинейных узлов замен критериями, выдвигаемыми к шифру DES, а так же метод имитации отжига S-блоков для произвольной размерности нелинейных узлов замен. Так же в программе по-умолчанию реализованы методы оценки и формирования нелинейных узлов замен для шифров: DES, MacGuffin, ГОСТ 28147-89.

4.3 Описание логической структуры

На рисунке 4.1 продемонстрирован алгоритм работы программы в режиме имитационного моделирования. В каждом цикле тестирования случайно инициализируется S-блок, после чего применяется алгоритм имитации отжига, описанный в разделе 3, и в результате оцениваются характеристики полученного S-блока.

Основными функциями программы являются:

— Синтез нелинейных узлов замен методом имитации отжига (см.

приложение А):
void SimulatedAnnealing::run()

— Оценка нелинейности, автокорреляции S-блока (см. приложение Б):
int SBox::get_NL(),
int SBox::get_AC();

— Оценка верхних границ вероятности дифференциального и линейного криптоанализа ГОСТ 28147-89 (см. приложение В):
double SBox::get_MD(),
double SBox::get_ML();

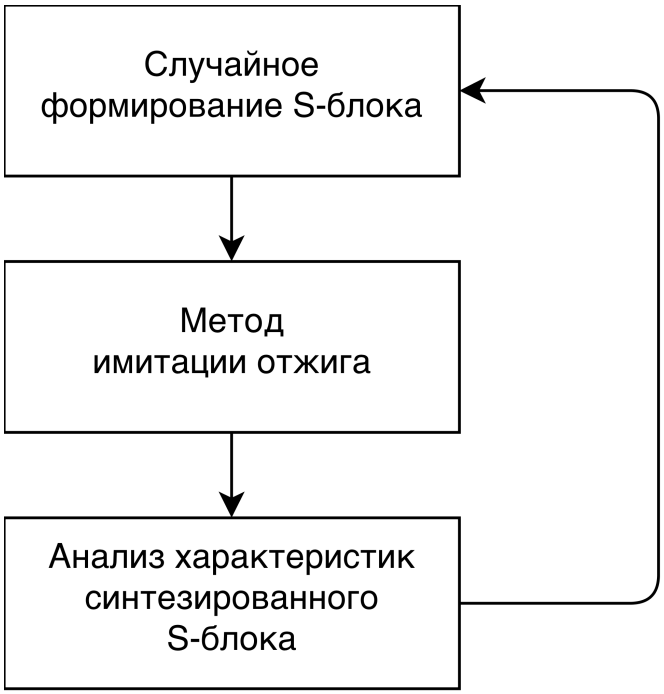

Рисунок 4.1 – Алгоритм работы программы

4.4 Используемые технические средства

Для работы данной программы необходимо устройство с процессором, архитектура которого поддерживается компилятором C++ кода (например, GCC поддерживает все наиболее распространённые архитектуры и множество менееизвестных). Реализация протестирована и гарантированно функционирует в ОС GNU/Linux.

4.5 Вызов и загрузка

Программа не принимает никаких параметров в момент запуска, все параметры константно задаются перед компиляцией.

4.6 Входные и выходные данные

Входными данными является случайно сгенерированное начальное состояние нелинейного узла замен.

Выходными данными является синтезированный нелинейный узел замен и его характеристики. Так же программа имеет режим тестирования, в котором она вычисляет наихудшие и средние характеристики сформированных S-блоков по критериям нелинейности, автокорреляции и значениям таблицы разностей.

5 ОХРАНА ТРУДА И БЕЗОПАСНОСТЬ В ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

5.1 Анализ условий труда на рабочем месте аналитика в НИЛ

Производственное помещение, научно-исследовательская лаборатория (НИЛ), содержит четыре рабочих мест, каждое из которых оборудовано ПК в комплекте: системный блок, жидкокристаллический экран, компьютерная мышь, клавиатура.

Размеры помещения составляют 5х4,6х3 м. Нормой, в соответствии с ДСанПиН 3.3.2-007-98, является площадь на одно робочее место не менее 6,0 м^2 объём — не менее 20,0 м^3. Помещение НИЛ включает 4 рабочих места площадью 23 м^2 и объёмом 69 м^3, что составляет 5,75 м^2 площади и 17.25 м^3 объёмом на одно рабочее место, что не соответствует требованиям ДСанПиН 3.3.2-007-98.

В помещении имеются два окна общей площадью 8 м^2.

С целью анализа условий труда в помещении НИЛ была рассмотрена система ”Человек-Машина-Среда” (Ч-М-С).

Ч1-Ч4 — коллектив людей, состоящий из 4 человека, работающих одновременно в пределах одного помещения. Состоит из трех функциональных частей:

Чх.1 — аналитик, который выполняет работу на ПК.

Чх.2 — аналитик, который рассматривается с точки зрения влияния на окужающую среду.

Чх.3 — психофизиологическое состояние человека.

М1-М4 — комплекс оборудования для осуществления трудового процесса (проведения исследований). Представлен четырьмя ПК:

Мх.1 — ПК, используемый аналитиком.

Мх.2 — аварийная защита ПК.

Мх.3 — влияние ПК на окружающую среду и человека.

Среда — внутренняя среда помещения: освещение, микроклимат.

ПТ — предмет труда — исследование методов формирования узлов замен блочных симметричных шифров.

Структура системы Ч-М-С рассмотрена на рисунке 5.1. Направление

и содержание связей сведены в таблицу 5.1

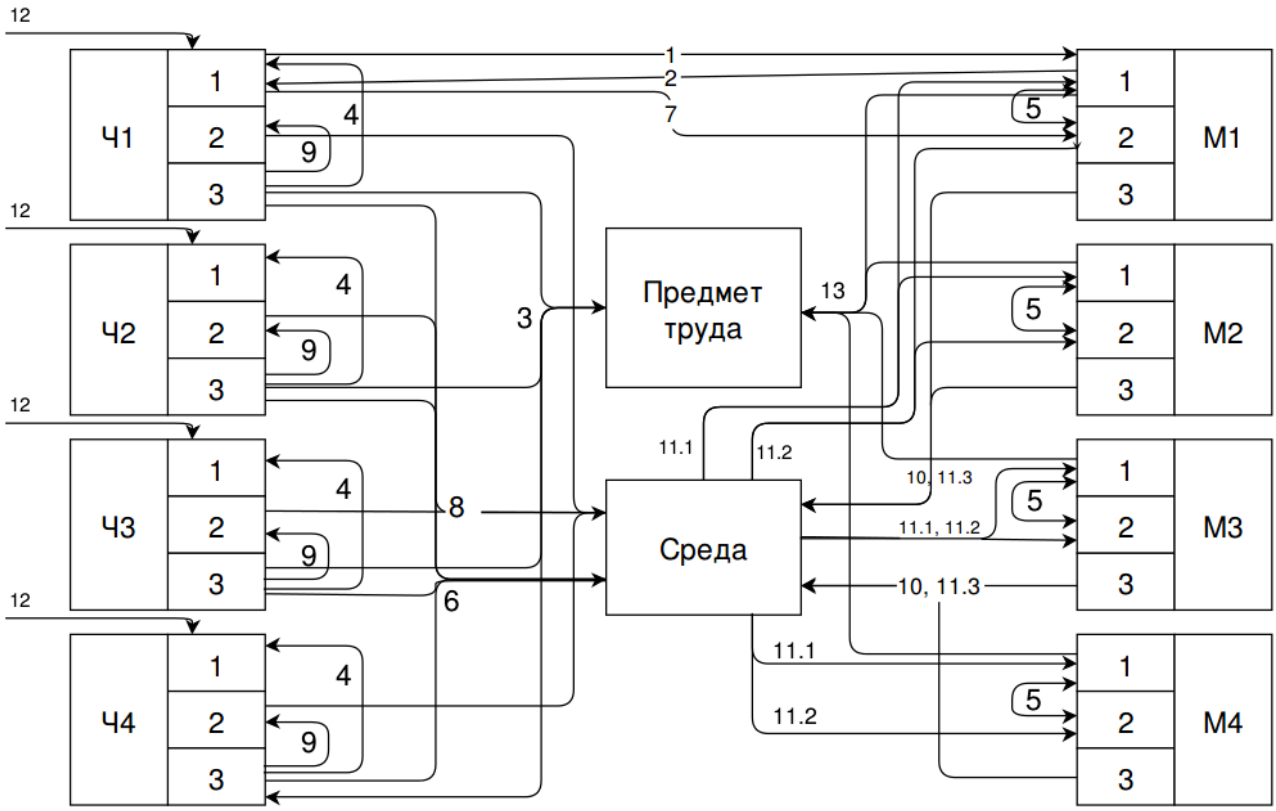

Рисунок 5.1 – Структура системы Ч-М-С

Потенциально опасными и вредными производственнми факторами по ГОСТ 12.0.003-74 для данного помещения НИЛ являются:

1) физические:
   — повышенная или пониженная температура воздуха рабочей зоны;
   — повышенная или пониженная подвижность воздуха;
   — отсутствие или недостаток естественного света;
   — недостаточная освещённость рабочей зоны;
2) химические: отсутствуют;
3) биологические: отсутствуют;
4) психофизиологические:
   — монотонность труда;
   — умственное перенапряжение;
   — перенапряжение анализаторов (зрительные).

Таблица 5.1 – Декомпозиция системы Ч-М-С.

Номер связи	Направления связи	Содержание связи
1	Чх.1-Мх.1	Влияние человека на ПК и его настройки
2	Мх.1-Чх.1	Информация про состояние ПК
3	ПТ-Чх.3	Влияние процесса анализа атак на психологическое состояние аналитика
4	Чх.3-Чх.1	Уменьшение продуктивности работы вследствие монотонности труда и умственного перенапряжения
5.1	Мх.1-Мх.2	Информация, необходимая для генерации аварийного управляющего влияния
5.2	Мх.2-Мх.1	Недостаточная освещённость и вентиляция рабочего места
6	С-Чх.3	Влияние среды на состояние организма аналитика
7	Чх.1-Мх.2	Влияние аналитика на аварийное состояние ПК
8	Чх.2-С	Выделения углекислого газа вследствие процесса дыхания, выделение тепла и пота
9	Чх.3-Чх.2	Влияние психофизиологического состояния на степень интенсивности обмена веществ между организмом и средой
10	Мх.3-С	Электромагнитные излучения, шум, температура
11.1	С-Мх.1	Влияние параметров окружающей среды (температура, влажность, запылённость) на работу ПК
11.2	С-Мх.2	
11.3	С-Мх.3	
12	Внешняя система управления - Лх.1	Информация про общий технологический процесс
13	Мх.1-ПТ	Влияние машины на предмет труда. Непредвиденное отлючение питания, приводящее к остановке рабочего процесса

Результаты оценки факторов производственной среды и трудового процесса приведены в табл. 5.2.

Таблица 5.2 – Оценка факторов производственной среды и трудового процесса

Факторы производственной среды и процесса труда	Значение фактора (ПДК, ПДР)		3-й класс — опасные и вредные условия, характер труда			Длительность действия фактора, в % за смену
	Норма	Факт	1 ст.	2 ст.	3 ст.	
1	2	3	4	5	6	7
1. Вредные хим. вещества: 1-й класс опасности	-	-	-	-	-	-
2-й класс опасности	-	-	-	-	-	-
3-4-й класс опасности	-	-	-	-	-	-
2. Вибрация	-	-	-	-	-	-
3. Шум, дБ	До 50	49	-	-	-	93
4. Инфразвук	-	-	-	-	-	-
5. Ультразвук	-	-	-	-	-	-
6. Неионизирующее излучение радиочастотного диапазона, В/м	5 Гц .. 2 кГц – 25; 2 кГц...400 кГц – 2,5	5 Гц .. 2 кГц – до 25; 2 кГц .. 400 кГц – до 2,5	-	-	-	93
7. Рентгеновское излучение, мкР/ч	До 100	14	-	-	-	100
8. Микроклимат: 8.1 Температура воздуха, С	х: 22-24	23	-	-	-	100
	т: 23-25	24	-	-	-	100
8.2 Скорость движения воздуха, м/с	х: 0,1	менее 0,1	-	-	-	100
	т: 0,1	менее 0,1	-	-	-	100
8.3 Относительная влажность, %	х: 60-40	57	-	-	-	100
	т: 60-40	52	-	-	-	100
9. Атмосферное давление, мм. рт. ст.	740-760	744	-	-	-	100
10. Освещение: 10.1 Естественное (КЕО)	1,2	1,6	-	-	-	93
10.2 Искусственное, лк	300-500	370	-	-	-	93
11. Тяжесть труда: 11.1 Мелкие стереотипные движения кистей и пальцев рук	До 40000	20000	-	-	-	80
11.2 Рабочая поза (нахождение в наклоненном положении в течение смены)	До 25% времени за смену	Поза свободная	-	-	-	93
11.3 Наклоны корпуса тела (раз за смену)	51-100	Произвольные	-	-	-	93

Продолжение таблицы 5.2

1	2	3	4	5	6	7
11.4 Перемещения в пространстве (по горизонтали), км за смену	До 8	0,1	-	-	-	93
Напряженность труда а) внимание - длительность сосредоточенного восприятия (% от времени смены	25-50	48	-	-	-	93
- плотность сигналов (световых, звуковых) и сообщений, за час	75-175	250		+		93
б) нагрузка на анализаторы - зрительный, наблюдение за экранами ВДТ, ч за смену	2-3	3	-	-	-	93
- слуховой, восприятие речи или сигналов	Разборчивость слов и сигналов от 90% до 70% от их кол-ва	99% разборчивых слов и сигналов	-	-	-	93
в) монотонность - количество элементов в многократно повторяемых операциях	9-6	Больше 10	-	-	-	93
- длительность выполнения повторяющихся операций, с	100-25	100-25	-	-	-	93
- время активных действий (в % от длительности смены)	76-80	80	-	-	-	80
г) режим труда - факт. длительность рабочего дня, ч	8-9	9	-	-	-	100
- сменность работы	Двусменная без ночной смены	Односменная без ночной смены	-	-	-	100
- наличие регламентированных перерывов и их длительность, % времени смены	3-7	7	-	-	-	100
Общее количество факторов	8	8	-	1	-	-

Доминирующим вредным производственным фактором является недостаток естественного света.

5.2 Промышленная безопасность в производственном помещении НИЛ

Характеристики сети электропитания: трёхфазная четырёхпроводная сеть переменного тока с глухозаземлённой нейтралью и напряжением 380/220 В, частотой 50 Гц. Согласно НПАОП 40.1-1.21-98 помещение по опасности поражения электрическим током относится к классу без

повышенной опасности.

В помещении отсутствуют другие опасные производственные факторы.

Для защиты людей от поражения электрическим током предусмотрено зануление, двойная изоляция, защитное отключение устройств в помещении (согласно НПАОП 40.1-1.32-01).

Для обеспечения безопасности работы проводится вводный, первичный и повторный (1 раз в 6 месяцев) иствруктажи по технике безопасности (согласно НПАОП 0.00-4.12.05).

5.3 Производственная санитария в помещении НИЛ

Работы в помещении согласно ДСН 3.3.6.042-99 относятся к категории работ с энергозатратами организма ”лёгкая 1а” - сидячая работа, не требует систематического физического напряжения и перемещения предметов с энергозатратами организма 90-120 кКал/час.

В соответствии с ДСН 3.3.6.042-99 для обеспечения установленных норм микроклиматических параметров и чистоты воздуха используется кондиционирование воздуха в тёплый период и отопление в холодный. Шум в помещении создается внутренними источниками: устройствами кондиционирования воздуха и другим оборудованием, а также шумом, проникающим извне и не привышает допустимой нормы, согласно ДСН 3.3.6.037-99.

В светлое время суток рекомендуется, согласно ДСанПиН 3.3.2-007-98, использовать естественное освещение, а искустенное только в условиях недостаточности естественного освещения. Для искуственного освещения используют люминисцентные лампы за счёт их высокой световой отдачи, длительного срока службы, экономности и спектру, наиболее близкому к ествественному.

Для оценки соответствия помещения требованиям НПАОП 0.00-1.28-10 относительно величины коэффициента естественного освещения расчитаем требуемую площадь светового проёма. При боковом одностороннем освещении суммарная площадь световых проемов определяется по

формуле:

$$S_0 = S_{\text{П}} \frac{e_N \cdot \eta_0 \cdot K_3 \cdot K_{\text{ЗД}}}{100 \cdot \tau_0 \cdot r_1} [\text{м}^2], \tag{5.1}$$

где S_0 — суммарная площадь всех световых проёмов, м^2;

$S_{\text{П}}$ — площадь пола помещения, м^2;

e_N — нормированное значение К.Е.О.;

η_0 — световая характеристика окна, определяется по таблицам СНиП на основании отношений:

$$\frac{L_{\text{П}}}{B} = \frac{5}{4,6} = 1,09; \text{ и } \frac{B}{h_1} = \frac{4,6}{2} = 2,3; => \eta_0 = 16 \tag{5.2}$$

K_3 — коэффициент запаса, учитывающий загрязнение светопропускающего материала светового проема, зависит от типа помещения и от расположения стекол. При вертикальном расположении K_3=1,2;

$K_{\text{ЗД}}$ — коэффициент, учитывающий затемнение окон противостоящими зданиями. При отсутствии противостоящих зданий $K_{\text{ЗД}} = 1$;

r_1 — коэффициент, учитывающий отраженный свет. $r_1 = 1,2$;

τ_0 — общий коэффициент светопропускания светового проема.

$$\tau_0 = \tau_1 \cdot \tau_1 \cdot \tau_2 \cdot \tau_3 \cdot \tau_4 \tag{5.3}$$

τ_1 — коэффициент светопропускания материала. Для оконного окна 0,8;

τ_2 — коэффициент, учитывающий потери света в переплетах окна. Для деревянных спаренных оконных рам 0,85;

τ_3 — коэффициент, учитывающий потери света в несущих конструкциях. При отсутствии несущих конструкций 1;

τ_4 — коэффициент, учитывающий потери света в солнцезащитных устройствах. При отсутствии таковых 1.

$$\tau_0 = 1,2 \cdot 0,8 \cdot 1 \cdot 1 = 1,02 \tag{5.4}$$

Вычислим суммарную расчётную площадь световых проемов:

$$S_0 = 23\frac{1,6 \cdot 16 \cdot 1,2 \cdot 1}{100 \cdot 1,02 \cdot 1,6} = 4.3\text{м}^2. \tag{5.5}$$

Действительная площадь световых проёмов составляет 8 м^2, что превышает рассчитанное значение, следовательно помещение отвечает требованиям НПАОП 0.00-1.28-10.

Организация и конструкция рабочего места должны обеспечивать соответствие всем элементов рабочего места и его расположение эргономичным требованиям ГОСТ 12.2.032-78 и НПАОП 0.00-1.28-10. На рисунке 5.2 изображена схема размещения рабочих мест в помещении НИЛ, включающая так же схему эвакуации работников.

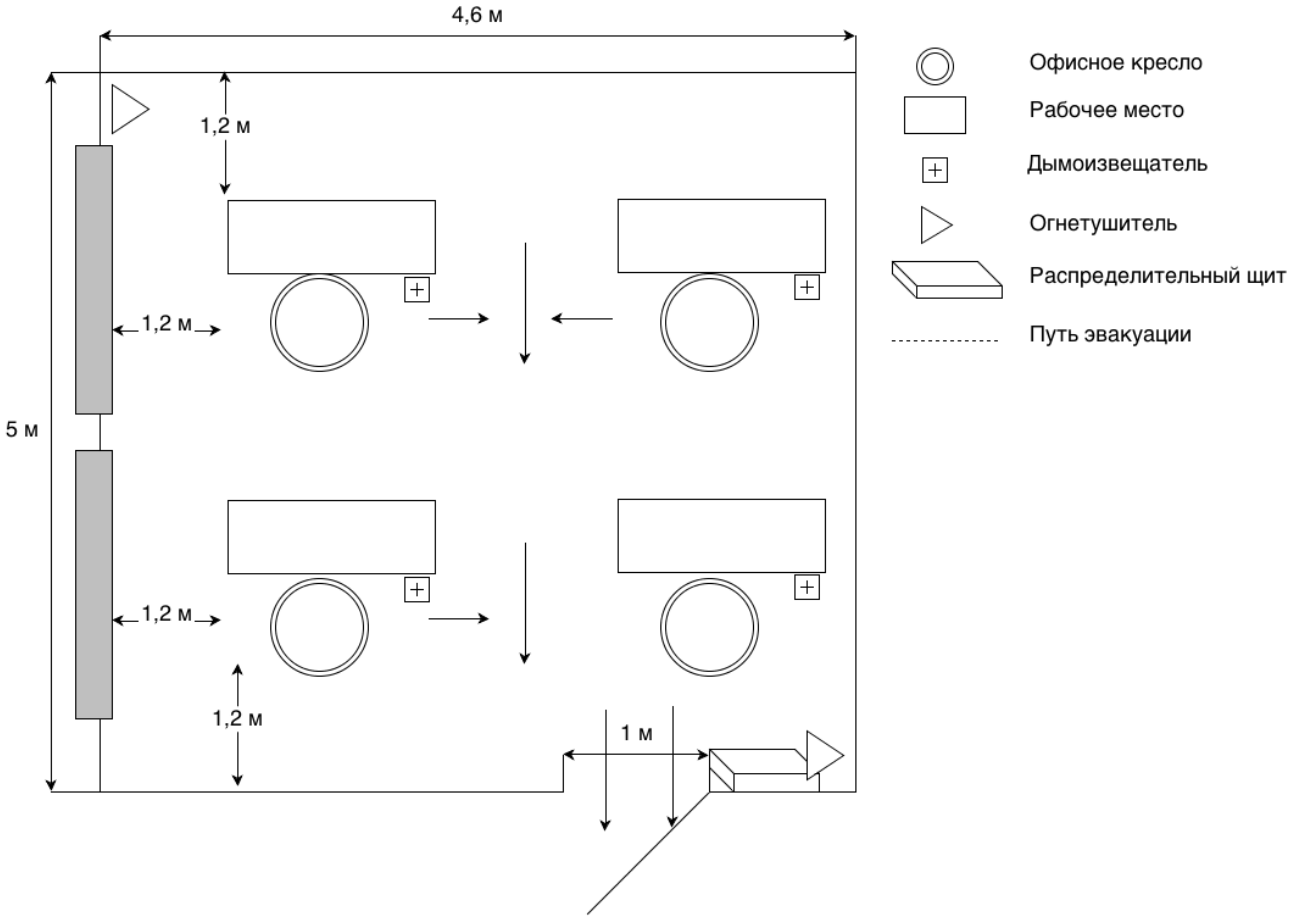

Рисунок 5.2 – Схема размещения рабочих мест в помещении НИЛ

5.4 Безопасность в чрезвычайных ситуациях

Защита населения в чрезвычайных ситуациях представляет собой комплекс взаимосвязанных по месту, времени, цели и ресурсам мероприятий, направленных на защиту жизни и здоровья людей в любых ЧС. Указанные мероприятия должны планироваться и в максимально возможной степени проводиться заблаговременно и на всей территории страны, охватывая все категории населения.

Объем и содержание мероприятий инженерно-технической защиты населения, правила и порядок их осуществления устанавливаются в соответствии с требованиями действующего законодательства и нормативных правовых актов по вопросам защиты населения и территорий от чрезвычайных ситуаций и от опасностей, возникающих при ведении военных действий и с учетом экономических, природных и иных особенностей конкретных территорий, зон, городских и сельских поселений и реальной опасности для населения в мирное и военное время.

Основными инженерно-техническими мероприятиями по защите населения являются:

— укрытие людей в приспособленных для их защиты помещениях производственных, общественных и жилых зданий, а также в специальных защитных сооружениях;

— повышение надежности систем жизнеобеспечения (водоснабжение, энергопитание, теплофикация и др.) при авариях, катастрофах, стихийных бедствиях и в военное время, а также устойчивости жизненно важных объектов социального и производственного назначения;

— выполнение ряда градостроительных требований, позволяющих при крупномасштабных ЧС и применении в военных конфликтах современных средств поражения уменьшить количество жертв, обеспечить выход населения из разрушенных частей города в парки и леса загородной зоны, а также создать условия для ввода в пораженную зону аварийно-спасательных сил.

Основным способом защиты населения от современных военных средств поражения, от крупномасштабных ЧС, вызванных авариями и катастрофами на химически и радиационно-опасных объектах, взрывами и пожарами, остается укрытие персонала предприятий и населения городов

в защитных сооружениях.

В соответствии с действующими нормами и правилами по вопросам выполнения инженерно-технических мероприятий гражданской обороны, а также строительными нормами и правилами (СНиП) к защитным сооружениям относятся убежища и противорадиационные укрытия.

Производство, включающее научно-исследовательскую лабораторию, имеет категорию В пожаровзрвыоопасности, согласно НАПБ Б.03.002-2007. Степень огнестойкости здания — II, согласно ДБН В.1.1.7-2002, так как помещение расположено в кирпичном здании, при строительстве использовались твёрдые несгораемые материалы.

Возможные причины возникновения пожара на рабоем месте или в помещении:

— короткое замыкание, сопровождающееся искрением и перегревом элементов ПК вследствие чего происходит воспламенение оборудования;

— перегрев элементов ПК в следствии высокой нагрузки во время проведения атаки;

— кабели для подачи электропитания.

Согласно ДБН В.2.5.-13-98 в помещении установлено четыре точечных дымовых пожарных извещателя. В помещении присутствуют два углекислотных огнетушителя ВВК-1,4 из расчета 1 огнетушитель на 3 ПК, но не менее 1 на помещение, согласно НАПБ Б.03.001-2204.

Схема эвакуации нанесена на схеме размещения рабочих мест в помещении НИЛ на рисунке 5.2.

ВЫВОДЫ

Полученные результаты экспериментальных исследований эффективности метода вычислительного поиска с использованием ценовых функций стоимости показывают, что направление исследования нелинейных узлов замен является актуальным. Использование предложенных динамических весовых коэффициентов в предлагаемых функциях стоимости позволяют существенно повысить эффективность метода имитации отжига — получены лучшие известные на сегодняшний день результаты по нелинейности и автокорреляции для S-блоков 8×2. Для S-блоков 6x4 удалось поднять значение показателя нелинейности. Таким образом, разработанный вычислительный метод позволяет формировать нелинейные узлы замен с улучшенными свойствами и использовать их для совершенствования DES-подобных симметричных криптоалгоритмов.

Перспективным направлением дальнейших исследований является развитие математического аппарата криптографических недвоичных функций для задач синтеза биективных S-блоков, экспериментальные исследования эффективности предлагаемого подхода для узлов замен больших размерностей, обобщение введенных в данной работе динамических весовых коэффициентов.

В разделе ”Охрана труда и безопасность в чрезвычайных ситуациях” был проведён анализ условий труда исследователя на своём рабочем месте. Исследованы промышленная безопасность в помещении научно-исследовательской лаборатории, производственная санитария, а также производственная санитария в данном помещении. Так же была расчитана нормативная площадь световых проёмов для помещения НИЛ.

ПЕРЕЧЕНЬ ССЫЛОК

1) Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. / Б. Шнайер. – Пер. с англ.: М.: Издательство ТРИУМФ, 2002. – 816 с.
2) Сорока, Л.С. Исследование вероятностных методов формирования нелинейных узлов замен / Л.С. Сорока, А.А. Кузнецов, С.А. Исаев // Системи обробки інформації. – 2011. – Вип. 8(98). – С. 113-122.
3) Кузнецов, А.А. Математическая модель регулярных нелинейных узлов замен с использованием аппарата недвоичных криптографических функций / А.А. Кузнецов, С.А. Исаев, В.В. Фролов // Системи управління, навігації та зв'язку: збірник наукових праць. – 2012. – Вип. 3(23). – С. 81-86.
4) Головашич, С.А. Анализ эффективности проектирования алгоритмов-участников конкурса БСШ Украины [Електронний ресурс] / С.А. Головашич // Х.: ООО КРИПТОМАШ, 2009. – С. 70. – Режим доступу до журн.: http://www.cryptomach.com/upload/ru/files/bc_-design_effectiveness.pdf.
5) Biham, E. Differential cryptanalysis of DES-like cryptosystems / E. Biham, A. Shamir // Journal of Cryptology. – 1991. – 4(1). P. 3-72.
6) Burnett, L. Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography: PhD Thesis / L. Burnett. – Queensland University of Technology, 2005. – 204 p.
7) O'Connor, L. An analysis of a class of algorithms for S-box construction / L. O'Connor // Journal of Cryptology. – 1994. 7(1). P. 133-151.
8) Millan, W. How to improve the nonlinearity of bijective s-boxes / W. Millan // Information Security and Privacy, ACISP '98. – Springer Verlag, 1998. Vol. 1438. – P. 181-192.
9) Millan, W. Evolutionary Heuristics for Finding Cryptographically Strong S-Boxes / W.Millan, L. Burnett, G. Carter, A. Clark, E. Dawson // Information and communication security. – Springer, Heidelberg, 1999. Vol. 1726. – P. 263-274.
10) Clark, J.A. The Design of S-Boxes by Simulated Annealing / J.A. Clark,

J.L. Jacob, S. Stepney // New Generation Computing. – 2005. – 23(3). – P. 219-231.

11) Laskari, C. Utilizing Evolutionary Computation Methods for the Design of S-Boxes / C. Laskari, C. Meletiou, N. Vrahatis // Computational Intelligence and Security. – 2006. –Vol. 2. – P. 1299-1302.

12) Tesar, P. A new method for generating high non-linearity S-Boxes // Radioengineering. – 2010. – Part I of II, Vol. 19 Issue 1. – P. 23-26.

13) Dawson, E. Designing boolean functions for cryptographic applications / E. Dawson, W. Millan, L. Simpson // Proceedings of General Algebra Conference (AAA58). Verlag Johannes Heyn, 1999. – P. 1-22.

14) Clark, J. Evolving Boolean Functions Satisfying Multiple Criteria / J. Clark, S. Jacob, S. Stepney, M. Maitra, W. Millan. // Proceedings of INDOCRYPT'02. – Springer, 2002. LNCS Vol. 2551. – P. 246-259.

15) Kavut, S. Improved Cost Function in the Design of Boolean Functions Satisfying Multiple Criteria / S. Kavut, M.D.Yücel // Progress in Cryptology, INDOCRYPT 2003, 4th International Conference. – Springer, 2003. – Vol. 2904. – P. 121-134.

16) Kwangjo, K. Securing DES S-Boxes against Three Robust Cryptanalysis / K. Kwangjo, L. Sangjin, P. Sangjoon, L. Daiki // Proceedings of the Workshop on Selected Areas in Cryptography, SAC '95. – 1995. – P.145-157.

17) Alekseychuk, A.N. Towards a Theory of Security Evaluation for GOST-like Ciphers against Differential and Linear Cryptanalysis [Електронний ресурс] / A.N. Alekseychuk, L.V. Kovalchuk // 2011. – 24 p. – Режим доступу: http://eprint.iacr.org/2011/489.pdf.

18) Heys, H.M. Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis / H.M. Heys, S.E. Tavares // J. Cryptology – 1996. V. 9, N 1. – P. 1-19.

19) Coppersmith, D. The Data Encryption Standard (DES) and its strength against attacks / D. Coppersmith // IBM J. Res. Dev. – 1994 – P. 243-250.

20) Matsui, M. Linear cryptanalysis method for DES cipher / M. Matsui // Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765. Springer-Verlag, 1994. P. 386-397.

21) ГОСТ 12.0.003-74. ССБТ. Опасные и вредные производственные

факторы. Классификация. Введ. 1976-01-01. – М : ИПК «Изд-во стандартов», 2004. – 4 с.

22) Правила безпечної експлуатації електроустановок споживачів [Електронний ресурс] : НПАОП 40.1-1.21-98 : затв. Держнаглядохоронпраці 09.01.1998 : введ. в дію з 20.02.1998. – 1998. – 108 с. . – Режим доступу: www/ URL: http://dbn.at.ua/_ld/8/821_____.doc

23) Правила будови електроустановок. Електрообладнання спеціальних установок [Електронний ресурс] : НПАОП 40.1-1.32.01 : затв. Держнаглядохоронпраці 05.04.2001 : введ. в дію з 01.01.2002. – 2001. – Режим доступу: www/ URL: http://www.dnaop.com/html/1692.html

24) Типове положення про проведення навчання і перевірки знань з питань охорони праці [Електронний ресурс] : НПАОП 0.00-4.12-05 : затв. Держнаглядохоронпраці 26.01.2005. – 2005. – 36 с. – Режим доступу: www/ URL: http://norma.org.ua/Download/law2/15.rar

25) Санітарні норми мікроклімату виробничих приміщень [Електронний ресурс] : ДСН 3.3.6.042-99 : затв. Держнаглядохоронпраці 01.12.1999. – 1999. – 12 с. – Режим доступу: www/ URL: http://korpmet.org.ua/wordpress/wp-content/uploads/2012/04/ДСН-3.3.6.042-99-Санітарні-норми-мікроклімату-виробничих-приміщень.doc

26) Правила охорони праці при експлуатації електронно-обчислювальних машин [Електронний ресурс] : НПАОП 0.00-1.28-10 : затв. Держнаглядохоронпраці 26.03.2010. – 2010. – Режим доступу: www/ URL: http://document.ua/pravila-ohoroni-praci-pid-chas-ekspluataciyi-elektronno-obch-nor17970.html

27) Природнє і штучне освітлення : ДБН В.2.5-28-06 : чинний з 2006-10-01. – К. : Мінбуд України, 2006. – 80 с.

28) Санітарні норми виробничого шуму, ультразвуку та інфразвуку [Електронний ресурс] : ДСН 3.3.6-037-99 : затв. головн. держ. сан. лікарем України 01.12.1999. – 1999. – Режим доступу: www/ URL: http://document.ua/sanitarni-normi-virobnichogo-shumu-ultrazvuku-ta-infrazvuku-nor4878.html

ПРИЛОЖЕНИЕ А
ЛИСТИНГ РЕАЛИЗАЦИИ МЕТОДА ИМИТАЦИИ ОТЖИГА

```
1  bool SimulatedAnnealing::run(SBox &sbox, int MIL, int MaxIL,
2                               int MUL, double alpha)
3  {
4      this->init(sbox);
5
6      SBox best_solution(sbox);
7      SBox temp_F(sbox);
8      best_solution.set(sbox);
9      long double cost = get_cost(sbox);
10     long double temp_cost, cost_delta;
11     int NL_start = sbox.get_NL();
12     int AC_start = sbox.get_AC();
13     int temp_NL, temp_AC;
14
15     double T = this->T0;
16     int MFC = 0;
17     temp_F.set(sbox);
18     for (int i = 0; i < MaxIL; ++i)
19     {
20         bool changed = false;
21         for (int j = 0; j < MIL; ++j)
22         {
23             generate_neighbor(temp_F);
24             temp_cost = get_cost(temp_F);
25
26             cost_delta = temp_cost - cost;
27             bool accepted = false;
28             if (cost_delta < 0)
29                 accepted = true;
30             else
31             {
32                 double U = double(rand()) / double(RAND_MAX);
33                 if (U < exp(double(-cost_delta / T)))
34                     accepted = true;
35                 else
36                     restore_generated_neighbor(temp_F);
37             }
38             if (accepted)
39             {
40                 changed = true;
41                 cost = temp_cost;
42                 temp_NL = temp_F.get_NL();
43                 temp_AC = temp_F.get_AC();
```

```
44                  #ifdef ENABLED_WISHED_BREAK
45                  if ((temp_NL >= WISHED_NL) && (temp_AC <= WISHED_AC))
46                      #ifdef DES_CRITERIA_IN_ANNEALING
47                      if (testDES(temp_F.F))
48                      #endif
49                  {
50                      sbox.set(temp_F);
51                      return true;
52                  }
53                  #endif
54                  if ((NL_start < temp_NL) || ((NL_start == temp_NL)
55                                               && (AC_start > temp_AC)))
56                  {
57                      best_solution.set(temp_F);
58                      NL_start = temp_NL;
59                      AC_start = temp_AC;
60                  }
61              }
62
63              ++this->pos_index;
64          }//for (MIL)
65          if (!changed)
66              ++MFC;
67          else
68              MFC = 0;
69          if (MFC == MUL)
70              break;
71          T *= alpha;
72      }//for (MaxIL)
73      sbox.set(best_solution);
74      return false;
75  }
```

ПРИЛОЖЕНИЕ Б
ЛИСТИНГ ОЦЕНКИ НЕЛИНЕЙНОСТИ И АВТОКОРРЕЛЯЦИИ

```
1  int SBox::get_NL()
2  {
3      int WHT_max = 0;
4      for (int i = 0; i < this->output_combinations - 1; ++i)
5          for (int w = 0; w < this->input_combinations; ++w)
6          {
7              int sum = 0;
8              for (int x = 0; x < this->input_combinations; ++x)
9                  sum += (boolean_f[i][x] ^ __builtin_popcount(w & x) & 0x1)
10                         ? -1 : 1;
11             if (sum < 0)
12                 sum = -sum;
13             if (sum > WHT_max)
14                 WHT_max = sum;
15         }
16     return (this->input_combinations - WHT_max) >> 1;
17 }
18
19 int SBox::get_AC()
20 {
21     int max = 0;
22     for (int i = 0; i < this->output_combinations - 1; ++i)
23         for (int delta = 1; delta < this->input_combinations; ++delta)
24         {
25             int sum = 0;
26             for (int x = 0; x < this->input_combinations; ++x)
27                 sum += (boolean_f[i][x] ^ boolean_f[i][x ^ delta]) ? -1 : 1;
28             if (sum < 0)
29                 sum = -sum;
30             if (sum > max)
31                 max = sum;
32         }
33     return max;
34 }
```

ПРИЛОЖЕНИЕ В
ЛИСТИНГ ОЦЕНКИ ВЕРХНЕЙ ГРАНИЦЫ ВЕРОЯТНОСТИ ДИФФЕРЕНЦИАЛЬНОГО И ЛИНЕЙНОГО КРИПТОАНАЛИЗА ГОСТ 28147-89

```
1  void SBox::get_MD_args(int& d, int& d_)
2  {
3      d = 0;
4      d_ = 0;
5      for (int alpha = 1; alpha < this->output_combinations; ++alpha)
6          for (int beta = 1; beta < this->output_combinations; ++beta)
7          {
8              int sum_d_a0 = 0;
9              int sum_d_a1 = 0;
10             for (int k = 0; k < this->output_combinations; ++k)
11             {
12                 // delta(a, b) == (1 if a == b else 0)
13                 if ((this->F[S_index((k + alpha) & (this->output_combinations
       - 1))] ^ F[S_index(k)]) == beta)
14                     // v(k, alpha) is the carry bit
15                     if (k + alpha >= this->output_combinations)
16                         ++sum_d_a1;
17                     else
18                         ++sum_d_a0;
19             }
20             if (sum_d_a0 > d_)
21                 d_ = sum_d_a0;
22             if (sum_d_a1 > d_)
23                 d_ = sum_d_a1;
24             if (sum_d_a0 + sum_d_a1 > d)
25                 d = sum_d_a0 + sum_d_a1;
26         }
27 }
28
29 double SBox::get_MD(int cipher_round)
30 {
31     int d, d_;
32     this->get_MD_args(d, d_);
33     if (cipher_round == 0)
34         cipher_round = this->cipher_rounds_count;
35     return std::max(
36         (
37             pow(double(d) / this->output_combinations, cipher_round + 1 - 2 *
       ceil(cipher_round / 3.0))
```

```
38              * pow(double(d_) / this->output_combinations, ceil(cipher_round /
    3.0))
39          ),
40          pow(double(d) / this->output_combinations, cipher_round - 1)
41      );
42  }
43
44  void SBox::get_ML_args(int& l)
45  {
46      l = 0;
47      for (int alpha = 1; alpha < this->output_combinations; ++alpha)
48          for (int beta = 1; beta < this->output_combinations; ++beta)
49          {
50              int k_sum = 0;
51              for (int k = 0; k < this->output_combinations; ++k)
52              {
53                  int x_sum = 0;
54                  for (int x = 0; x < this->output_combinations; ++x)
55                      x_sum += ((__builtin_popcount(beta & this->F[S_index((x +
    k) & (this->output_combinations - 1))]) ^ __builtin_popcount(alpha & x)) &
    0x1) ? -1 : 1;
56                  k_sum += x_sum * x_sum;
57              }
58              if (k_sum > l)
59                  l = k_sum;
60          }
61  }
62
63  double SBox::get_ML(int cipher_round)
64  {
65      int l;
66      this->get_ML_args(l);
67      if (cipher_round == 0)
68          cipher_round = this->cipher_rounds_count;
69      return pow(
70          double(l) / this->output_combinations / this->output_combinations /
    this->output_combinations,
71          round(2.0 / 3 * cipher_round)
72      );
73  }
```

ПРИЛОЖЕНИЕ Г
ПЕРЕЧЕНЬ НАУЧНЫХ РАБОТ

1) Кузнецов, А.А. Математическая модель регулярных нелинейных узлов замен с использованием аппарата недвоичных криптографических функций / А.А. Кузнецов, С.А. Исаев, В.В. Фролов // Системи управління, навігації та зв'язку: збірник наукових праць. – 2012. – Вип. 3(23). – С. 81-86.

2) Кузнецов, А.А. Вычислительный метод синтеза регулярных нелинейных узлов замен с использованием недвоичных криптографических функций / А.А. Кузнецов, С.А. Исаев, В.В. Фролов // Системи управління, навігації та зв'язку: збірник наукових праць. – 2012. – Вип. 3(24). – С. 112-117.