Представляються матеріали по додатковому обґрунтуванню справедливості гіпотези про те, що великі шифри асимптотичне є випадковими підстановками. Порівнюються між собою кореляційні характеристики ряду сучасних шифрів і їхніх зменшених моделей. Встановлено, що за показниками статистичної безпеки українські шифри Калина, Мухомор і Лабіринт перевершують визнаного світового лідера блокового симетричного шифрування – шифр AES

Ключові слова: доказова стійкість, статистична безпека, показники випадковості моделі і прототипу, випадкова підстановка

Представляются материалы по дополнительному обоснованию справедливости гипотезы о том, что большие шифры асимптотическое являются случайными подстановками. Сравниваются между собой корреляционные характеристики ряда современных шифров и их уменьшенных моделей. Установлено, что по показателям статистической безопасности украинского шифры Калина, Мухомор и Лабиринт превосходят признанного мирового лидера блочного симметричного шифрования – шифр AES

Ключевые слова: доказуемая стойкость, статистическая безопасность, показатели случайности модели и прототипа, случайная подстановка

УДК 681.3.06: 519.248.681

БОЛЬШИЕ ШИФРЫ – СЛУЧАЙНЫЕ ПОДСТАНОВКИ. СРАВНЕНИЕ ПОКАЗАТЕЛЕЙ СТАТИСТИЧЕСКОЙ БЕЗОПАСНОСТИ БЛОЧНЫХ СИММЕТРИЧНЫХ ШИФРОВ, ПРЕДСТАВЛЕННЫХ НА УКРАИНСКИЙ КОНКУРС

И.В. Лисицкая
Доктор технических наук, доцент*
Контактный тел.: (057) 702-14-25
E-mail: ai@kture.kharkov.ua
А.А. Настенко
Аспирант*
К.Е. Лисицкий*
*Кафедра безопасности информационных технологий
Харьковский национальный университет радиоэлектроники
пр. Ленина, 16, г. Харьков, Украина, 61166

1. Введение

В числе задач проблемного характера для Украины, которые требуют решения в условиях признанной необходимости разработки и принятия национального стандарта блочного симметричного шифрования (БСШ), стоит задача разработки методик оценки показателей стойкости БСШ, которые позволяли бы в отличии от существующих подходов в реальные временные сроки получить решения (оценки), имеющие высокий уровень доверия и надёжности.

Одним из направлений сокращения временных и вычислительных затрат на проведение экспертизы предлагаемых решений может стать подход основанный на изучении и исследовании криптографических свойств уменьшенных версий шифров, – подход активно развиваемый нами в последнее время [1-4 и др.]. В процессе разработки этого подхода сформировалась новая точка зрения (новая идеология) в вопросах оценки безопасности блочных шифров к атакам дифференциального и линейного криптоанализа, которая строится на установленном в ходе исследований факте, что все современные блочные шифры после нескольких начальных циклов шифрования приобретают свойства случайных подстановок соответствующей степени.

Хотя, казалось бы, то, что хороший шифр должен быть случайной подстановкой известное в криптографической литературе положение, но полученные нами в этом направлении свидетельства и результаты воспринимаются многими специалистами неоднозначно, так как они не согласуются с имеющимися и развиваемыми в публикациях подходами и доказательствами.

Имеются в виду, прежде всего, идеи и подходы, относящиеся к понятию доказуемой стойкости.

Напомним, что, как показывает анализ [5], в основе всех известных подходов к оценке показателей стойкости блочных симметричных шифров к атакам дифференциального и линейного криптоанализа лежит процедура определения максимума среднего значения дифференциальной вероятности (MADP) (полного дифференциала) для всего шифра и максимума среднего значения вероятности линейного корпуса (MALHP), при этом полученные оценки этих показателей в разных работах отличаются в значительных пределах.

Ещё один вывод из анализа, представленного в [5], заключается в том, что показатели стойкости шифров практически во всех работах связываются с соответствующими дифференциальными и линейными показателям S-блоковых конструкций, входящих в шифры. Полагалось, что предлагаемые порой стройные теории и доказательства, цифры и результаты нельзя проверить экспериментально, так как они находились в области вычислительно нереализуемых значений.

Предложенный подход, основанный на изучении и исследовании криптографических свойств уменьшенных версий шифров, позволил преодолеть вычислительные ограничения, и оказалось, что результаты экспериментов не подтвердили доказанные положения и теоремы (практика не подтвердила теории). Существующие подходы и оценки оказались далеко не объективными.

В частности, оказалось, что показатели стойкости шифров к атакам дифференциального и линейного криптоанализа от свойств использованных в них S-блоков, не зависят.

Они определяются дифференциальными и линейными свойствами случайных подстановок соответствующей степени, к показателям которых приходит практически любой шифр после нескольких начальных циклов шифрующих преобразований. Несправедливым оказалось и утверждение, что шифры со случайными ключами асимптотически приходят к равномерным распределениям дифференциалов и смещений. Сделан также вывод, о том, что неаккуратным является и деление шифров на марковские и немарковские, а также сами используемые показатели стойкости в виде MADP и MALHP не являются адекватными решаемым задачам.

Основные аргументы возражений против выдвигаемых нами положений сосредоточились на сомнениях в том, что большие шифры асимптотически являются случайными подстановками – положении, которое, казалось бы, не противоречит даже здравому смыслу. Поэтому нами были предприняты исследования для подтверждения гипотезы, что и большие шифры тоже ″асимптотически″ приходят к случайным подстановкам (являются случайными подстановками). В частности, в наших работах [6,7] было показано, что большие версии шифров (Rijndael, ГОСТ 28147-89 и Fox) при использовании их в режиме зашифрования укороченных (16-битных и 32-х битных) блоков данных повторяют законы распределения вероятностей переходов XOR таблиц и таблиц смешений линейных аппроксимаций, свойственные соответствующим законам распределения вероятностей случайных подстановок.

Продолжая развивать это направление, в настоящей работе мы представляем материалы по дополнительному обоснованию справедливости отмеченной выше гипотезы. Теперь сравниваются между собой корреляционные характеристики ряда современных шифров и их уменьшенных моделей. В их числе будут рассмотрены шифры, представленные на украинский конкурс, а также финалист конкурса AES шифр Rijndael (AES). Мы, кроме того, рассмотрим и корреляционные свойства шифра ГОСТ 28147-89, как представителя уходящей в прошлое технологии построения БСШ.

2. Показатели статистической безопасности

До сих пор полагается, что статистические испытания являются единственной стратегией испытания больших криптографических систем с секретными ключами, построенных в виде чередующихся слоёв блоков замен и перестановок [8], как это сделано в шифрах Rijndael, Serpent, ГОСТ и мн.др. Это объясняется трудностью составления систем уравнений, связывающих входы и выходы таких систем, и практической невозможностью их решения сегодня строгими аналитическими методами, ввиду большой размерности получающихся систем уравнений, далеко превосходящей вычислительные возможности современных компьютеров.

В этой работе статистические испытания и станут основным инструментом исследований. Мы здесь говорим до сих пор, имея теперь в виду отмеченный выше новый подход к оценке показателей стойкости блочных симметричных шифров, основанный на изучении показателей случайности уменьшенных моделей прототипов [5], обоснованию которого и посвящена настоящая работа.

Следует заметить, что статистические методы оценки криптографических показателей шифров уже получили достаточно широкое распространение в современных технологиях блочного симметричного шифрования. Это и тесты NIST STS, и оценка лавинных характеристик шифров, рассматриваемая в виде отдельного метода, и измерение корреляционных показателей шифров, как подстановочных преобразований.

Эти методы широко применялись и при оценке показателей шифров, представленных на прошедших конкурсах.

В этой работе мы будем следовать методике анализа показателей статистической безопасности, изложенной в работе [9], с помощью которой оцениваются корреляционные свойства блочных симметричных шифров, как управляемых ключами перестановок.

Здесь мы рассмотрим такие показатели статистической безопасности, как:

- среднее число выходных битов, которые изменяются, когда изменяется один входной бит (лавинный эффект);
- степень полноты (d_c);
- степень лавинного эффекта (d_a);
- степень строгого лавинного критерия (d_{sa}).

Они будут рассматриваться для различного числа циклов и случайно взятых ключей зашифрования.

Напомним здесь определения этих показателей в трактовке работы [8].

Пусть для вектора $x=(x_1,x_2,\dots,x_n\in(GF(2))^n$ вектор $x^{(i)}\in(GF(2))^n$ обозначает вектор, полученный дополнением i-того бита (для $i=1,\dots,n$). $(f(x))_j$ – обозначает выделение j-того бита вектора $f(x)$. Хэмминговый вес $w(x)$ вектора x определяется как число ненулевых компонент этого вектора.

Говорят, что функция $f:(GF(2))^n\to(GF(2))^m$, отображающая n входных бит в m выходных бит является полной (совершенной), если каждый выходной бит зависит от каждого входного бита, т.е.

$\forall i=1,\dots,n \quad \forall j=1,\dots,n \quad \exists x\in(GF(2))^n$ такое, что $\left(f(x^{(i)})\right)_j\neq(f(x))_j$.

Функция $f:(GF(2))^n \to (GF(2))^m$ обладает лавинным эффектом, если в среднем $\frac{1}{2}$ выходных битов изменяется, когда изменяется любой одиночный бит входа, т.е. когда

$$\frac{1}{2^n}\sum_{x\in(GF(2))^n} w\left(f(x^{(i)})-f(x)\right)=\frac{m}{2},$$

для всех $i=1,\ldots,n$.

Функция $f:(GF(2))^n \to (GF(2))^m$ удовлетворяет строгому лавинному критерию, если каждый выходной бит изменяется с вероятностью $\frac{1}{2}$, когда дополняется (изменяется) любой одиночный бит входа, т.е.

$$\forall i=1,\ldots,n \quad \forall j=1,\ldots,n \quad \Pr\left((f(x^{(i)})_j \neq (f(x))_j\right)=\frac{1}{2}.$$

Для определения соответствующих корреляционных характеристик вводятся две матрицы A и B.

Матрица зависимостей входов и выходов функции $f:(GF(2))^n \to \ \to (GF(2))^m$ есть $n\times m$ матрица A, у которой (i,j) элемент a_{ij} обозначает число входов для которых дополнение i-того входного бита приводит к изменению j-того выходного бита, т.е.

$$a_{ij}=\#\left\{x\in(GF(2))^n \middle| \left(f(x^{(i)})\right)_j \neq \left(f(x)\right)_j\right\}$$

для $i=1,\ldots,n$ и $j=1,\ldots,m$.

Матрица расстояний функции

$$f:(GF(2))^n \to (GF(2))^m$$

есть $n\times m+1$ матрица B, у которой элемент b_{ij} обозначает число входов для которых дополнение (изменение) i-того входного бита приводит к изменению j выходных битов, т.е.

$$b_{ij}=\#\left\{x\in(GF(2))^n \middle| w\left(f(x^{(i)})-f(x)\right)=j\right\}$$

для $i=1,\ldots,n$ и $j=1,\ldots,m$.

Конечно, если число входных битов мало, то можно подсчитать матрицу зависимостей и матрицу расстояний для всего возможного числа входов. Поэтому для шифров обычно рассматривается некоторое "подходящее" число случайно выбранных входов.

Матрица зависимостей и матрица расстояний также определяются как

$$a_{ij}=\#\left\{x\in X \middle| \left(f(x^{(i)})\right)_j \neq \left(f(x)\right)_j\right\},$$

$$a_{ij}=\#\left\{x\in(GF(2))^n \middle| \left(f(x^{(i)})\right)_j \neq \left(f(x)\right)_j\right\},$$

$$b_{ij}=\#\left\{x\in X \middle| w\left(f(x^{(i)})-f(x)\right)=j\right\}$$

для $i=1,\ldots,n$ и $j=1,\ldots,m$, где X "подходящее" случайно выбранное подмножество $(GF(2))^n$.

Проверка показателей статистической безопасности шифра начинается с построения матрицы зависимости A и матрицы расстояний B шифра, описываемого функцией $f:(GF(2))^n \to (GF(2))^m$ для множества из X входов, где X является само множество $(GF(2))^n$ или случайно выбранное подмножество множества $(GF(2))^n$.

Если такие матрицы построены, то степень полноты определяется как:

$$d_c=1-\frac{\#\left\{(i,j)\middle|a_{ij}=0\right\}}{nm}.$$

Степень лавинного эффекта определяется как

$$d_a=1-\frac{\sum_{i=1}^{n}\left|\frac{1}{\#X}\sum_{j=1}^{m}2jb_{ij}-m\right|}{nm}.$$

Степень строгого лавинного критерия определяется как

$$d_{sa}=1-\frac{\sum_{i=1}^{n}\sum_{j=1}^{m}\left|\frac{2a_{ij}}{\#X}-1\right|}{nm}.$$

Функции (шифры), имеющие хорошую степень полноты, хороший лавинный эффект и удовлетворяющие строгому лавинному критерию, отмечается в работе [9], должны иметь значения d_c, d_a и d_{sa} удовлетворяющие условиям: $d_c \approx 1$, $d_a \approx 1$, $d_{sa} \approx 1$.

3. Методика обработки результатов статистических экспериментов

Применяемая далее методика строится на последовательном использовании расчётных соотношений представленных выше для обработки результатов статистических экспериментов по определению интересующих нас показателей.

Первая часть экспериментов связана с оценкой показателей глубины лавинного эффекта для больших и малых моделей шифров, которая определяется числом циклов шифра, после которого изменение любого бита на его входе приводит к изменению в среднем половины выходных битов.

В нашем случае, во избежание нивелирования различий между отдельными битами, лавинный эффект считался не в виде среднего значения по всем битам, как в [9], а по каждому биту отдельно, и среди полученных значений для каждого бита выбиралось минимальное и максимальное значение. Если брать среднее по этим значениям, то получим результаты, практически повторяющие [9]. Они будут представлены в отдельных колонках таблиц.

Здесь сразу возникает вопрос, каким образом определять номер цикла, после которого можно считать, что изменение входного бита, влияет сразу на все выходные биты цикла?

С одной стороны, математическим свидетельством влияния изменения бита в открытом тексте одновременно на все выходные биты цикла является ортогональность (некоррелированность) зашифрованных текстов, соответствующих отличающимся на один бит открытым текстам, т.е. среднее значение числа изменившихся бит в зашифрованных текстах должно

быть равным $m_w = 64$ (для 128-ми битного шифра), $m_w = 32$ (для 64-ёх битного шифра) или $m_w = 8$ (для 16-ти битного шифра).

Действительно, если, например, рассматривать чисто случайный 64-битный блок (состоящий из независимых и равновероятных двоичных символов с вероятностью каждого однобитного значения $p_0 = \frac{1}{2}$), то, представляется очевидным, что закон распределения числа ненулевых (нулевых) битов в таких блоках будет биномиальным с параметрами

$$m_w = np_0 = 64 \cdot \frac{1}{2} = 32,$$

$$\sigma_w^2 = np_0(1-p_0) = 64 \cdot \left(\frac{1}{2}\right)^2 = 16.$$

Напомним здесь, что при значении $np_0(1-p_0) \geq 10$ биномиальное распределение с высокой степенью приближения аппроксимируется нормальным законом распределения вероятностей (формула Муавра Лапласа [10]).

С другой стороны, формируемые оценки m_w являются случайными и редко равны точно в данном случае 32.

Однозначный ответ на поставленный выше вопрос можно получить, если воспользоваться методом доверительных интервалов, являющимся методом математической статистики, специально предназначенным для построения множества приближенных значений неизвестных параметров вероятностных распределений [10].

Мы уже освещали сущность этого подхода при изучении лавинных показателей шифра ГОСТ [11].

В соответствии с изложенным в [11] подходом, задаваясь доверительной вероятностью $P_0(\theta_1,\theta_2) = 0,999 \rightarrow \alpha = 0,001$, на основании таблицы распределения Стьюдента [10] для заданных значений α и n = 10000 (объём выборки из входных текстов в наших опытах) и дисперсии нормально распределённой генеральной совокупности для 128-битных версий шифров равной $\sigma_w^2 = 32$, для 4-битных шифров $\sigma_w^2 = 16$ и для 16-битных моделей шифров $\sigma_w^2 = 4$, полагая $S^2 \approx \sigma_w^2$, получим соответственно:

$$\frac{t \cdot S}{\sqrt{n}} = \frac{3,291 \cdot 5,656}{\sqrt{10000}} = 0,1861; \frac{t \cdot S}{\sqrt{n}} = \frac{3,291 \cdot 4}{\sqrt{10000}} = 0,13164;$$

$$\frac{t \cdot S}{\sqrt{n}} = \frac{3,291 \cdot 2}{\sqrt{10000}} = 0,06582,$$

и, следовательно, можно считать попавшими в доверительные интервалы все значения m_w, удовлетворяющие соответственно условиям:

$$64 - 0,1861 \leq m_w \leq 64 + 0,1861;$$

$$32 - 0,131 \leq m_w \leq 32 + 0,131;$$

$$8 - 0,066 \leq m_w \leq 8 + 0,066.$$

Аналогичным образом можно выполнить оценки параметров распределений при обработке результатов других корреляционных показателей.

Далее излагаются уже результаты выполненных исследований.

4. Результаты экспериментальных исследований показателей статистической безопасности

Исследования проводились с малыми 16-ти битными моделями шифров и их большими прототипами. Описание малых моделей шифров, рассмотренных в работе, можно найти в [1-4]. Программные реализации "больших" шифров, представленных на украинский конкурс, заимствованы из [12-15].

В табл. 1 представлены результаты оценки показателей статистической безопасности шифра Калина (полная версия).

Таблица 1

Поцикловые значения показателей статистической безопасности шифра Kalina (полная версия, 128 бит блок и 256 бит ключ)

Цикл №	Kalina (полная версия, 128 бит блок и 256 бит ключ)							
	M_{min}	D_{min}	M_{max}	D_{max}	m_w	d_c	d_a	d_{sa}
1	31,9423	16,0136	32,2046	16,0136	32,0863	0,5	0,49467	0,495205
2	63,868	31,8812	64,1539	31,8812	64,0109	1	0,992067	0,992018
3	63,8827	32,0289	64,1232	32,0289	64.0029	1	0,992037	0,992073
4	63,8555	31,641	64,1486	31,641	64,0020	1	0,99204	0,991959
5	63,8543	32,1099	64,1617	32,1099	64,008	1	0,992134	0,991966
6	63,8537	31,9269	64,2011	31,9269	64,0274	1	0,992038	0,991984
7	63,8119	31,9275	64,1172	31,9275	63,9645	1	0,992031	0,991999
8	63,762	32,1172	64,1822	32,1172	63,9721	1	0,99212	0,992027
9	63,878	32,2575	64,1819	32,2575	64,0299	1	0,992007	0,992087
10	63,8029	33,1195	64,167	33,1195	63,9849	1	0,992019	0,992064
11	63,8367	31,1654	64,1499	31,1654	63,9933	1	0,992047	0,992045
12	63,816	31,7851	64,143	31,7851	63,9795	1	0,991968	0,991942
13	63,8177	31,9403	64,1221	31,9403	63,9699	1	0,991911	0,992075
14	63,852	31,9271	64,1362	31,472	63.9941	1	0,99204	0,992012

В этой и других таблицах использованы обозначения: M_{min} – минимальное значение математического ожидания количества изменившихся бит для некоторого бита на входе; M_{max} – максимальное значение математического ожидания количества изменившихся бит для некоторого бита на входе; D_{min} и D_{max} – дисперсии числа изменившихся бит при побитной оценке минимумов и максимумов средних значений, m_w – среднее число изменившихся бит, которое здесь вычисляется как

$$m_w = \frac{M_{min} + M_{max}}{2}.$$

Из представленных данных следует, что глубина лавинного эффекта для шифра Kalina 128/256 (полная версия, 128 бит блок и 256 бит ключ) равна 2-ум циклам. Начиная со второго цикла, значение m_w попадает в установленные границы. Естественно, что результат для нашего среднего значения m_w является несколько завышенным по сравнению с глобальным средним значением, но он показывает более тонкую (побитную) структуру формирования лавинных показателей.

Видно также, что однобитные значения максимумов и минимумов оказываются весьма близкими к среднему значению. Другие показатели статистической безопасности и большого и малого шифров, начиная со второго цикла, также укладываются в нужные границы.

В табл. 2 представлены показатели статистической безопасности уменьшенной версии шифра Калина.

Как следует из представленных результатов, и большая и малая версии шифров ведут себя практически одинаково, разве лишь получается, что для малой версии процесс перехода к стационарному состоянию затягивается на один дополнительный цикл (большая Калина входит в границы доверительного интервала на втором цикле, а малая версия – на третьем).

Заметим здесь, что значения дисперсий и для большой и для малой версий шифров с большой точностью удовлетворяют использованному выше при определении доверительных интервалов условию. Как мы увидим далее, и во всех последующих экспериментах значения дисперсий, будут весьма близкими к теоретическим значениям. Можно отметить, что значения дисперсий в стационарном режиме укладываются в границы $\left|\{D_{min}, D_{max}\}\right| \le 0{,}11$ для 128-битных версий шифров и $\left|\{D_{min}, D_{max}\}\right| \le 0{,}07$ для 16-битных версий.

В табл. 3 и табл. 4 представлены уже показатели статистической безопасности большой и малой версии шифра Мухомор.

Таблица 2

Поцикловые значения показателей статистической безопасности шифра mini-Kalina

Цикл №	Kalina (мини-версия)							
	M_{min}	D_{min}	M_{max}	D_{max}	m_w	d_c	d_a	d_{sa}
1	4,0508	1,47762	4,4784	1,91513	4,2646	0,5	0,52646	0,45980
2	8,4219	3,1135	8,6301	3,17267	8,526	1	0,93167	0,93410
3	7,9089	3,9117	7.99	3,9824	7,94945	1	0,99602	0,98949
4	7,9536	3,91176	8,029	4,04145	7,9913	1	0,99799	0,9906
5	7,9844	3,95436	8,0507	3,98133	8,01755	1	0,99707	0,99077
6	7,9638	3,99289	8,0601	4,12949	8,01195	1	0,99826	0,99147
7	7,9707	4,01324	8,0426	4,07299	8,00665	1	0,99703	0,99098
8	7,9556	4,00221	8,0836	4,09403	8,0196	1	0,99733	0,99124
9	7,9729	3,95417	8,0503	3,96717	8,0116	1	0,99722	0,99087
10	7,9449	3,87109	8,0375	3,96166	7,9912	1	0,99816	0,99131

Таблица 3

Поцикловые значения показателей статистической безопасности шифра Muhomor

Цикл №	Muhomor 128/256 (полная версия)							
	M_{min}	D_{min}	M_{max}	D_{max}	m_w	d_c	d_a	d_{sa}
1	63,8699	31,8784	64,1345	32,5338	64,0022	1	0,999263	0,99203
2	63,8373	32,96	64,1439	31,0942	63,9906	1	0,999293	0,991993
3	63,8829	32,1558	64,1827	32,2213	64,0328	1	0,9993	0,992035
4	63,807	32,5806	64,1754	32,4144	63,9912	1	0,999247	0,99204
5	63,8868	31,9398	64,1385	31,4805	64,01265	1	0,999243	0,991908
6	63,826	32,3273	64,1348	32,4362	63,9804	1	0,999329	0,992026
7	63,8657	32,0441	64,1987	31,917	64,0322	1	0,999287	0,99201
8	63,8568	31,8119	64,1248	32,2994	63,9908	1	0,999268	0,992064
9	63,858	32,2152	64.1136	31,7231	63,9858	1	0,99933	0,991976
10	63,8566	32,647	64,1528	31,7147	64,0047	1	0,999389	0,992085
11	63,8657	31,8967	64,1279	31,4871	63,9968	1	0,999345	0,992004

С точностью до первого цикла поведение показателей шифра mini Muhomor (мини-версии) совпадает с поведением Muhomor-a 128/256 (полная версия). Следует здесь отметить, что в малой версии шифра Muhomor, результаты измерения показателей статистической безопасности которого представлены в табл. 4, не удаётся повторить в уменьшенном масштабе SL преобразование (оно было заменено полубайтовой подстановкой), поэтому малая версия шифра это приближение, но как показывают результаты это приближение достаточно хорошее. Интересно отметить, что и большая и малая версии шифра Muhomor входят в границы доверительных интервалов прямо с первого цикла.

Следующие результаты исследований относятся к ещё одному шифру, представленному в своё время на украинский конкурс, который получил название Лабиринт (Labyrinth). Эксперименты с этим шифром, результаты которых представлены в табл. 5 и табл. 6, практически повторяют соответствующиерезультаты,

Таблица 4

Поцикловые значения показателей статистической безопасности шифра mini-Muhomor

Цикл №	Muhomor (мини-версия)							
	M_{min}	D_{min}	M_{max}	D_{max}	m_w	d_c	d_a	d_{sa}
1	7,5117	6,88286	8,5087	3,63012	8,0102	1	0,981017	0,91618
2	7,9389	3,91637	8,045	3,93337	7,99195	1	0,995898	0,986245
3	7,9483	3,89383	8,0416	3,94227	7,99495	1	0,997069	0,990842
4	7,9723	4,07833	8,041	4,10192	8,00665	1	0,996814	0,991684
5	7,9778	3,98811	8,0334	4,02848	8,0056	1	0,997751	0,991359
6	7,9672	4,03392	8,03	4,0777	7,9986	1	0,997938	0,991227
7	7,963	4,07643	8,0355	3,94344	7,99925	1	0,997667	0,991181
8	7,9718	4,0004	8,0337	3,89456	8,00275	1	0,997813	0,992023
9	7,9502	4,11352	8,0395	4,06454	7,99485	1	0,997891	0,990234
10	7,9654	4,0546	8,0174	4,0309	7,9914	1	0,998399	0,991056

Таблица 5

Поцикловые значения показателей статистической безопасности основной версии шифра Labyrinth

Цикл №	Labyrinth 128/256 (полная версия)							
	M_{min}	D_{min}	M_{max}	D_{max}	m_w	d_c	d_a	d_{sa}
1	63,8295	31,3928	64,2159	31,8043	64,0227	1	0,999286	0,992042
2	63,8169	32,3568	64,2089	30,8193	64,0129	1	0,999284	0,991996
3	63,8568	31,8683	64,154	32,6777	64,0054	1	0,999294	0,991936
4	63,866	31,726	64,1693	32,2984	64,01765	1	0,99933	0,992042
5	63,8372	32,5633	64,1745	31,7706	64,00585	1	0,999239	0,991995
6	63,8119	32,6301	64,1028	32,1988	63,95735	1	0,999232	0,992094
7	63,86	31,39	64,1365	32,1729	63,99825	1	0,999265	0,992034
8	63,8634	31,5789	64,1692	31,7576	64,0163	1	0,999277	0,992035

Таблица 6

Поцикловые значения показателей статистической безопасности шифра mini Labyrinth

Цикл №	Labyrinth (мини-версия)							
	M_{min}	D_{min}	M_{max}	D_{max}	m_w	d_c	d_a	d_{sa}
1	7,9033	4,22695	8,2194	3,49846	8,06135	1	0,986825	0,976955
2	7,9307	3,9381	8,0483	3,95737	7,9895	1	0,997285	0,989624
3	7,9608	3,98686	8,0535	3,87164	8,00715	1	0,997862	0,991661
4	7,9649	4,03127	8,0361	3,9134	8,0005	1	0,998221	0,990859
5	7,9537	4,04096	8,0191	4,05794	7,9864	1	0,997896	0,990595
6	7,9211	4,13207	8,055	4,06078	7,98805	1	0,997234	0,990575
7	7,9444	4,10391	8,0448	3,88039	7,9946	1	0,997234	0,990879
8	7,953	4,05359	8,0475	3,95844	8,00025	1	0,997812	0,991162

полученные для шифра Мухомор (Muhomor). Показатели статистиче ской безопасности и для большой и для малой версий шифра с первого цикла попадают в соответствующие границы доверительных интервалов. И для этого шифра средние значения дисперсий также укладываются в установленные границы доверительных интервалов.

Заметим, что рассмотренные шифры по спецификациям имеют Мухомор-128 – 11 циклов зашифрования, Лабиринт – 8 циклов, Калина 128/254 – 14 циклов, ADE 128/128 – 10 циклов. Результаты экспериментов привязаны к этим показателям.

В табл. 7 и табл. 8 представлены результаты экспериментов с шифром ADE (128/128), также принявшем участие в украинском конкурсе.

Как следует из приведенных данных, этот шифр по лавинным показателям для большой версии оказался вышедшим далеко за допустимые пределы, в то время как для малой модели шифр начиная с третьего цикла вошёл в границы доверительного интервала. Наблюдается сильная зависимость результатов для большого шифра от мастер-ключа. Есть даже ключи, на которых шифр не входит в границы доверительного интервала на полном наборе циклов (при 10-ти циклах). Заметим здесь, что подсчёт глобального среднего значения не позволяет выделить замеченного дефекта (минимальных значений среди общего числа средних мало). Поэтому не удивительно, что другие корреляционные показатели как для этого шифра, как для малой, так и для большой его версии оказываются в допустимых границах. Здесь уместно напомнить результаты работы [16], посвящённой анализу этого алгоритма шифрования. В этой работе сделан вывод, что в алгоритме ADE существует значительное количество слабых ключей, при использовании которых алгоритм обладает серьёзной уязвимостью (128-битный шифр работает как 4 независимых 32-битных шифра, и структура открытого текста полностью отображается в структуру шифртекста). В результате получается, что модель малого шифра свойства большого прототипа. И можно понять почему. В большой версии в преобразовании ShiftRows состояния сдвигаются на различное количество позиций, задаваемых значениями раундового ключа (пункт 4.3.2 спецификации). Пары байтов циклового ключа $\{\lambda_j^*, \lambda_{j+1}^*\}$ после модульного сложения с соответствующим значением сдвига строки в алгоритме AES определяют значение сдвига в алгоритме ADE [16].

Таблица 7

Поцикловые значения показателей статистической безопасности шифра ADE

Цикл №	ADE (полная версия)							
	M_{min}	D_{min}	M_{max}	D_{max}	m_w	d_c	d_a	d_{sa}
1	1	0	1	0	1	0,01	0,01562	0
2	15,9756	8,12667	64,3864	27,5943	40,180	0,75	0,99603	0,49598
3	16,0261	7,91822	64,3434	29,3967	40,184	0,75	0,75186	0,74343
4	31,9029	16,3167	64,1253	32,0766	48,014	1	0,99936	0,99201
5	31,9814	16,0193	64,1364	31,8304	48,058	1	0,99929	0,99201
6	31,9662	15,7563	64,1411	31,1996	48,053	1	0,99929	0,99203
7	31,9793	15,8435	64,1587	32,1006	48,069	1	0,99928	0,99196
8	63,8636	48,5338	64,2071	31,765	64,035	1	0,99935	0,99206
9	31,9906	16,3077	64,1873	32,0361	48,047	1	0,99933	0,99211
10	63,8852	31,5844	64,1127	32,04	64,02	1	0,99924	0,99216

Таблица 8

Поцикловые значения показателей статистической безопасности шифра мини ADE

Цикл №	ADE (мини-версия)							
	M_{min}	D_{min}	M_{max}	D_{max}	m_w	d_c	d_a	d_{sa}
1	3,9826	1,2423	5,0205	1,24108	4,50155	0,5	0,523902	0,376323
2	8,4122	4,94269	8,8114	4,75323	8,6118	1	0,938238	0,908982
3	7,9272	3,8627	7,9736	4,1199	7,9454	1	0,995636	0,988745
4	7,9709	4,00185	8,045	4,02598	8,00795	1	0,997513	0,991304
5	7,9525	3,89484	8,048	4,0319	8,00025	1	0,997477	0,991226
6	7,9678	3,89256	8,0291	3,93465	7,99845	1	0,997556	0,991503
7	7,9699	3,94199	8,0572	3,99293	8,01355	1	0,996935	0,990659
8	7,942	3,95664	8,0367	3,97995	7,98935	1	0,998345	0,991035
9	7,9525	3,95444	8,025	4,01237	7,98875	1	0,997405	0,991227
10	7,9504	3,97154	8,0314	4,09221	7,9909	1	0,998283	0,991027

В то же время в малой версии ADE MixColumn выполнена умножением на матрицу размера 4×4, т.е. идёт перемешивание всех четырёх полубайтов (операции ShiftRows и не требуется, она лишняя) [17].

Поэтому если в большой версии шифра с вероятностью 1/4 может возникать ситуация, когда сдвиг равен нулю, то в мини ADE сдвиг всегда сохраняется ненулевым. Этим и объясняется отличие в представленных результатах.

Далее мы хотим представить результаты по оценке показателей статистической безопасности всем хорошо известного и всё ещё сохраняющего реальное практическое применение стандарта шифрования СССР ГОСТ 28147-89 (см. табл. 9 и табл. 10).

Примечательно, что малая версия этого шифра практически повторяет поцикловое поведение всех показателей статистической безопасности большого прототипа.

И в том и в другом случае глубина лавинного эффекта оказывается близкой к 9-10 циклам, что хорошо согласуется с известными из литературы данными [18].

Малая модель наглядно демонстрирует повторение поведения показателей прототипа.

Наконец, в табл. 11 и табл. 12 представляются показатели статистической безопасности 128-битной версии шифра AES 256, как признанного лидера среди блочных симметричных шифров.

Таблица 9

Поцикловые значения показателей статистической безопасности шифра GOST

Цикл №	GOST (полная версия)							
	M_{min}	D_{min}	M_{max}	D_{max}	m_w	d_c	d_a	d_{sa}
1	1	0	5,2316	1,5478	3,1158	0,1103	0,0719	0,0289
2	2,5224	0,7389	11,176	8,5079	6,8494	0,4402	0,1771	0,1222
3	6,0662	3,6210	17,126	12,994	11,596	0,7883	0,3166	0,2645
4	10,043	10,555	23,217	24,149	16,630	0,9568	0,4948	0,4511
5	15,184	19,594	27,901	22,534	21,543	0,9973	0,6798	0,6328
6	21,673	30,089	31,376	17,769	26,524	1	0,8389	0,8246
7	26,450	29,259	31,910	16,195	29,180	1	0,9441	0,9344
8	30,108	20,970	31,977	16,135	31,043	1	0,9820	0,9766
9	31,558	17,031	32,061	16,054	31,810	1	0,9960	0,9899
10	31,871	16,24	32,077	16,021	31,974	1	0,9989	0,9919
11	31,899	16,034	32,086	15,980	31,993	1	0,9990	0,9917
12	31,901	16,231	32,084	16,125	31,993	1	0,9990	0,9920
...	...	...	...	...	...	...	...	...
32	31,907	15,819	32,074	16,176	31,990	1	0,9990	0,9919

Таблица 10

Поцикловые значения показателей статистической безопасности шифра мини GOST

Цикл №	GOST (мини-версия)							
	M_{min}	D_{min}	M_{max}	D_{max}	m_w	d_c	d_a	d_{sa}
1	1	0	3,7133	1,8353	2,35665	0,25	0,25555	0,10702
2	2,901	0,74171	6,601	4,5677	4,7515	0,6406	0,53116	0,40306
3	4,559	6,46861	7,284	4,8631	5,922	0,9375	0,74522	0,73526
4	6,172	6,40994	7,910	4,0530	7,0414	1	0,88696	0,86999
5	7,072	5,46801	7,840	4,4406	7,4566	1	0,93987	0,92109
6	7,478	5,35793	7,921	4,2227	7,6998	1	0,96687	0,95706
7	7,609	4,99883	7,975	4,0449	7,7924	1	0,98231	0,97728
8	7,805	4,52547	8,021	4,0686	7,9133	1	0,99271	0,98286
9	7,879	4,4407	7,990	4,1024	7,9349	1	0,99558	0,98732
10	7,946	4,11679	8,026	4,0018	7,9864	1	0,99527	0,99028
11	7,953	4,06805	8,031	3,9379	7,9887	1	0,99750	0,99049
12	7,969	4,14766	8,023	4,0195	7,9964	1	0,99805	0,99083
...	...	...	...	...	...	...	...	...
32	7,959	3,99812	8,043	3,9270	8,0011	1	0,99734	0,99143

Таблица 11

Поцикловые значения показателей статистической безопасности шифра AES 128/256

Цикл №	AES 128/256 (полная версия)							
	M_{min}	D_{min}	Mmax	D_{max}	m_w	d_c	d_a	d_{sa}
1	15,7607	16,604	16,5318	13,4396	16,14925	0,25	0,253308	0,23655
2	64,0415	66,9514	64,4935	66,1048	64,2675	1	0,996076	0,99070
3	63,827	31,8389	64,1385	31,8065	63,98275	1	0,999353	0,99207
4	63,8199	32,1553	64,1484	31,8878	63,98415	1	0,999307	0,99207
5	63,7944	32,7001	64,133	32,1005	63,9637	1	0,999337	0,99205
6	63,8825	31,7803	64,153	31,9256	64,01775	1	0,999329	0,992012
7	63,8536	31,3078	64,1394	32,0058	63,9965	1	0,999266	0,99198
8	63,8399	32,2379	64,1196	31,5861	63,97975	1	0,999342	0,99208
9	63,7888	32,0618	64,1819	31,247	63,98535	1	0,999268	0,99208
10	63,8527	31,8646	64,1416	31,7809	63,99715	1	0,999292	0,99202
11	63,8936	31,6963	64,1122	31,9582	64,0029	1	0,999279	0,99203
12	63,8302	32,6242	64,156	30,9783	63,9931	1	0,99928	0,99195
13	63,8567	32,5672	63,8302	32,6242	63,84345	1	0,99936	0,99195
14	63,8475	32,175	64,1333	31,8389	63,9904	1	0,999342	0,99200

Таблица 12

Поцикловые значения показателей статистической безопасности шифра mini-AES 256

Цикл №	AES mini (мини-версия)							
	M_{min}	D_{min}	M_{max}	D_{max}	m_w	d_c	d_a	d_{sa}
1	3,738	3,9520	4,269	3,4705	4,0041	0,5	0,49941	0,41955
2	8,302	4,6147	8,508	4,8911	8,4055	1	0,95024	0,90200
3	7,936	3,6321	7,991	3,7956	7,9638	1	0,99557	0,98789
4	7,923	4,0740	8,044	4,1274	7,9843	1	0,99717	0,99136
5	7,942	3,9918	8,033	3,9618	7,9876	1	0,99776	0,99046
6	7,947	4,0382	8,046	3,9926	7,997	1	0,99707	0,99100
7	7,965	3,9969	8,040	4,0576	8,003	1	0,99756	0,99085
8	7,964	4,0106	8,055	4,1011	8,0100	1	0,99768	0,99067
9	7,965	4,0280	8,075	4,0014	8,0206	1	0,99728	0,98986
10	7,970	4,0928	8,037	4,0799	8,0042	1	0,99768	0,99095
11	7,9607	3,95896	8,0291	3,98745	7,9949	1	0,997893	0,990334
12	7,9648	3,89756	8,0498	4,10952	8,0073	1	0,997303	0,989963
13	7,9579	3,98533	8,0481	4,05479	8,003	1	0,99747	0,991055
14	7,9813	3,92815	8,0226	4,03549	8,00195	1	0,997995	0,990114

Обращает на себя внимание то, что по показателям статистической безопасности шифр AES уступает трём шифрам, представленным на украинский конкурс: Калине, Мухомору и Лабиринту. И лавинные и другие корреляционные показатели у него оказываются хуже, чем у этих шифров.

5. Выводы

Представленные результаты однозначно свидетельствуют, что малые модели всех рассмотренных в работе шифров: Rijndael, ГОСТ и шифров, представленных на украинский конкурс: Мухомор, Калина, ADE, Лабиринт практически повторяют корреляционные характеристики своих прототипов. Тем самым подтверждается гипотеза о том, что можно построить малые модели шифров, повторяющие поведение показателей случайности своих больших аналогов, а, следовательно, выводы, полученные для малых моделей можно переносить на большие версии шифров.

В частности, это касается вывода о том, что и малые и большие шифры асимптотически приобретают свойства случайных подстановок.

Получены дополнительные аргументы и свидетельства в пользу справедливости предлагаемой в [5] методики оценки показателей стойкости блочных симметричных шифров на основе изучения показателей стойкости их уменьшенных моделей.

Корреляционные показатели по динамике их изменений в этом отношении практически повторяют результаты, полученные ранее при изучении дифференциальных и линейных свойств малых и больших моделей шифров [1-6].

В качестве дополнительного результата, выходящего за рамки задач исследований работы, можно отметить подтверждение дефекта в конструкции шифра ADE. Он не прошёл тест по лавинным характеристикам.

Одновременно следует отметить, что удалось доказать, что остальные шифры, представленные на украинский конкурс, продемонстрировали более высокие криптографические показатели чем признанный лидер блочного симметричного шифрования – шифр AES (Rijndael). Украинские шифры (три из четырёх) оказались более совершенными.

Общий вывод, который можно сделать по результатам работы, состоит в том, что полностью подтверждается гипотеза, что и большие шифры асимптотически становятся случайными подстановками, причём при увеличении размеров входного блока данных шифры приобретают свойства случайных подстановок скорее (на один-два цикла).

Литература

1. Долгов, В.И. Исследование циклических и дифференциальных свойств уменьшенной модели шифра Лабиринт. [Текст] / В.И. Долгов, И.В. Лисицкая, А.В. Григорьев, А.В. Широков // Прикладная радиоэлектроника. – 2009. – Т.8, №3 – С. 283-289.
2. Долгов, В.И. Исследование дифференциальных свойств мини-шифров Baby-ADE и Baby-AES. / В.И. Долгов, А.А. Кузнецов, Р.В. Сергиенко, О.И. Олешко // Прикладная радиоэлектроника. – 2009.– Т.8, №.3. – С. 252-257.
3. Долгов, В.И. Дифференциальные свойства блочных симметричных шифров, представленных на украинский конкурс. [Текст] / В.И. Долгов, А.А. Кузнецов, С.А. Исаев. // Электронное моделирование. – 2011.– Т33, № 6. – С. 81-99.
4. Кузнецов, А.А. Линейные свойства блочных симметричных шифров, представленных на украинский конкурс. [Текст] / А.А. Кузнецов, И.В. Лисицкая, С.А. Исаев // Прикладная радиоэлектроника. – 2011. – Т.10, №2 – С. 135-140.
5. Лисицкая, И.В. Методология оценки стойкости блочных симметричных шифров. [Текст] / И.В. Лисицкая // Автоматизированные системы управления и приборы автоматики. – 2011. – № 163. – С. 123-133.
6. Лисицкая, И.В. Большие шифры – случайные подстановки. [Текст] / И.В. Лисицкая, А.А. Настенко // Межведомственный научн. технический сборник "Радиотехника". – 2011. – вып. 166. – С. 50-55.
7. Лисицкая, И.В. Дифференциальные свойства шифра FOX. [Текст] / И.В. Лисицкая, Д. С. Кайдалов // Прикладная радиоэлектроника. – 2011. – Т.10, №2. – С. 122-126.
8. Жильников, В. Криптография от компьютера до папируса [Текст] / В. Жильников // М.: ABF, 1996.- 336 с.
9. Pascale, S. The degrees of completeness, of avalanche effect, and of strict avalanche criterion for MARS, RC6, Rijndael, Serpent, and Twofish with reduced number of rounds. [Text] / S. Pascale // Siemens AG, ZT IK 3. April 3, 2000.
10. Бронштейн, И.Н. Справочник по математике для инженеров и учащихся вузов. [Текст] / И.Н. Бронштейн, К.А. Семендяев // Изд-во М:. "Наука" 1980, 976 с.
11. Лисицкая, И.В. Сравнительный анализ механизмов образования лавинного эффекта в алгоритмах DES и ГОСТ 28147-89. [Текст] / И.В. Лисицкая, А.С. Бондаренко, Т.В. Цепурит // Інформаційно-керуючи системи на залізничному транспорті. – 1999. – №3. – С.24-30.
12. Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікації. [Текст] / І.Д. Горбенко, В.І. Долгов, Р.В. Олейніков та ін. // Прикладна радіоелектроніка. – 2007. – Т.6. – № 2. – С. 195-208.
13. Перспективний блоковий симетричний шифр «Мухомор» – основні положення та специфікація. [Текст] / І.Д. Горбенко, М.Ф. Бондаренко, В.І. Долгов та ін. // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2007. – Том. 6, №2. – С. 147-157.
14. Головашич, С.А. Спецификация алгоритма блочного симметричного шифрования «Лабиринт». [Текст] // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2007. – Том. 6, №2. – С. 230-240.
15. Кузнецов, А.А. Симметричный криптографический алгоритм ADE (Algorithm of Dynamic Encryption). [Текст] / А.А. Кузнецов, Р.В. Сергиенко, А.А. Наумко // Прикладная радиоэлектроника. – Харьков: ХТУРЭ. – 2007. – Том 6, №2 – С. 241-249.
16. Олейников, Р.В. Результаты анализа алгоритма шифрования ADE. [Текст] / Р.В. Олейников, В.И. Руженцев, М.С. Михайленко, А.Б. Небывайлов / Прикладная радиоэлектроника. – 2008. – Т.7, №3 – С. 210-214.
17. Долгов, В.И. Мини-версия блочного симметричного алгоритма криптографического преобразования информации с динамически управляемыми криптопримитивами (Baby-ADE). [Текст] / В.И. Долгов, А.А. Кузнецов, Р.В. Сергиенко, А.Л. Белоковаленко // Прикладная радиоэлектроника. – 2007. – Т.7, №3. – С. 215-224.
18. Шнаер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. [Текст] / Б. Шнаер // – М:. Триумф. – 2002. – 727 с.

Abstract

This paper represents additional materials to prove the hypothesis that modern ciphers are asymptotically random substitutions. Here we compare statistics between real modern ciphers and their reduced models. The following indicators are considered: to be avalanche effect, completeness, degree of avalanche effect and degree of the strict avalanche criterion. We describe methods for determining these indicators and analyze the results of applying them to Ukrainian block cipher competitors and also for Rijndael and GOST ciphers.

The presented results clearly confirm that the reduced models have practically the same statistics as their cipher prototypes discussed in this paper (Rijndael, GOST and Ukrainian block cipher competitors – Muhomor, Kalina, ADE, Labirint). This means we can build reduced models with randomness indicators that correspond to their big counterparts, and, therefore, the conclusions we get for 'small' ciphers can be applied to the real ciphers. In particular, it refers to the conclusion that both 'small' and real ciphers asymptotically acquire properties of random permutations.

Correlative indicators in dynamics of their changes are generally the same as the results obtained from studying differential and linear properties for 'small' and real ciphers.

We get additional evidence and arguments in favor of proposed method for measuring block ciphers security by studying their reduced models.

As the additional result of the research, it was concluded that three of the four Ukrainian block cipher competitors have better statistic indicators than well-known Rijndael and thus are superior

Keywords: *provable stability, safety statistics, indicators random model and prototype, the random substitution, cipher reduced model*

Запропоновані методи зменшення впливу перешкод загального вигляду для інтегральних перетворювачів напруги фірми Traco Power AG з метою їх застосування у вузлах гальванічної розв'язки інтерфейсу RS-485. Використання індуктивних фільтрів придушення електромагнітних перешкод значно зменшує вплив шумів інтегральних перетворювачів на якість передачі сигналів у ланцюгах гальванічної розв'язки та збільшує захищеність від перешкод комунікаційних блоків мережі інтерфейсу RS-485

Ключові слова: перетворювач, перешкода, гальванічна розв'язка, інтерфейс

Предложены методы уменьшения влияния помех общего вида для интегральных преобразователей напряжения фирмы Traco Power AG с целью их применения в узлах гальванической развязки интерфейса RS-485. Использование индуктивных фильтров подавления электромагнитных помех значительно уменьшает влияние шумов интегральных преобразователей напряжения на качество передачи сигналов в цепях гальванической развязки и увеличивает помехозащищенность коммуникационных блоков интерфейса RS-485

Ключевые слова: преобразователь, помеха, гальваническая развязка, интерфейс

УДК 004.3

ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ШУМІВ ІНТЕГРАЛЬНИХ ПЕРЕТВОРЮВАЧІВ НАПРУГИ В ЛАНЦЮГАХ ГАЛЬВАНІЧНОЇ РОЗВ'ЯЗКИ

В.С. Кардашук
Кандидат технічних наук, доцент
Кафедра комп'ютерної інженерії
Східноукраїнський національний університет ім. В. Даля
пр. Радянський, 59, м. Сєвєродонецьк, Луганська обл., Україна, 93400
Контактний тел.: 095-477-92-43
E-mail: kardashuk@mail.ru

1. Вступ

Робота з експериментального дослідження шумів ІПН проводилася в рамках науково-технічної програми співпраці між кафедрою комп'ютерної інженерії Технологічного інституту Східноукраїнського національного університету ім. В. Даля (м. Сєвєродонецьк) та науково-виробничим підприємством «Уніконт» (м. Сєвєродонецьк), що займається розробкою і впровадженням програмно-логічних контролерів і робочих станцій для інформаційних систем та систем автоматизації технологічних процесів різного призначення.

Боротьба з перешкодами у комп'ютерних системах набуває все більшої актуальності з багатьох причин:

– зростання частки затримок сигналів у лініях зв'язку в порівнянні з затримками власне логічних елементів, що обумовлюються кінцевою швидкістю поширення сигналів у лініях зв'язку і перехідними процесами в них;

– зростаюча залежність швидкодії комп'ютерних систем, правильності її функціонування від оптималь-