3. *Laguillaumie F., Langlois A., Libert B., Stehle D.* Lattice-based group signatures with logarithmic signature size. URL: http://eprint.iacr.org/2013/308.pdf.
4. *Langlois A., Ling S., Nguyen K., Wang H.* Lattice-based group signature scheme with verifier-local revocation // Public Key Cryptography – PKC2014. Springer, 2014. LNCS. Vol. 8383. P. 345–361.
5. *Cash D., Hofheinz D., Kiltz E., Peikert C.* Bonsai trees, or How to delegate a lattice basis. URL: http://www.cc.gatech.edu/~cpeikert/pubs/bonsai.pdf.
6. *Kawachi A., Tanaka K., Xagawa K.* Concurrently secure identification schemes based on the worst-case hardness of lattice problems // ASIACRYPT. Springer, 2008. LNCS. Vol. 5350. P. 372–389.

REFERENCES:

1. *Chaum D., Heyst van E.* Group signatures // Proceedings of Eurocrypt 1991. Springer-Verlag. Apr. 1991. P. 257–265.
2. *Gordon S.D., Katz J., Vaikuntanathan V.* A group signature scheme from lattice assumptions. URL: https://eprint.iacr.org/2011/060.pdf.
3. *Laguillaumie F., Langlois A., Libert B., Stehle D.* Lattice-based group signatures with logarithmic signature size. URL: http://eprint.iacr.org/2013/308.pdf.
4. *Langlois A., Ling S., Nguyen K., Wang H.* Lattice-based group signature scheme with verifier-local revocation // Public Key Cryptography – PKC2014. Springer, 2014. LNCS. Vol. 8383. P. 345–361.
5. *Cash D., Hofheinz D., Kiltz E., Peikert C.* Bonsai trees, or How to delegate a lattice basis. URL: http://www.cc.gatech.edu/~cpeikert/pubs/bonsai.pdf.
6. *Kawachi A., Tanaka K., Xagawa K.* Concurrently secure identification schemes based on the worst-case hardness of lattice problems // ASIACRYPT. Springer, 2008. LNCS. Vol. 5350. P. 372–389.

V. M. Barbashov, V. G. Ivanenko, N. S. Trushkin

Experiment-Calculated Estimate of a LSIC Operation Reliability in order to Ensure Safety of Information under Radiation Influence

Key word: criteria-based membership function, Brower automat, topological probabilistic models

In this paper digital systems safety operation prediction methods under radiation influence, founded on Brower digital automate and a digital systems operation estimate topological probabilistic models, is considered.

В. М. Барбашов, В. Г. Иваненко, Н. С. Трушкин

РАСЧЕТНО-ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА НАДЕЖНОСТИ ФУНКЦИОНИРОВАНИЯ БИС ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ВОЗДЕЙСТВИИ РАДИАЦИИ

Создание сложных систем БИС, устойчивых к воздействию радиационных дестабилизирующих факторов, на сегодняшний день невозможно без активного использования логического моделирования, обеспечивающего необходимую адекватность описания и точность расчетов. При этом реальный характер радиационного поведения сложной электронной системы определяется конкретным соотношением радиационно-чувствительных параметров ее элементов и учетом влияния их статистического разброса. Соотношение между функцией распределения плотности вероятности разброса и критериальной функцией принадлежности (КФП) определяет, в конечном итоге, целесообразность использования функционально-логических моделей радиационного поведения БИС применительно к каждому конкретному случаю [1].

Для этого, в основном, используют операторы порядковых моделей качества функционирования, которые приведены как пример в таблице 1.

Использование математического аппарата теории нечетких множеств позволяет более корректно и полно сформулировать основы теории качества функционирования цифровой БИС при воздействии радиации [2].

Пусть уровень работы цифровой БИС задается функцией $\psi(z_1, z_2, ..., z_n) = \min z_i$, тогда ее функционирование можно задать последовательной системой, и $\psi(z_1, z_2, ..., z_n) = \max_{i=1,n} z_i$, в этом случае функционирование описывается параллельной системой, где z_i — функция принадлежности элемента БИС. Функция ψ является структурной функцией системы S, а также показателем качества функционирования БИС на структурно-логическом уровне ее описания [2]. Следует отметить, что функция ψ по своей сути является агрегированной функцией принадлежности.

Расчетно-экспериментальное моделирование на базе аналитической формы автомата Брауэра и результаты экспериментов для структур КМОП БИС (триггерного элемента синхронного входного усилителя считывания) (рис. 1—2) показали практически полное совпадение расчетных и экспериментальных результатов функциональных радиационных отказов БИС.

Таблица 1. Операторы порядковых моделей качества функционирования

№ пп.	Название операторов	Операторы	
		пересечение F(x, y) (конъюнкция)	объединение G(x, y) (дизъюнкция)
1	вероятностные операторы	xy	$x + y - xy$
		$\frac{xy}{x + y - xy}$	$\frac{x + y - 2xy}{1 - xy}$
2	минимаксные операторы Заде	$\min(x, y)$	$\max(x, y)$
		$\frac{xy}{a + (1 - a)(x + y - xy)}$	$\frac{x + y + (a - 2)xy}{1 - (1 - a)xy}$

При этом адекватность расчетов сводится к определению критериальных функций принадлежности (рис. 3).

$a = y_1 \cdot z_2$, $z_1 = \overline{(a + \mu_{20})} \cdot y_2 = \bar{\mu}_{20}(\bar{y}_1 + \bar{z}_2) \cdot y_2$;

$b = y_2 \cdot z_1$, $z_2 = \overline{(b + \mu_{21})} \cdot y_1 = \bar{\mu}_{21}(\bar{y}_2 + \bar{z}_1) \cdot y_1$.

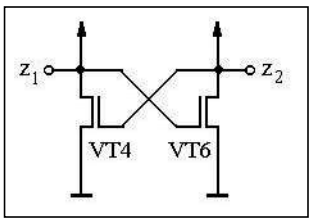

Рис. 1. Триггерный элемент синхронного входного усилителя считывания

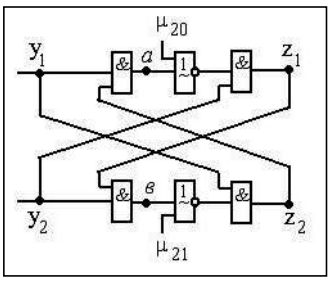

Рис. 2. Нечеткая функционально-логическая модель триггерного элемента синхронного входного усилителя считывания

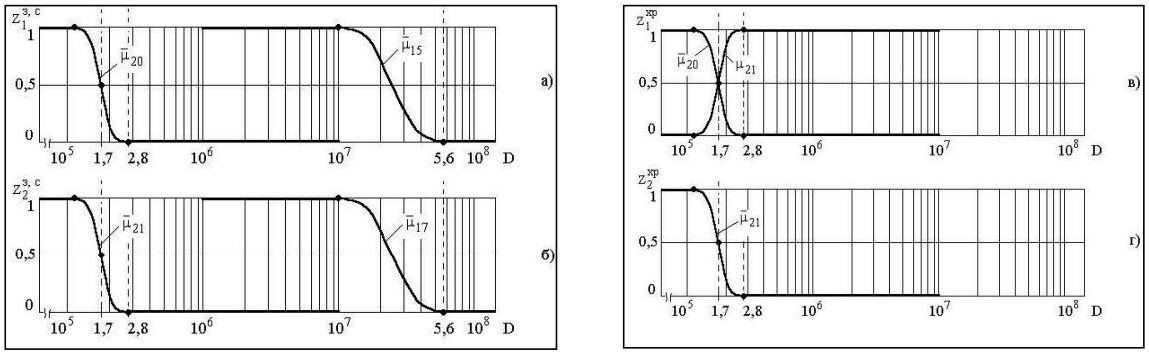

Рис. 3. Расчетные зависимости критериальных функций принадлежности триггера — элемента синхронного входного усилителя считывания КМОП БИС ОЗУ 1617РУ6 при разных режимах работы от поглощенной дозы

Некоторые результаты расчета приведены на рис. 3. Из них видно, что влияние ЛЭ с μ_{20} на стойкость всего устройства доминирует над остальными при режиме «запись-считывание» (рис. 3а) на выходе триггера z_1, а на выходе триггера z_2 доминирует ЛЭ с μ_{21} (рис. 3б). В режиме «хранение» на выходе z_1 состояние устойчивое в заданном диапазоне доз (рис. 3в), а на выходе z_2 доминирует ЛЭ с КФП – μ_{21} (рис. 3г).

Для сравнительной оценки влияния составляющих узлов триггера на его радиационное поведение найдем функцию работоспособности при разных режимах работы, которую можно представить в виде: $\Psi_1 = z \oplus z = z\cdot\bar{z} + \bar{z}\cdot z$.

В заключение следует отметить, что предлагаемая процедура использования теории нечетких множеств обоснована и показывает, что обладает универсальностью и может быть использована в моделях для прогнозирования радиационного поведения БИС. Определена взаимосвязь бесконечнозначной и вероятностной логик, позволяющая наиболее точно оценивать качества функционирования цифровых БИС при воздействии радиации.

СПИСОК ЛИТЕРАТУРЫ:

1. *Барбашов В. М., Трушкин Н. С.* Взаимосвязь вероятностных и порядковых моделей при моделировании функциональной безопасности БИС // Безопасность информационных технологий. 2008. № 3. С. 90–95.
2. *Барбашов В. М., Трушкин Н. С.* Функционально-логическое моделирование качества функционирования ИС при воздействии радиационных и электромагнитных излучений // Микроэлектроника. 2009. Т. 38. № 1. С. 34–47.

REFERENCES:

1. *Barbashov V. M., Trushkin N. S.* Vzaimosvyaz veroyatnostnyx i porydkovyx modelei pri modelirovanii funktsionalnoi besopasnosti BIS // Bezopasnost' informatsionnyx tehnologii. 2008. № 3. P. 90–95.
2. *Barbashov V. M., Trushkin N. S.* Funktsionalno-logicheskoe modelirovanie kachestva funktsionirovaniya IS pri vozdeistvii radiatsionnyh i elektromagnitnyh izluchenii // Mikroelektronika. 2009. T. 38. № 1. P. 34–47.