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).

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

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

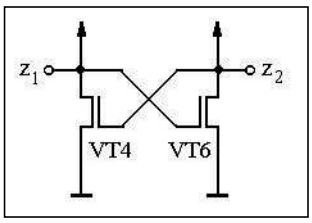

Рис. 1. Триггерный элемент синхронного входного усилителя считывания

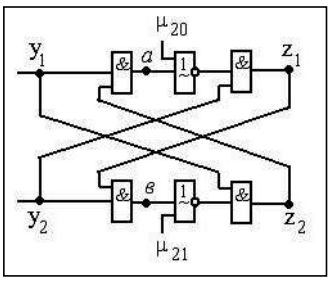

Рис. 2. Нечеткая функционально-логическая модель триггерного элемента синхронного входного усилителя считывания

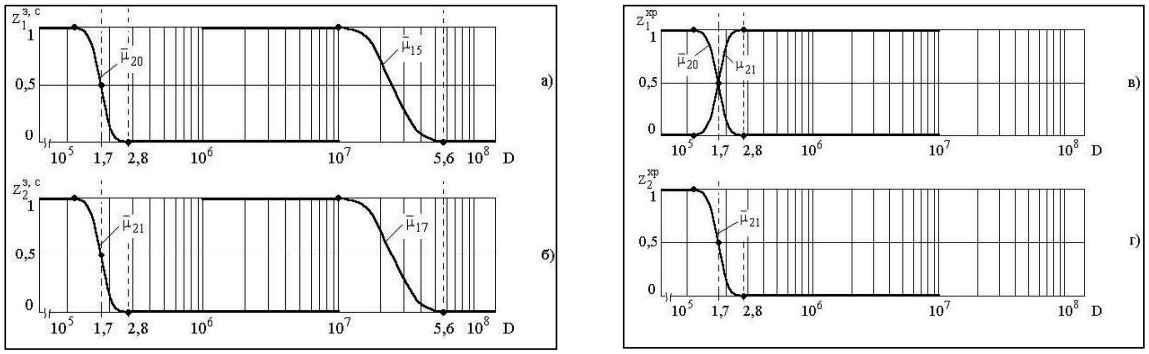

Рис. 3. Расчетные зависимости критериальных функций принадлежности триггера — элемента синхронного входного усилителя считывания КМОП БИС ОЗУ 1617РУ6 при разных режимах работы от поглощенной дозы

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.

A. I. Belozubova, K. G. Kogos

On the Limitation of Covert Channels Bandwidth in IP Networks

Key words: covert channels, bandwidth, IP networks

Features of packet switching networks and the blanket distribution of high-speed IP networks result in widespread research of covert channels. Adversary's possibilities used to build covert channels in IP networks were analyzed. Traffic encryption does not protect against a wide range of covert channels, and the presence of resistant to the detection encoding schemes makes necessary to introduce preventive countermeasures against to the potential covert channels. The compliance between the mechanisms of covert channels construction in IP networks and the methods of eliminating and bandwidth limitation was matched

А. И. Белозубова, К. Г. Когос

ОБ ОГРАНИЧЕНИИ ПРОПУСКНОЙ СПОСОБНОСТИ СКРЫТЫХ КАНАЛОВ В IP-СЕТЯХ

Противодействие утечке информации по скрытым каналам в IP-сетях путем отправки пакетов максимальной длины через равные промежутки времени приводит к существенному понижению пропускной способности канала связи. Актуальным остается исследование методов ограничения пропускной способности скрытого канала до критического значения, такого, что функционирование скрытого канала с меньшей пропускной способностью считается неопасным. Количественные характеристики таких методов выбираются как компромисс между остаточными пропускными способностями скрытого канала и канала связи.

Выделены следующие способы построения скрытых каналов в IP-сетях [1, 2]:

- К1 — изменение полей заголовков передаваемых пакетов;
- К2 — изменение длин передаваемых пакетов;
- К3 — изменение длин межпакетных интервалов;
- К4 — переупорядочивание пакетов, подлежащих отправке.

В таблице 1 представлены возможности нарушителя, необходимые для построения скрытых каналов типов К1—К4.

Таблица 1. Возможности нарушителя, необходимые для построения скрытых каналов

Возможности нарушителя, необходимые для построения скрытых каналов	**Способы построения скрытых каналов**			
	К1	К2	К3	К4
Изменение содержимого полей пакетов	Да	Нет	Нет	Да
Изменение длины передаваемых пакетов	Нет	Да	Нет	Нет
Формирование фиктивных пакетов	Да	Да	Да	Нет
Буферизация пакетов, подлежащих отправке, и передача в определенный момент времени	Нет	Да	Да	Да
Добавление случайных временных задержек при передаче пакетов	Нет	Нет	Да	Нет

В таблице 1 «Да» означает, что данная возможность нарушителя может быть использована для построения скрытого канала, «Нет» означает, что возможность нарушителя не позволяет построить скрытый канал.

В таблице 2 приведено соответствие между механизмами построения скрытых каналов в IP-сетях и способами устранения и ограничения их пропускной способности. В таблице 2 символы имеют следующие обозначения:

– «+» — устранение возможности построения скрытого канала;

– «±» — ограничение пропускной способности скрытого канала;

– «—» — пропускная способность скрытого канала не ограничена.

Таблица 2. Способы устранения и ограничения пропускной способности скрытых каналов

Способы устранения и ограничения пропускной способности скрытых каналов	**Способы построения скрытых каналов**			
	К1	К2	К3	К4
Нормализация значений полей заголовков пакетов	+	—	—	±
Нормализация длин пакетов	—	+	—	—
Нормализация длин межпакетных интервалов	—	—	+	—
Фрагментация и агрегирование пакетов	—	±	±	±
Шифрование трафика	+	—	—	±
Генерация фиктивного трафика	±	±	±	±
Увеличение длин пакетов случайным образом перед отправкой	—	±	—	—
Введение дополнительных случайных задержек перед отправкой пакетов	—	—	±	±
Использование промежуточных шлюзов	+	+	±	+
Установление нескольких допустимых скоростей передачи пакетов	—	—	+	—

В результате проведенного исследования способов ограничения пропускной способности скрытых каналов в IP-сетях актуальным направлением дальнейшей работы было выбрано получение количественных характеристик влияния методов генерации фиктивного трафика и введения дополнительных случайных задержек перед отправкой пакетов на пропускную способность скрытых каналов типа К3.

СПИСОК ЛИТЕРАТУРЫ:

1. *Zander S., Armitage G., Branch P.* A Survey of Covert Channels and Countermeasures in Computer Network Protocols // IEEE Communications Surveys and Tutorials. 2007. Vol. 9. № 3. P. 44–57.

2. *Cabuk S., Brodley C. E., Shields C.* IP covert timing channels: design and detection // Proceedings of the Eleventh ACM Conference on Computer and Communications Security. 2009. P. 22–59.

REFERENCES:

1. *Zander S., Armitage G., Branch P.* A Survey of Covert Channels and Countermeasures in Computer Network Protocols // IEEE Communications Surveys and Tutorials. 2007. Vol. 9. № 3. P. 44–57.
2. *Cabuk S., Brodley C. E., Shields C.* IP covert timing channels: design and detection // Proceedings of the Eleventh ACM Conference on Computer and Communications Security. 2009. P. 22–59.

A. V. Beresneva, A. V. Epishkina

Review and Analysis of Cryptographic Schemes Implementing Threshold Signature

Key words: digital signature, threshold signature, elliptic curves

This work is devoted to the study of threshold signature schemes. The systematization of the threshold signature schemes was done, cryptographic constructions based on interpolation Lagrange polynomial, elliptic curves and bilinear pairings were investigated. Different methods of generation and verification of threshold signatures were explored, e.g. used in a mobile agents, Internet banking and e-currency. The significance of the work is determined by the reduction of the level of counterfeit electronic documents, signed by certain group of users.

А. В. Береснева, А. В. Епишкина

О СИСТЕМАТИЗАЦИИ КРИПТОГРАФИЧЕСКИХ СХЕМ, РЕАЛИЗУЮЩИХ ПОРОГОВУЮ ПОДПИСЬ

Вопрос о применении электронной подписи является крайне актуальным. Растет число ситуаций, когда необходимо, чтобы сообщение было подписано группой пользователей и все они обладали равными правами по отношению к подписи. Кроме того, зачастую возникает задача распределения криптографических ключей между различными устройствами, принадлежащими одному пользователю. В таких случаях необходимо применять пороговое разделение секрета, а именно пороговую подпись.

Пороговая подпись — схема электронной подписи, в которой любые t или более участников группы, состоящей из n абонентов ($t \le n$), могут формировать подпись от имени группы. Секретная информация распределена среди всех n пользователей. Любое подмножество из более чем t пользователей может восстановить секрет.

Схема пороговой подписи (t, n) состоит из трех протоколов:

- протокол генерации ключа;
- протокол генерации подписи, заключающийся в генерации частичных подписей, возможной проверке частичных подписей и их объединении;
- протокол проверки подписи.

Перечислим основные математические аппараты, применимые для формирования пороговой подписи:

- интерполяционный многочлен Лагранжа;
- эллиптические кривые;
- билинейные спаривания.