элементах схемы большого количества тепла и, как следствие, их расплавление (выгорание) и катастрофический отказ.

Помехи меньшей мощности могут вызывать ложные запуски и сбои в схеме, приводить к полному нарушению ее работы.

Существенного снижения воздействия ЭМП ВЧ-диапазона можно добиться различными конструктивно-технологическими методами, и прежде всего подбором высокоэффективного корпуса – экрана из материала с высокой проводимостью, обеспечением его непрерывности и электрогерметичности, рационально организованной системой заземления, позволяющей поддерживать элементы конструкции БГИМС при одном и том же потенциале, равном или близком к потенциалу "земли", и обеспечивать низкоомную нагрузку для опасных токов, которые по тем или иным причинам могут возникать в схеме устройства.

Организация заземления (соединение схемы с общим корпусом) также требует к себе самого пристального внимания, поскольку играет важную роль в уменьшении влияния ЭМП и излучений на нормальное функционирование схемы.

Широкие перспективы при разработке и создании МКМ с повышенной устойчивостью к ЭМП и излучениям открывает электрохимическая алюмооксидная технология (ЭЛАТ), позволяющая на едином технологическом оборудовании с использованием минимальной номенклатуры недорогих материалов изготавливать алюминиевые анодированные подложки (ААП), системы межсоединений высокой степени интеграции, пассивные элементы и корпуса МКМ.

Малый удельный вес, высокие коэффициент теплопроводности, электрические и прочностные свойства ААП наиболее полно удовлетворяют жестким требованиям, предъявляемым к массогабаритным характеристикам и тепловым режимам функционирования схем. Применение ААП при создании МКМ открывает возможность компоновки устройств без дополнительного основания. При этом ААП является одновременно подложкой схемы и основанием корпуса устройства. Герметизация осуществляется крышкой из сплава алюминия, припаиваемой к опорному контуру (рамки), сформированному по периметру подложки.

Для повышения электрической однородности корпуса и обеспечения надежного заземления схемы предложено создавать замкнутый электромагнитный контур между металлическим основанием, рамкой и крышкой корпуса, заземлять схему с помощью проводящих каналов, выполненных в изоляционном оксидном слое подложки.

Проводящие каналы формируются селективным пористым анодированием алюминиевой заготовки одновременно с формированием диэлектрического оксидного слоя на обеих поверхностях заготовки.

При работе микросборки в условиях интенсивного электромагнитного излучения с помощью вертикальных проводящих каналов создается электрический контакт между основанием, рамкой и крышкой корпуса, в результате чего вокруг рабочей части схемы образуется замкнутый электромагнитный контур, исключающий проникновение электромагнитного излучения внутри корпуса и возникновение помех при работе схемы. При этом земляная шина схемы связывается одним из проводников с рамкой, что исключает возникновение "плавающих емкостей" между элементами схемы и корпуса, и как следствие позволяет сохранить быстродействие устройства.

Проведенные испытания опытных образцов МКМ показали, что разработанные конструктивно-технологические методы позволяют в значительной степени повысить устойчивость интегральных схем к воздействию электромагнитных помех и излучений.

СРАВНЕНИЕ КРИСТАЛЛОВ ПЛАСТИКОВЫХ КАРТ ПО СТЕПЕНИ ЗАЩИТЫ ИНФОРМАЦИИ

Д.В. ВЕЧЕР, А.В. ПРИБЫЛЬСКИЙ, В.С. РЕУЦКИЙ, Т.Г. ТАБОЛИЧ

Одной из важнейших характеристик всех видов электронных пластиковых карт (ЭПК) (телефонных, банковских и других) служит степень защиты информации в них от несанкционированного доступа [1]. Процедура несанкционированного доступа злоумышленника к информации в карте обязательно должна включать операцию расшифровки (вскрытия, вычисления) индивидуального ключа карты, аналогичную процедуре аутентификации ЭПК в рабочем модуле безопасности таксофона или банкомата. Сложность процедуры расшифровки определяется сложностью алгоритма шифрования. Для шифрования информации в ключах ЭПК используются симметричные криптосистемы [2, 3], большинство из которых являются национальными или ведомственными стандартами (например, стандарт DES, США, 1975, криптосистемы IDEA, GOST и другие). В свою очередь ключи ЭПК характеризуются своей разрядностью (размером, длиной) – обычно от 40 бит и более.

В таблице [4] проведен сопоставительный анализ времени на расшифровку ключа и затрат на его вскрытие различными категориями злоумышленников, которых в совокупности удобно именовать атакующей стороной.

При этом в таблице обозначено:

ТВК СК — технология восстановления (дешифровки, взлома) ключа симметричной криптосистемы, (ASIC или FPGA),

ASIC — технология с использованием интегральных схем для конкретных приложений,

FPGA — технология с использованием программируемых пользователем логических матриц,

"надежный" ключ — ключ, на расшифровку которого злоумышленникам понадобится 1,5 года и более.

Из таблицы следует, что чем больше разрядность ключа, тем сложнее расшифровать содержащуюся в ключе информацию, и тем выше степень защиты информации в ЭПК. С другой стороны, при увеличении разрядности ключа возрастает сложность ЭПК и, соответственно, ее себестоимость.

Сопоставительный анализ времени на расшифровку ключа ЭПК и затрат на его вскрытие

Атакующая сторона	Затраты, тысяч USD	ТВК СК	Время расшифровки		Длина "надежного" ключа, бит
			Ключ 40 бит	Ключ 56 бит	
Хакер (индивидуальный злоумышленник)			Неделя	бесконечно	45
Малый бизнес	0,4	FPGA	5 часов	38 лет	50
	10	ASIC	12 минут	556 дней	55
Отдел корпорации	300	FPGA	24 секунды	19 дней	60
	300	ASIC	18 секунд	3 часа	60
Крупная компания	10 000	FPGA	7 секунд	13 часов	70
	10 000	ASIC	0,005 секунды	6 минут	70
Федеральное агентство	300 000	ASIC	0,0002 секунды	12 секунд	75

В подразделении НИРУП "ЦНИИТУ", занимающемся разработкой и производством ЭПК, было проведено сравнение по степени защиты информации различных кристаллов, используемых в ЭПК. Установлено, что в телефонном кристалле 4406 защита информации от несанкционированного доступа отсутствует, а в кристалле 4436 имеется ключ длиной 48 бит. Согласно [4] для расшифровки 56-битовых ключей с помощью суперкомпьютера Cray T3D (стоимость такого компьютера в 2000 году составляла 30 млн. долларов) понадобится 453 дня. В то же время длина ключа в телефонной и банковской ЭПК разработки НИРУП "ЦНИИТУ" составляет 256 бит. Это говорит о высокой степени защищенности информации в ЭПК разработки НИРУП "ЦНИИТУ", что в свою очередь свидетельствует о соответствии этих карточек по показателю безопасности информации в них современному научно-техническому уровню и современным тенденциям развития научно-технического прогресса в РБ и за рубежом.

Литература

1. Прибыльский А.В., Таболич Т.Г. Основные направления защиты информации на промышленных предприятиях // В этом сборнике. С.
2. Харин Ю.С., Берник В.И., Матвеев Г.В. Математические основы криптологии. Мн. 1999.
3. Харин Ю.С., Агиевич В.С. Компьютерный практикум по математическим методам защиты информации. Мн. 2001.
4. Калинцев Ю.К. Обеспечение безопасности информации в современных сетях связи//Электросвязь. 2000. N 12. С. 6–8.

СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПРОИЗВОДСТВЕ И ЭКСПЛУАТАЦИИ ТЕЛЕФОННОЙ ЭПК

В.С. РЕУЦКИЙ, Д.В. ВЕЧЕР, А.В. ПРИБЫЛЬСКИЙ

Основные элементы действующей системы обеспечения информационной безопасности телефонной электронной пластиковой карты (ЭПК) НИРУП "ЦНИИТУ" — это криптозащищенная предоплаченная таксофонная карта и модуль безопасности (МБ). Карта изготавливается на основе кристалла российского производства, разработанного в ОАО "Ангстрем" в 1998 году и известного под маркой "Tay-98". Разработчики кристалла учли и устранили ошибки, допущенные при проектировании наиболее близкого аналога 4436 [1, 2].

ЭПК имеет достаточно большой потенциальный ресурс (до 29 тысяч тарифных единиц) и функцию защиты от прерванной записи. Каждая карта имеет индивидуальный ключ карты длиной 256 бит, зашифрованный по ГОСТ 28147-89 и хранящийся в области памяти, закрытой для чтения. Карта является автономным компонентом системы безналичных расчетов и может использоваться как самостоятельное платежное средство. Однако из-за жесткой логики работы ЭПК гарантировать высокую защищенности информации в ней нельзя.

Поэтому в качестве второго компонента системы предлагается использовать освоенный в производстве в НИРУП "ЦНИИТУ" модуль безопасности. Этот МБ представляет собой 8-разрядный микроконтроллер с RISK архитектурой, внутренней операционной системой и протоколом обмена T=0 по ISO 7816-3. Конструктивно МБ выполнен под разъем "PLUG IN" по GSM 11.11 и предназначен для установки в таксофон. В МБ могут храниться одновременно до 16 ключей, которые недоступны для