Шифраторостроение

в постПЛИСовую эпоху

Баранов Александр Павлович, д-р физ.-мат. наук
Баранов Петр Александрович, канд. техн. наук

МАССОВАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПОРОЖДАЕТ МАССОВУЮ КРИПТОГРАФИЮ

1. Массовые корпоративные системы с числом точек шифрования более 2 тысяч различных схем связей: Налог-3, ГАС «Выборы, ГАС «Правосудие», ГАС «ЗАГС» и т. д.
2. Массовые системы взаимодействия пользователей: использующие криптографию: Госуслуги, Социальные сети, автоматизированные системы торгов, частные системы, предоставляющие аналитические и информационные услуги с числом пользователей сто тысяч и более.
3. По п.1, как правило, аппаратное шифрование, а по п.2, программное. Аппаратных шифраторов десятки тысяч.
4. Телефон-смартфон отдельное явление - феномен шифратора миллиардного тиражирования невысокой стойкости. ФЕНОМЕН МАССОВОЙ КРИПТОГРАФИИ

УРОВНИ ТРЕБОВАНИЙ ШИФРОВАНИЯ И МАССОВОСТЬ

1. Программное шифрование ограничивается уровнем КС2, для реализации КС3 нужна аппаратная поддержка.
2. Для скоростного шифрования в протоколе связи, как правило, используется аппаратный шифратор по требованиям КС3 и выше. Это системы п.1.
3. Требования ИБ - К, Ц, Д по прежнему актуальны, но в изменяющихся пропорциях.
4. Ц - освоенная массовая Электронная подпись разных уровней с Конфиденциальностью, удовлетворяющей требованиям Регуляторов систем.
5. Массовая Д(доступность) есть новая реальность. Требований по технической Д от регуляторов НЕТ.
6. Д простирается как на телеком так и на шифротехнику, опирающуюся на телеком

ДОСТУПНОСТЬ В УСТРОЙСТВАХ РЕАЛЬНОГО ВРЕМЕНИ

1. Какие требования по доступности для устройств связи сформулировали Регуляторы?
2. Требования для ЦОДов TIER 1, 2, 3 известны, но к коммутаторам или шифртехнике не применимы.
3. Существуют требования к безотказной работе аппаратуры при безусловной реализации предписанных функций.
4. Однако утвержденной модели воздействия, при которой функции продолжают реализовываться я не встречал
5. Есть сейчас требования ФСТЕК России по гарантиям отсутствия НДВ, предполагающие формирование модели угроз заказчиком системы.
6. Модель угроз неизбежно опирается на модель системы или прибора с моделированием среды функционирования.

ПОДХОДЫ К ОЦЕНКЕ ПАРАМЕТРОВ ДОСТУПНОСТИ

1. Доступность с точки зрения выполнения функционала устройства. Полное или частичное и тогда градация функций.
2. Стандарты по надежности и анализу безотказности.

   ГОСТ Р 27.301-2011, ГОСТ Р 27.002-2015, ГОСТ Р 27-606-2013 и т.д.
3. Общая черта – ПРОГНОЗИРОВАНИЕ на основе гипотетической модели воздействия.
4. Предполагаю, что НДВ можно рассматривать как возможность прекращения доступности функционала устройства в полном объеме или искажение функций. Тогда есть требование ФСТЭК, основанное на модели угроз (модели воздействия) формируемой заказчиком.

ОБЩАЯ СХЕМА УСТРОЙСТВ РЕАЛЬНОГО ВРЕМЕНИ

1. Модель среды функционирования заведомо континуальна

2. Модель шифраторов, коммутирующих устройств телекома-канальных или пакетных, цифровых радиостанций и других систем может быть конечна.

3. Управляющий блок (УБ), например PC, осуществляющий выбор режима работы и взаимодействующий с пользователем.

4. Исполнительный блок (ИБ) - коммутирующая матрица, криптосхема и (или) блок выработки ключей, формировщик волны с заданным законом изменения и т.д.

5. Совокупность устройств, формирующих физический сигнал в среду передачи. Например ASIC микросхемы, радиомодемы.

РОЛЬ ПЛИС В ОТЕЧЕСТВЕННЫХ РАЗРАБОТКАХ

1. ПЛИС может выполнять функции практически любого компьютерного блока, кроме памятей. Все зависит только от его объема и быстродействия-цены. Это обусловило ее привлекательность в России и в мире.
2. ПЛИС можно было производить на обычной фабрике. Например на TSMC. Воронеж примерно так и делал, но это не дешево и схемы не большие.
3. В серийном производстве ПЛИСы используются в основном в России. В мире после использования их при разработке их заменяют на серийные микросхемы. Например ASICи.
4. Intel купил Altera, а AMD купил Xilinx. Санкции и уже больших ПЛИС серийно невозможно использовать

ЭТАПЫ СОЗДАНИЯ ПРОЦЕССОРА ИЛИ МИКРОСХЕМЫ

1. Определение и выбор направления применения процессора или специализированной микросхемы.
2. Разработка архитектуры и выбор системы команд, например MIPS.
3. Подбор имеющихся или покупных частей: IP-блоков, контроллеров, шин, памятей и т.д.
4. Блоки – это программы, написанные на специальном языке. Все части процессора компилируются затем строго для места производства. Перекомпиляция только на иное место производство стоит порядка 1 млн. $ на процессор. Итог: пластины с кристаллами.
5. Корпусирование – отдельная задача. Стоимость среднего производственного участка 2 млн. $. Имеется несколько видов корпусов. Каждому виду свой участок.

ОСОБЕННОСТИ РЕАЛИЗАЦИИ ПРОЦЕССА

1. IP-блоки, как и другие части, можно было приобрести в значительном разнообразии на внешнем рынке. Исходные тексты и скомпилированные (Байкал, Элвис).
2. Блоки процессора можно написать самим с регистрового уровня. В НИИСИ РАН со времен СССР. В СССР был также «Эльбрус 1, 2, 3».
3. Возможно совмещение подходов: IP-блоки покупные, а стыковка и/или ядро управления собственные, предположительно так в КМ211.
4. Необходимо разработать способы создания кристаллов, упрощающие проверку их неизменности после компиляции.

ВОЗМОЖНОСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАЗРАБОТКЕ

1. Разработка модели угроз для ИБ микросхемы-новелла. Изолированность аппаратуры многие проблемы решала. Актуально: появление внешнего воздействия как следствие контроля внешней обстановки или появления управления.
2. Установление возможностей противника на различных этапах процесса создания. Явные описания последствий.
3. Приобретаемые и разрабатываемые IP-блоки необходимо анализировать на отсутствие НДВ. Этого ещё никто не делал для универсальных процессоров. Большой объём даже исходных текстов на специальном языке.
4. Обоснование возможностей изоляции или неизменности порядка использования покупных блоков.

КОНТРОЛЬ КОНЕЧНОЙ ПРОДУКЦИИ

1. Раскорпусирование и выборочный контроль. Раскорпусированый процессор выбрасывается. Корпусирование не в России в разы дешевле.
2. Тестирование кристалла на выполнение им заданных требований: температура, частота, работоспособность интерфейсов и т.д. возможно в России только после корпусирования.
3. Тестирование работоспособности ответственных чипов необходимо независимо от производства в России или вне её.
4. Контроль топологии слоёв целесообразен только при разработке на регистровом уровне или после полного анализа покупных блоков на НДВ. Поскольку анализ никто не знает как это делать, при покупных IP блоках процессору в шифраторе и других устройствах доверять нельзя!