DOI:

Доверенная ЭКБ для доверенных аппаратно-программных платформ: проблемы и пути решения

УДК 621.382 | ВАК 05.27.01

Часть 2

А. Белоус, чл.-корр. НАН Беларуси, д. т. н., профессор[1], В. Солодуха, д. т. н.[2]

Предпринята попытка представить в упрощенном, по возможности систематизированном, виде результаты анализа текущего состояния, проблем и перспектив развития одного из сложных научно-технических направлений развития современной микроэлектроники – проектирования и организации производства ЭКБ, предназначенной для создания современных доверенных аппаратно-программных платформ.

ЧТО ТАКОЕ JFAC?

Объединенный федеративный центр обеспечения безопасности (JFAC) является структурным подразделением Министерства обороны США (МО). Основной задачей этого подразделения является обеспечение его участников программными и аппаратными доверенными средствами, доверенными электронными компонентами и системами с целью создания доверенных систем и сетей **(Trustted Systems and Networks – TSN)**.

Члены JFAC предоставляют свое программное обеспечение в этот центр для проведения экспертизы его безопасности и обеспечения последующей поддержки аппаратного обеспечения, включая выявление уязвимостей, услуги по обнаружению, анализу и смягчению последствий; а также периодически обновляют информацию о возникающих новых киберугрозах, способствуют доведению до членов центра «лучших практических примеров» программных и аппаратных средств оценки и обеспечения безопасности.

Ключевой частью миссии JFAC является распространение среди членов инновационных технологий, которые помогут обеспечить безопасность программного обеспечения в промышленных системах и системах Министерства обороны, включая системы вооружений. Для достижения этой цели агентствами-членами используется структура *Code Dx Enterprise* для автоматической корреляции результатов нескольких инструментов тестирования безопасности приложений (AST), определения приоритетов уязвимостей и непосредственного управления процессом «исправления».

Code Dx Enterprise автоматизирует многие трудозатратные операции, необходимые для запуска инструментов AST, обобщает результаты и определяет приоритеты обнаруженных уязвимостей на основе отраслевых и нормативных стандартов. Он также выявляет слабые места в системе безопасности, которые ставят под угрозу соответствие программного обеспечения дюжине правил или стандартов, включая DISA STIG (Техническое руководство по внедрению безопасности Агентства оборонных информационных систем) версий 3.1 и 4.3 и NIST (Национальный институт стандартов и технологий) 800–53. Любые строки проверяемых кодов, нарушающие эти правила или стандарты, помечаются, и указывается точный характер нарушения, а также способы его устранения, что исключает необходимость для пользователя читать «правила» и позволяет им тратить больше времени на обеспечение качества и безопасности приложения.

Решение **Code Dx Enterprise** объединяет (интегрирует) результаты нескольких статических, динамических и интерактивных инструментов тестирования безопасности приложений, сторонних анализаторов компонентов, инструментов моделирования угроз и ручных проверок в консолидированный набор результатов для быстрой сортировки и исправления уязвимостей. Основная технология была частично профинансирована Министерством науки и технологий национальной безопасности США (DHS S&T), чтобы помочь защитить национальную цепочку поставок программного обеспечения.

[1] ОАО «ИНТЕГРАЛ» – управляющая компания холдинга «ИНТЕГРАЛ», заместитель генерального директора по научно-техническим программам и научной работе, ABelous@integral.by.

[2] ОАО «ИНТЕГРАЛ» – управляющая компания холдинга «ИНТЕГРАЛ», генеральный директор, VSaladukha@integral.by.

Основные функции JFAC:

- поддержка членов JFAC путем выявления типовых уязвимостей, облегчение доступа к экспертным знаниям и возможностям доверенных SwA и HwA (SwA (soft ware) – программное обеспечение, HwA (hard ware) – аппаратное обеспечение);
- разработка политики безопасности, требований, формулировок типовых контрактов и лучших практик, основанных на коллективном опыте поставщиков SwA и HwA по всем учреждениям министерств обороны и энергетики;
- приобретение и поддержание надежной библиотеки корпоративных лицензий для обнаружения и анализа уязвимостей;
- создание базы знаний для управления методиками оценок программного и аппаратного обеспечения, которые могут совместно использоваться поставщиками услуг, инженерами систем безопасности и всеми членами JFAC;
- координация реализуемых мероприятий между многочисленными группами JFAC и создание единого интерфейса для связи всех заинтересованных сторон.

Услуги по анализу программного обеспечения

Через своих поставщиков услуг SwA JFAC может оказывать помощь клиентам по запросу в удовлетворении их потребностей в оценке программ, включая:

- статический анализ исходного кода;
- динамический бинарный анализ;
- статический бинарный анализ;
- анализ веб-приложений;
- анализ базы данных;
- анализ мобильных приложений.

Услуги по разработке программного обеспечения:

- проектирование безопасного программного обеспечения;
- анализ критичности систем защиты;
- управление рисками цепочки поставок ЭКБ;
- интеграция инструментов SwA в конкретную среду разработки, тестирования и развития программного обеспечения;
- обучение управленческого и программно-технического персонала особенностям SwA.

Услуги аппаратного анализа

Через своих поставщиков услуг HwA JFAC может оказывать помощь клиентам по запросу в удовлетворении их потребностей в оценке программ, включая:

- оценку программных особенностей, угроз, рисков цепочки поставок и других факторов;
- предоставление экспертной поддержки по вопросам HwA;
- оказание помощи в разработке и отслеживании технических показателей HwA.

ЭВОЛЮЦИЯ ПАРАДИГМЫ ПРОЕКТИРОВАНИЯ МИКРОСХЕМ ОТВЕТСТВЕННОГО НАЗНАЧЕНИЯ

В работах [1, 2] рассмотрены основные причины, особенности и следствия эволюции классической парадигмы проектирования современных микросхем в части введения в технические задания на разработку микросхем, касающихся вопросов отечественной безопасности их применения в системах ответственного назначения.

Следует сказать, что сегодня не существует таких методов противодействия, которые гарантировали бы абсолютную защиту от различных киберугроз.

Точно так же как и не существует методов, позволяющих с вероятностью 100% их выявить в уже изготовленных микросхемах.

Однако сегодня сотни коллективов исследователей во всем мире, осознав реальную угрозу, работают над этими проблемами, и уже есть весьма эффективные решения, позволяющие существенно повысить безопасность.

Во-первых, уже разработаны и внедрены в практику методы построения безопасных электронных систем, надежно функционирующих в том числе в присутствии аппаратного трояна произвольного типа. Большое разнообразие угроз безопасности, связанных с ними, а также огромное пространство состояний для размещения аппаратных закладок поставило перед разработчиками доверенных микросхем и систем на их основе вопрос об обеспечении безопасной эксплуатации системы с «инфицированными» ИС и, в частности, задачу предотвращения активации внедренных троянов. Такой подход позволяет использовать аппаратуру, не обращая внимания на внедренные аппаратные трояны, и даже использовать COTS-компоненты (коммерческие электронные компоненты, находящиеся в свободной продаже) для построения устойчивых к программным и аппаратным троянам и надежных электронных систем.

Во-вторых, большинство теоретически разработанных и экспериментально проверенных механизмов контрмер можно разделить на следующие большие группы:

- защита данных;
- новые архитектуры на уровне регистровых передач;
- реконфигурируемые архитектуры;
- стратегии репликации, фрагментации и мажоритарной выборки.

Защита данных (включая защиту команд процессора) предполагает предотвращение активации аппаратного трояна или / и блокирование прямого доступа троянского оборудования к любым уязвимым данным. Специальное защитное устройство должно контролировать выборку данных, хранимых или передаваемых внутри или между ИС и логическими модулями системы, блокируя

механизм, посредством которого троян может взаимодействовать с данными. В частности, использовать «гомоморфное» шифрование, позволяющее вычислительным блокам работать непосредственно с зашифрованными данными.

Защищенные архитектуры на RTL-уровне предполагают использование специального программно-аппаратного обеспечения под названием Blue Chip, включая алгоритм под названием UCI (Untrashed Circuit Identification). Отметим, что концепция Blue Chip была использована при проектировании известного радиационно-стойкого процессора Leon 3 (Aeroflex Caisler AB), который является базовым для большинства космических аппаратов NASA и ЕКА. В работе [10] всем этим вопросам посвящена отдельная глава «Основы проектирования кибербезопасных микросхем и систем на кристалле».

О ТЕКУЩЕМ СОСТОЯНИИ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ В РОССИИ И БЕЛАРУСИ

В Правительствах России и Беларуси хорошо понимают сложившуюся в этой сфере ситуацию и предпринимают соответствующие действия.

Республика Беларусь сегодня по праву входит в число современных государств с развитой IT-инфраструктурой и над проблемами обеспечения кибербезопасности (в отечественной терминологии – «доверенные системы») работают многочисленные коллективы белорусских ученых и специалистов, проводятся ежегодные форумы (БАНКИТ) и научно-практические международные конференции (IT-Security Conference-2021, VI Конференция «Технология защиты и информационная безопасность организаций»), вносятся необходимые изменения в «цифровое» белорусское законодательство. Так, введены в действие «Концепция информационной безопасности РБ» (утверждена Постановлением Совета Безопасности Республики Беларусь 18 марта 2019 года № 1), «Концепция обеспечения кибербезопасности в банковской сфере (утверждена Постановлением Правления Национального банка Республики Беларусь 20 ноября 2019 года № 466) и ряд аналогичных руководящих документов.

В **Республике Беларусь** имеется также определенный опыт в области выявления и противодействия аппаратным троянам (методики, ПО, специализированное оборудование).

Поскольку изделия холдинга «ИНТЕГРАЛ» (микросхемы, диоды, дискретные полупроводниковые приборы) включены в «Перечень электронной компонентной базы, разрешенной для применения при разработке, модернизации, производстве и эксплуатации вооружения, военной и специальной техники» редакции 2019 года (Перечень ЭКБ 01-22-2019), специалисты холдинга «ИНТЕГРАЛ» уже много лет занимаются проблемами обеспечения кибербезопасности отечественной ЭКБ, поставляемой российским разработчикам и изготовителям высоконадежных электронных систем и устройств, предназначенных для использования в вышеперечисленных критических инфраструктурах, системах вооружения, военной и космической техники, системах обеспечения безопасности АЭС.

По результатам проведенных многолетних теоретических и экспериментальных исследований, в итоге далеко вышедших за рамки только микроэлектроники, специалистами холдинга «ИНТЕГРАЛ» совместно с белорусскими и российскими учеными был подготовлен и опубликован в отечественной и зарубежной печати ряд научных статей и монографий, посвященных современному кибероружию, методам защиты от него, методам создания современной безопасной ЭКБ для доверенных программно-аппаратных платформ для различных критических инфраструктур [3–10].

«Белорусский» опыт отличается от «мирового» тем, что в исследовательском комплексе задействуется в основном «белорусское» наукоемкое прецизионное технологическое оборудование (производитель – государственный научно-производственный концерн «Планар», г. Минск), которое используется в технологическом процессе изготовления микросхем. Иными словами, для задач анализа не разрабатывается новое специальное оборудование, а используется стандартное, которое работает в производственной линии холдинга «ИНТЕГРАЛ».

В основу методологического подхода специалистов холдинга «ИНТЕГРАЛ» и концерна «Планар» к проблемам выявления троянов положены следующие исходные предположения:

- любая аппаратная закладка (троян) предполагает наличие в микросхеме дополнительных активных элементов (n- или p-канальных МОП-транзисторов или биполярных транзисторов);
- включение таких дополнительных активных элементов предполагает наличие в топологии дополнительных областей затвора, сток / истока и дополнительную активную область, изоляцию между дополнительными элементами.

Так как дополнительные активные элементы не должны исключать действующие активные элементы, то они будут размещаться на свободных местах топологии микросхем, где в исходном варианте находилась изоляция.

Следовательно, на первых уровнях слоев металлизации (1Me, 2Me) должны появиться дополнительные связи по сравнению с оригинальной топологией, а на первом уровне «контактов» (контакты с активной структурой) и контактах между 1Me и 2Me также должны появиться «дополнительные контакты».

Перед производителями ИМС специального назначения, которые используются в доверенных платформах,

стоит задача применения отечественных комплектующих. Как известно, сегодня для производства ИМС специального назначения используются три модели.

1. Фотошаблоны и ИМС производятся на предприятиях, аттестованных МО РФ и имеющих соответствующие Представительства.
2. ИМС производится на производстве, аттестованном МО РФ, а фотошаблоны – на зарубежной фабрике.
3. ИМС и фотошаблоны производятся на зарубежной фабрике.

При производстве на зарубежных фабриках возникает высокая вероятность внесения неконтролируемых изменений в топологию фотошаблонов и изготавливаемых ИМС, хотя исходная топология и разрабатывалась в дизайн-центре на территории Беларуси или России.

Какие есть пути поиска таких изменений (закладок)? Простейший способ – проверка изготовленных за рубежом фотошаблонов на соответствие исходным данным конструкторского проекта. Для этого фотошаблон сканируется с использованием ПЗС-матрицы высокого разрешения, полученные результаты (образ) попиксельно сравнивается с образом топологии из проекта. Все выявленные отличия тщательно анализируются. Данный метод позволяет выявить отличия топологии изготовленного фотошаблона от исходного проекта и является наиболее информативным.

В **Российской Федерации** последнее время также ведутся многочисленные исследования и разработки в области создания доверенных АПП и кибербезопасной ЭКБ для них. В 2015 году в РФ была создана **Ассоциация «Доверенная платформа»**, своего рода аналог JFAC, объединяющая 11 предприятий, первоначально ориентированная на создание доверенных и безопасных мобильных решений. В настоящее время эта ассоциация объединяет уже несколько десятков компаний, включая не только производителей электронного оборудования, лидеров в области безопасности поставщиков различного рода платформенных решений, академические институты, но и практически всех разработчиков и производителей ЭКБ.

В настоящее время эта ассоциация плотно взаимодействует с Департаментом РЭП Минпромторга России и принимает самое активное участие в реализации стратегии развития электронной промышленности РФ на период до 2024 года в качестве «технологического консорциума», решая важнейшую для государства задачу – обеспечение критической информационной инфраструктуры отечественными кибербезопасными (доверенными) решениями на отечественной ЭКБ.

Отдельно следует отметить тот факт, что в Российской Федерации разрабатывается **КНТП «Комплексная разработка и производство приоритетных доверенных интеллектуальных программно-аппаратных платформ на основе отечественных электронных компонентов и программного обеспечения».**

В программе определены 14 направлений работ, направленных на решение этой задачи, которые разделены на шесть крупных проектов, предусмотрена разработка не менее 16 образовательных программ по доверенным АПП, СФ-блокам и модулям, подготовка не менее 390 специалистов в данной области.

В частности, первый проект включает в себя четыре крупных направления исследований:

- исследования в области специфики методов проектирования, производства и контроля доверенной ЭКБ;
- исследования в сфере создания доверенных АПП СКМ, включая основные модели угроз и атак для АПП различных классов СКМ и возможности их парирования;
- исследования оптимальных путей создания семейства доверенных СФ-блоков для отечественных универсальных микропроцессоров с развитыми средствами самоконтроля и диагностики для интеллектуальных АПП;
- исследования по оптимизации семейства электронных модулей, сопроцессоров, технологий создания приложений, средств статистического анализа программ, обеспечивающих отслеживание и интеллектуальный анализ, выявление, самолечение и ликвидацию уязвимостей в режиме реального времени.

* * *

В представленных выше разделах авторы предприняли попытку представить в упрощенном, по возможности систематизированном, виде результаты анализа текущего состояния, проблем и перспектив развития одного из сложных и многочисленных научно-технических направлений развития современной микроэлектроники – проектирования и организации производства ЭКБ, предназначенной для создания современных доверенных аппаратно-программных платформ.

Авторы надеются, что представленная информация будет полезна как разработчикам ЭКБ, так и специалистам, занимающимся проблемами создания отечественных доверенных программно-аппаратных платформ.

ЛИТЕРАТУРА

1. **Белоус А. И., Солодуха В. А.** Современная микроэлектроника: тенденции развития, проблемы и угрозы // Компоненты и технологии. 2019. № 10 С. 6–14.
2. **Белоус А. И., Солодуха В. А.** Основные тенденции развития, проблемы и угрозы современной микроэлектроники // Живая электроника России. 2019. С. 4–12.
3. **Белоус А. И., Солодуха В. А., Шведов С. В.** Программные и аппаратные трояны. Способы внедрения и мето-

ды противодействия. Первая техническая энциклопедия. В 2-х кн. М.: ТЕХНОСФЕРА, 2018. ISBN 978-5-94836-524-4 (in Russian).
4. **Белоус А. И., Гайворонский К. В., Турцевич А. С.** Программные и аппаратные трояны – технологическая платформа кибероружия. М-во образования РБ, Гомельский гос. ун-т им. Ф. Скорины. Гомель, 2018.
5. **Белоус А. И., Солодуха В. А.** Кибероружие и кибербезопасность. О сложных вещах простыми словами. Инфра-Инженерия, 2020. ISBN 978-5-9729-0486-0.
6. **Белоус А. И.** Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения. Инфра-Инженерия, 2020. ISBN 978-5-9729-0512-6.
7. **Belous A., Saladukha V.** Viruses, Hardware and Software Trojans. (Springer Nature Switzerland AG – 2020 ISBN 978-3-030-47218-4).
8. **Belous A., Saladukha V.** Cybersecurity in the 21st Century Kindle.
9. Edition ASIN: B08R8XHC46 https://www.amazon.com/gp/product/B08PPW1J4C?ref_=dbs_p_mng_rwt_ser_shvlr&storeType=ebooks
10. **Белоус А. И., Солодуха В. А.** Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. М.: ТЕХНОСФЕРА, 2021.
11. **Белоус А. И., Красников Г. Я., Солодуха В. А.** Основы проектирования субмикронных микросхем. М.: ТЕХНОСФЕРА, 2020. ISBN 978-5-94836-603-6.