DOI: 10.22184/1992-4178.2021.204.3.98.104

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

Часть 1

А. Белоус, чл.-корр. НАН Беларуси, д. т. н., профессор[1], В. Солодуха, д. т. н.[2]
УДК 621.382 | ВАК 05.27.01

Рассмотрены основные концепции, тенденции, особенности развития относительно нового и стремительно развивающегося направления микроэлектроники – проектирования кибербезопасной ЭКБ для доверенных аппаратно-программных платформ.

Как известно, сегодня вирусы, черви, программные и аппаратные трояны представляют огромную угрозу практически для всех базовых объектов инфраструктуры современного государства, но прежде всего – для информационных систем обеспечения национальной безопасности, банковских и финансовых структур, систем управления вооружением и военной техникой, навигации и связи, промышленной и транспортной инфраструктуры и особенно – для объектов топливно-энергетического комплекса (атомные, тепловые и гидростанции, нефте- и газообрабатывающие заводы, системы управления магистральными газопроводами) [1–6].

На смену любителям, пишущим вирусы и троянские программы ради развлечений, а потом и киберпреступникам, вымогающим или крадущим деньги, сегодня пришли профессиональные сообщества людей, воспринимающих современные информационные системы и киберпространство в целом исключительно как «поле боя».

Проблемы кибербезопасности сегодня стали одной из ключевых проблем для операторов во всех секторах критической инфраструктуры. Быстрый прогресс в использовании наступательных кибервозможностей и практически экспоненциальный рост числа инцидентов, связанных с кибербезопасностью, требуют адекватной реакции со стороны операторов, регулирующих органов и международного сообщества. Однако всем этим заинтересованным сторонам приходится сталкиваться с глобальными тенденциями, которые увеличивают уязвимость кибербезопасности критических объектов. К ним относятся процессы цифровизации АСУ ТП на важнейших объектах; широкое подключение корпоративных офисов и даже промышленных сетей к Интернету с появлением IoT и IoE, использование «иностранной» ЭКБ. Наконец, чрезвычайная сложность трансконтинентальных цепочек поставок программного обеспечения ICS, SCADA и оконечных устройств сегодня стала общей проблемой для большинства секторов критических инфраструктур.

Основная проблема здесь заключается в том, что ежегодно технологии, характер и принципы кибератак (ландшафт киберугроз) изменяются и усложняются, тем не менее, существует ряд общеизвестных киберугроз, о которых надо знать и принимать соответствующие меры защиты.

ЭВОЛЮЦИОННЫЙ ПЕРЕХОД ОТ КЛАССИЧЕСКОЙ «ПИРАМИДЫ ПРОИЗВОДСТВЕННОЙ БЕЗОПАСНОСТИ» К «ПИРАМИДЕ КИБЕРБЕЗОПАСНОСТИ»

Чисто геометрический термин «*пирамида*» давно и часто используется философами, политиками и техническими специалистами различных сфер производственной и научно-технической деятельности, чтобы наиболее доступным способом «визуализировать» различные концептуальные решения по обоснованию выбора тех или иных направлений развития конкретной отрасли – будь то направление коммерческого бизнеса, фундаментальных научных исследований или конкретного производственного направления (пирамида Дюпона, пирамида Маслоу, пирамида Михерина, пирамида происшествий, пирамида Понци и др.).

Впервые термин «пирамида безопасности» был предложен основателем компании DiPont Элетер-Ирене Дюпоном в далеком 1803 году. Эта всемирно известная сегодня компания полвека назад предложила миру бизнеса совершенно новый рыночный продукт, название этого продукта – «промышленная безопасность». Надо сказать, что в результате дальнейшего развития этого направления бизнеса уже

[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.

в 2016 году общий объем продаж фирмой DiPont серии таких продуктов под общим названием Protection Solutions (решения по защите) составил не менее 3 млрд долл.

Общий вид **статистической «пирамиды безопасности»** (в оригинале она называлась «пирамида происшествий»), предложенной Дюпоном, представлена на рис. 1 [4]. В основание этой пирамиды положены так называемые «опасные действия» людей, но не имеющие ощутимых последствий; пусть этих действий будет от 10 до 30 тыс. Ступенью выше располагаются «действия работника и условия труда» (то есть это уже действия другого работника – ответственного за эти условия), которые в итоге привели к микротравмам (порезы, ушибы) – от 1 до 3 тыс. таких действий. Еще выше от основания пирамиды расположены статистические факты от 100 до 300 «настоящих» производственных травм, пока что тоже относительно «легких». Ближе к вершине пирамиды расположены 10–30 тяжелых производственных травм. Венчает эту «пирамиду» всего лишь один «смертельный исход» на производстве. Образно говоря, эта «пирамида» похожа на айсберг с очень небольшой видимой частью (несчастными случаями и смертельным «Титаником») и огромной «подводной», невидимой частью (слишком многочисленными неосторожными действиями персонала).

Еще тогда, много лет назад, трудившиеся в компании Дюпонов «аналитики» впервые пришли к очень важному и сегодня для нас выводу: чтобы уменьшить общее число несчастных случаев, необходимо снизить число подобных неосторожных, небезопасных, опрометчивых действий. То есть фактически изменить поведение людей, говоря «по-современному» – *изменить их отношение к выполнению прямых служебных обязанностей*. Собственно, это решение интуитивно нашел Элетер-Ирене Дюпон, приказавший *поселить семьи работников пороховых заводов непосредственно на производственной территории*: каждый должен был помнить, что от его действий зависят не только его жизнь, но и жизни близких. Но поскольку наше «либеральное» законодательство не разрешает брать заложников, современным менеджерам пришлось искать иные способы уменьшения величины основания современной «пирамиды безопасности», то есть снизить число неосторожных и потенциально опасных действий. Оказалось, что для этого как минимум надо, чтобы каждый инженерно-технический работник, каждый руководитель среднего и низшего звена на своем рабочем месте сам устранял опасные действия и опасные ситуации и саму возможность их возникновения.

Основной принцип безопасности («золотое правило»), к которому, в конце концов, пришли эксперты по безопасности DiPont, гласит: *в ответе за травматизм и безопасность производства не вещи, а люди*. Другими словами, травматизм на любом производстве – это всегда только внешний (видимый) результат плохой организации труда, недостатков техники безопасности или низкой квалификации сотрудников. При жестком соблюдении всех стандартов и необходимых регламентов и достигнутом необходимом уровне производственной и технической дисциплины несчастные случаи будут исключены либо сведены к минимуму.

Следует подчеркнуть, что представленный на рис. 1 пример визуально немного отличается от классической «пирамиды происшествий» времен Элтера Дюпона (www.otpfo.ru). Создатели этого рисунка немного «осовременили» структуру пирамиды (правая часть рисунка) применительно к реалиям нынешней «производственной безопасности», связанным с появлением киберугроз и реальных киберинцидентов. А именно, вместо последовательных «строительных кирпичей» пирамиды: *опасные действия, легкие травмы, тяжелые травмы и «смертельные случаи»*, здесь использованы более современные «строительные блоки», а именно: *угроза инцидента, событие инцидента (небольшая авария, отказ), серьезная авария, катастрофа (массовая гибель людей)*.

Но ведь, объективно говоря, со времен старика Дюпона здесь ничего не поменялось. Если в те далекие времена капиталист Дюпон заставлял своих работников пороховых заводов жить с семьями «на пороховой бочке»

Рис. 1. Модернизированная пирамида происшествий (пирамида безопасности) [4]

с целью поддержания производственной безопасности на должном уровне, то ведь и сегодня все работники критических инфраструктур, сидя на своих комфортабельных рабочих местах, тоже фактически сидят непосредственно на пороховой (нефтяной, газовой, энергетической) «бочке». Но в отличие от капиталиста Дюпона, современные менеджеры предприятий критических инфраструктур не всегда уделяют должное внимание вопросам обеспечения промышленной безопасности, забывая «золотое правило» Дюпона.

Используя и далее этот удобный для пояснения сути проблем популярный «язык пирамид», приведем, как пример, типовую «пирамиду управления электроэнергетическим объектом» (рис. 2).

Здесь в качестве базисного «основания» пирамиды выступают многочисленные исполнительные механизмы, распределители и датчики (сенсоры), на котором базируются все остальные «уровни» пирамиды: ПЛК, ПК, ПИД-регуляторы, SCADA-системы и промышленные сети, а завершает эту пирамиду система управления производством, надежное функционирование которой базируется на безупречной и синхронизированной работе всех компонентов вышеперечисленных «слоев» пирамиды. Однако эта классическая «пирамида управления» промышленным предприятием не учитывает уже очевидных для всех экспертов новых угроз безопасности, а именно – киберугроз.

Вариант такой «модернизированной пирамиды», учитывающий как особенности процессов современной автоматизации и цифровизации промышленных предприятий, так и новые угрозы безопасности – возможность внедрения программных и аппаратных троянов в базовые блоки и модули электронного оборудования программно-аппаратных комплексов АСУ ТП, представлен на рис. 3.

Основой «пирамиды кибербезопасности» современных промышленных инфраструктур является

Рис. 2. Типовая пирамида управления ресурсами промышленного предприятия

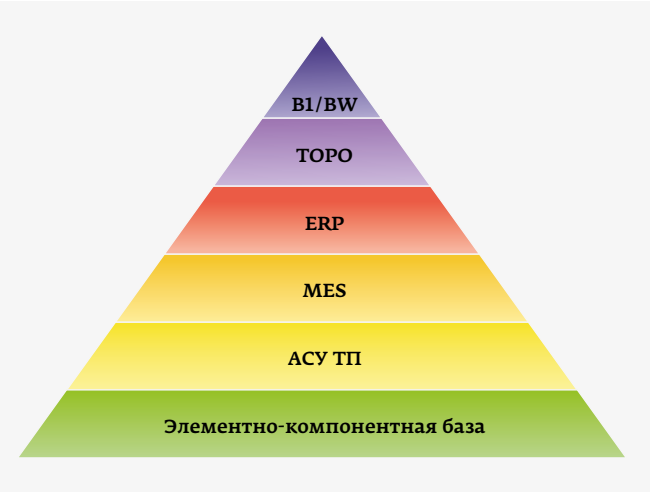


Рис. 3. «Пирамида кибербезопасности» современных промышленных инфраструктур [6]

элементно-компонентная база (ЭКБ) – микросхемы, дискретные полупроводниковые приборы, полупроводниковые датчики физических величин, полупроводниковые сенсоры, интегральные источники питания, электронные коммутаторы, преобразователи и др.

На втором уровне нашей «пирамиды» располагаются АСУ ТП, обычно включающие в себя два основных компонента: APC – Advance Process Control (усовершенствованное управление технологическим процессом) и РСУ – распределенная система управления (DCS – Distributer Control System – система управления технологическим процессом, базирующимся на использовании распределительной системы интерфейсов ввода-вывода с децентрализованной обработкой данных (применяется для управления непрерывными технологическими процессами).

На третьем уровне иерархии нашей «пирамиды кибербезопасности» мы расположили MES – информационно-аналитическую систему, предназначенную для решения задач синхронизации координации, анализа и оптимизации параметров производства.

Четвертый уровень, более высокий в иерархии, занимает ERP – организационно-информационная система, интегрирующая функции управления производством, технологическими операциями маршрута изготовления продукции (изделий), управление трудовыми ресурсами (персоналом), финансовый и бухгалтерский менеджмент и управление активами предприятия. В частности, в состав стандартной ERP обычно входит SCM (Supply Chain Management – система снабжения на предприятии) – информационная система, предназначенная для автоматизации и управления всеми этапами снабжения предприятия необходимым сырьем, материалами и комплектующими изделиями, организации автоматического учета и контроля всего процесса движения товара (продукта). Эта система

охватывает весь цикл: от закупки сырья и требуемых материалов, производства продукта и заканчивая распространением готовой продукции на рынке.

Также на этом уровне пирамиды располагается EAM – Enterprise Asset Management – систематизированная информационная система, предназначенная для оптимизации управления физическими активами предприятия, режимами их работы, управления рисками, материальными и финансовыми затратами на протяжении всего жизненного цикла в соответствии с установленными стратегическими планами предприятия.

На пятом уровне мы расположили техническое обеспечение и ремонт производственного оборудования (ТОРО). Поскольку именно в процессе регламентного технического обслуживания и ремонта существует потенциальная опасность внедрения программных и (или) аппаратных троянов [2–6].

Венчает эту «пирамиду безопасности» современная, широко используемая на цифровых производствах, информационная система (BI/BW), предназначенная для решения задач бизнес-анализа. Эта система позволяет быстро обрабатывать большие объемы данных из различных источников, выявлять так называемые «неявные зависимости» между обрабатываемыми параметрами, автоматически формировать статистическую, финансовую и бухгалтерскую отчетность.

В основу современной «пирамиды кибербезопасности» промышленных инфраструктур должна быть положена именно элементно-компонентная база, а не, например, технические средства обеспечения кибербезопасности, потому что **в любой** аппаратно-программный комплекс обеспечения безопасности (защиты) может быть внедрен либо программный, либо аппаратный троян, а то и оба «зловреда» вместе. Объектом кибердиверсии, как мы показали в [6], может стать, например, даже самый «защищенный» маршрутизатор «безопасных» промышленных сетей, использующих импортную ЭКБ. Поэтому в современных условиях существенно возрастают требования к обеспечению безопасности микроэлектронных изделий.

Следует отметить, что при разработке и организации серийного производства подобных «защищенных» и «сверхзащищенных» маршрутизаторов для различных систем АСУ ТП американские разработчики доверенных программно-аппаратных комплексов и сетевых решений широко используют возможности специальной аналитико-диагностической структуры Федерального объединенного Центра обеспечения безопасности (Joint Federated Assurance Center – JFAC) [2]. Вся ЭКБ, предназначенная для использования в этих доверенных системах, проходит аттестацию в лабораториях этого Центра. Более того, при проектировании ЭКБ для таких систем МО и МЭ США используют целый ряд специальных правил и методов обеспечения безопасности, в том числе так называемую «золотую пятерку безопасности в микроэлектронике», более подробно рассмотренную нами ниже.

ОСНОВНЫЕ НАПРАВЛЕНИЯ РАБОТ США В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ИНФРАСТРУКТУР

Более 15 лет назад в США, одной из первых среди индустриально развитых стран, начали активно заниматься на правительственном уровне проблемами кибербезопасных (*в отечественной терминологии – доверенных*) аппаратно-программных платформ.

Первой реакцией АНБ, Пентагона и DARPA на появление новых угроз стала разработка специальных «программ безопасности».

Агентство национальной безопасности США (АНБ) еще в 2004 году договорилось с корпорацией IBM о запуске совместного (поначалу секретного) проекта под названием Trusted Foundry Access («Доступ к доверяемому цеху»). Эта программа производства «эксклюзивно американских» чипов для нужд Министерства обороны США за период с 2004 по 2010 год обошлась США в 600 млн долл., а за прошедшие годы к ней присоединилось еще более 50-ти других компаний военно-промышленного комплекса США (в том числе BAE, Intersil, Northrop Grumman, Raytheon, Sarnoff, Teledyne).

Затем в DARPA (Defence Advance Recearch Project Agency), оборонном агентстве передовых исследовательских проектов США, была запущена одна из первых программ в этом направлении под названием *Trust in ICs* («*Доверие к интегральным схемам*»). Программа была направлена *на поиск эффективных превентивных решений для защиты кристаллов микросхем ответственного применения от закладок* и заблаговременного выявления различных уязвимостей в случае их появления.

В основе действующей сегодня долговременной стратегии МО США (Department of Defence – DOD) лежат начатые еще в 80-х годах прошлого века работы по созданию национальной **«доверенной технологической платформы»** – аппаратно-программных комплексов, базирующихся только на американских технологиях и решениях, с целью исключить зависимость критически важных государственных объектов США от применений злонамеренных информационных технологий потенциального противника, обеспечения достоверного контроля всех базовых процессов критических производств, обеспечения гарантии отсутствия скрытых возможностей на программном и аппаратном уровнях. **Составные части этой доверенной технологической платформы – это программное обеспечение, аппаратное обеспечение и элементная база (микросхемы).**

Такая программно-аппаратная платформа должна быть защищена на любом технологическом уровне, включая уровень микроэлектронного технологического базиса,

которая позволяет использовать и обрабатывать любую информацию при гарантированном неизменном уровне доверия в соответствующем окружении («доверенной среде»).

Аппаратное обеспечение этой **доверенной среды** базируется на двух основных компонентах: элементной (микроэлектронной) базе и специальных аппаратных **средствах защиты информации**.

Все эти задачи решаются Министерством обороны США в рамках реализации соответствующих мероприятий (элементов) специальной «Программы доверенных фаундри производств», называемой Trusted Foundry Program Element (PE).

Кроме этих основных задач вышеуказанная долгосрочная стратегия планирования ставит и целый ряд более частых задач, которые большинство отечественных экспертов пока считают просто абстрактными «лозунгами», но за этими «лозунгами» стоят конкретные пункты мероприятий конкретных программ, находящихся под непосредственным контролем Министерства обороны.

Ниже мы перечислим только наиболее известные из этих «частных» задач:

- приоритетное развитие методов «упреждающего» планирования при разработке программных (SwA) и аппаратных (HwA) средств с обязательным учетом требований безопасности. Доведение этих стратегических установок до сведения всех задействованных разработчиков SwA и HwA;
- административная и финансовая поддержка научных аналитических исследований, направленных на поиск различных новых уязвимостей и методов защиты от них, на снижение уровней технологических и производственных рисков каналов поставок доверенных микросхем;
- организация жесткого контроля за реализацией всех пунктов утвержденных ранее программ мероприятий по безопасности, персональную ответственность, включая и контроль за соблюдением сроков выполнения каждого этапа заключенных контрактов по этому направлению;
- привлечение представителей промышленности к работе по созданию новых стандартов безопасности, предназначенных для организации общей координации деятельности в сфере выявления потенциально уязвимых мест, наиболее полного использования уже имеющихся производственных возможностей и разработки соответствующих эффективных контрмер;
- всемерная активация и стимулирование человеческого фактора – в части повышения уровня персональной ответственности исполнителей, совершенствования квалификационных требований к исполнителям (включая их периодическую аттестацию), зарегистрированных в цепочках разработки, производства и поставки доверенных микросхем и систем на их основе.

В качестве примера к вышесказанному можно привести только один из нормативных документов МО США, относящихся к обеспечению безопасности каналов поставки микросхем для систем вооружений и военной техники [3]. Этот документ называется Program Protection Plan (PPP). Он имеет подзаголовок Outline and Cuidance (структура и руководство). Об уровне нормативного документа говорит тот факт, что он утверждается приказом заместителя министра обороны США. В этом документе содержатся подробная структура, информация и отформатированное руководство для другого документа – Плана защитных мероприятий в соответствии с основополагающими инструкциями МО США (DoDI 5000.02 и DoDI 5200.39).

Порядок ввода в действие этого и аналогичных документов по американским законам определен специальным «меморандумом для министров военных департаментов и руководителей оборонных ведомств», утвержденным первым заместителем министра обороны США.

В этой связи следует упомянуть и серию программно-аппаратных платформ «Эйнштейн-1, 2, 3», которые исследуют специализированные управляющие технологии для проведения в масштабе реального времени полной инспекции «важных» (критических) объектов и принятия решений на основе анализа спектра всех возможных угроз по сетевому (входящему или исходящему) трафику стандартной сети исполнительных ветвей власти. Программы серии «Эйнштейн» **обеспечивают возможность автоматически обнаруживать и соответствующим образом реагировать на любые киберугрозы прежде, чем будет нанесен ущерб.**

Более подробно результаты анализа основных программ Министерства обороны США в сфере доверенной ЭКБ рассмотрены в главе 10 «Основы государственной политики США в области обеспечения безопасности каналов поставки микросхем» нашей книги «Программные и аппаратные трояны. Способы внедрения и методы противодействия» [3].

ИЗ АМЕРИКАНСКОГО ОПЫТА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭКБ

В ряде научных статей и монографий [1–7] специалисты холдинга «ИНТЕГРАЛ» достаточно подробно описали американский и мировой опыт, накопленный в этой области за почти двадцать лет исследований, в том числе привели формы и полные тексты ряда наиболее важных, на наш взгляд, нормативных документов МО США, относящихся к этой теме. В США именно Министерство обороны (совместно с входящими в структуры МО АНБ и ЦРУ) отвечает за подготовку и реализацию работ по кибербезопасности.

Достаточно просто пролистать эти документы, чтобы понять – у любого злоумышленника действительно нет никаких шансов внедрить свой троян в американскую микросхему на любом этапе ее жизненного цикла, а если у него это каким-то чудесным образом получится, жесткая американская система противодействия и контроля все равно выявит его на финишных испытаниях. Более того, существующие методы уже позволяют не только найти конкретный «этап вставки» трояна, но и конкретного исполнителя этой операции – вплоть до его должности, места работы и даже времени совершения диверсии. Это, конечно, при условии, что исполнители и менеджеры будут жестко выполнять директивные требования соответствующих документов Министерства обороны США.

Но есть, конечно, и другая (обратная) сторона этой американской модели, которая будет крайне неприятна менеджерам, главным конструкторам и научным руководителям отечественных НИОКР и федеральных программ по ЭКБ (конечно, в том случае, если аналогичные нормативные и директивные документы будут приняты на уровне Минпромторга и Минобороны РФ).

Почти на каждой странице этих многостраничных инструкций встречаются фразы типа: «Под персональную ответственность руководителя (менеджера)», «Вы отдаете себе отчет о персональной ответственности за этот пункт?».

Но, внимательно изучив «от корки до корки» эти документы, вы в итоге для себя решите – действительно, если реализовать все последовательные пункты этих обязательных американских инструкций, у вас, как у главного конструктора НИОКР (руководителя проекта), будет твердая уверенность, что в вашей микросхеме не появится никакой лишний элемент и вы с чистой совестью можете передать изготовленную на любой фабрике микросхему своему заказчику.

Специалистами Министерства обороны США и федерального агентства DARPA часто применяется термин «технология контроля безопасности в микроэлектронике». Этот термин впервые появился в технической литературе после 2005 года, после опубликования Министерством юстиции США первого известного судебного отчета о контрафактной китайской ЭКБ.

На рис. 4 представлен взятый с сайта Министерства обороны США соответствующий этой теме слайд «Технологии контроля безопасности в микроэлектронике», который описывает структуру действующего объединенного центра обеспечения безопасности микросхем (JFAC).

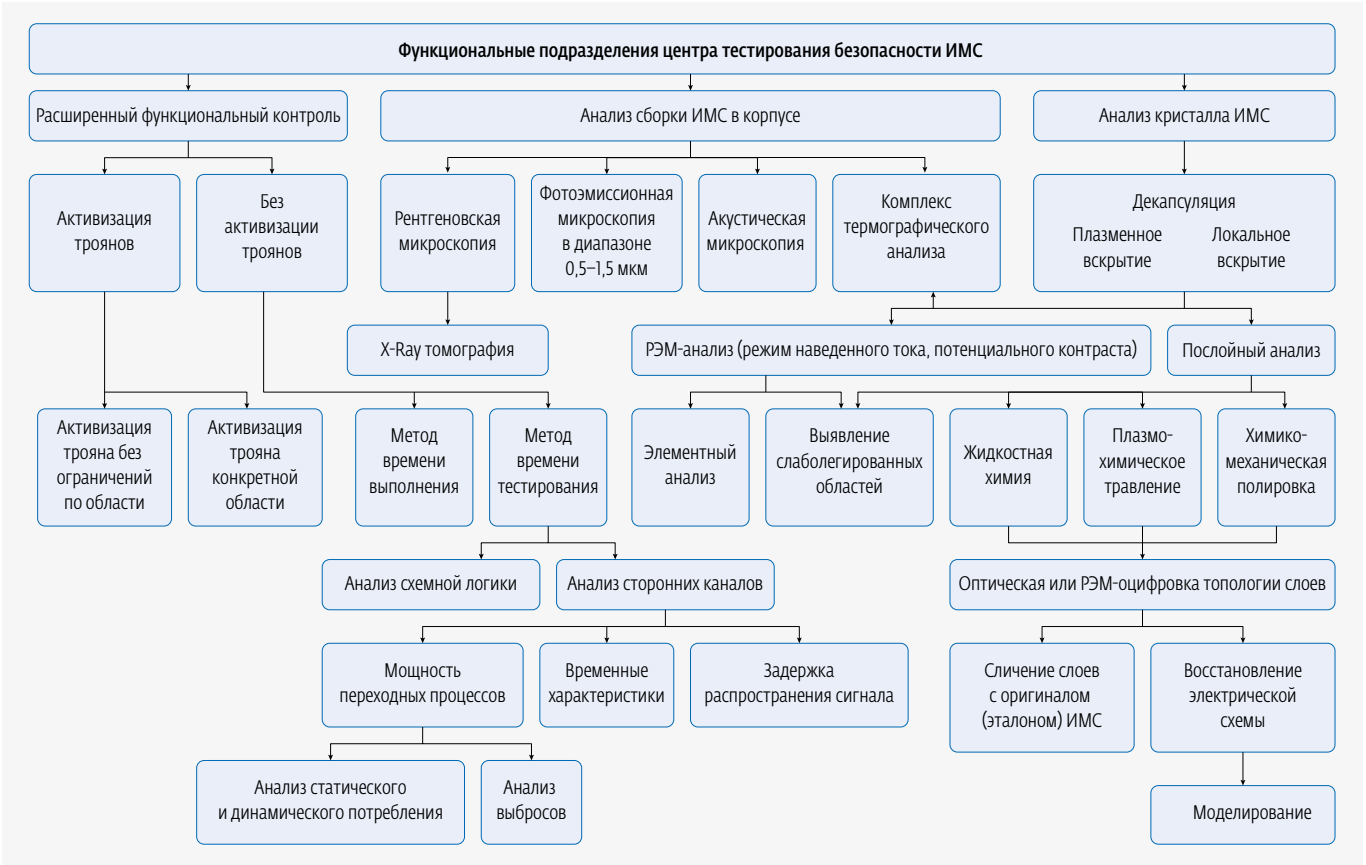
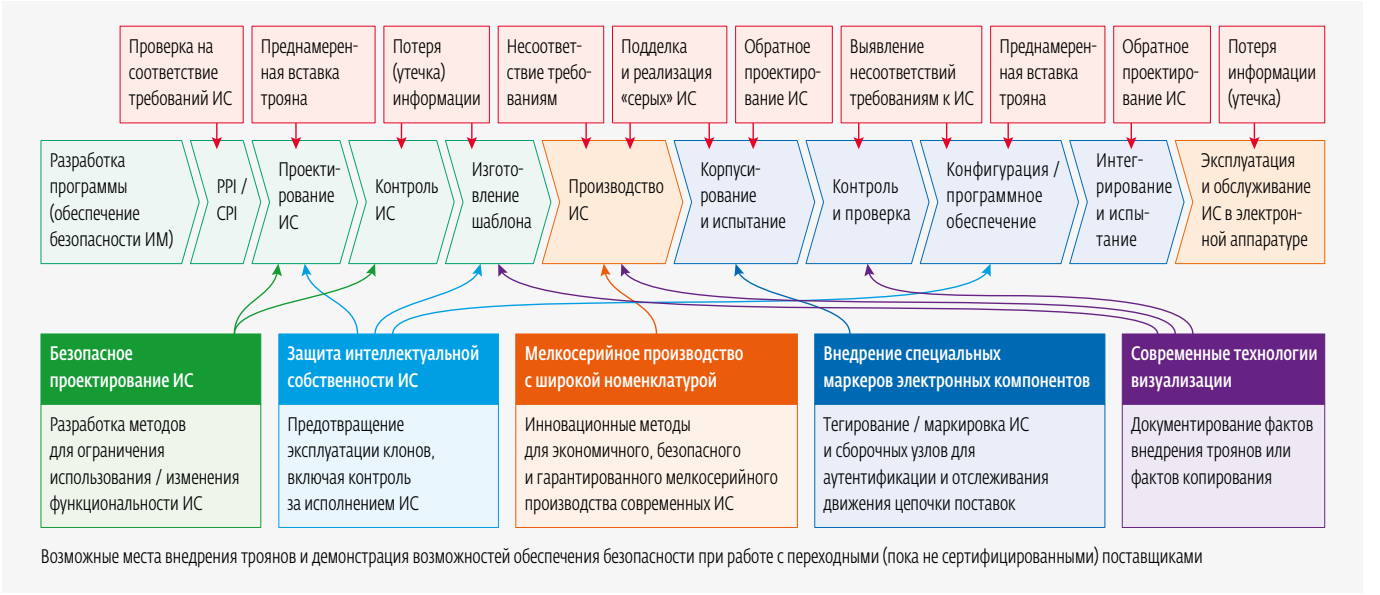


Рис. 4. Основные функции центра JFAC в области обеспечения безопасности ЭКБ



Возможные места внедрения троянов и демонстрация возможностей обеспечения безопасности при работе с переходными (пока не сертифицированными) поставщиками

Рис. 5. Графическое представление последовательности основных этапов цикла изготовления и контроля микросхем на несертифицированной (ненадежной) фабрике

Понятно, что как подобная организационная структура такого Центра, так и описание конкретных задач входящих в его состав функциональных подразделений (лабораторий), описания типов и характеристик используемого оборудования, несомненно, являются служебными и техническими ноу-хау соответствующих служб и департаментов МО США. В этом можно убедиться, зайдя на официальный сайт этого Центра. Это мировая практика. Действительно, что, например, вы знаете о 18 ЦНИИИ МО РФ, кроме самого факта его существования в структуре российского Министерства обороны?

Очевидно, что создание аналогичного Центра в России потребует не только огромных финансовых вложений, но и постановку целого ряда программ научных, прикладных исследований и проблемно-ориентированных научно-технических проектов.

Полный жизненный цикл изготовления микросхем для МО США с указанием как конкретных «проверочных» функций, так и возможных нежелательных для заказчика ИС последствий (утечка конфиденциальной информации, клонирование, изготовление и поставка на рынок лишних («серых») микросхем с аналогичными функциями и т. д.) представлен на рис. 5.

Во второй части статьи будет проанализировано текущее состояние проблемы обеспечения кибербезопасности в России и Беларуси.

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 методы 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. Edition ASIN: B08R8XHC46 https://www.amazon.com/gp/product/B08PPW1J4C?ref_=dbs_p_mng_rwt_ser_shvlr&storeType=ebooks
9. **Белоус А. И., Солодуха В. А.** Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. М.: ТЕХНОСФЕРА, 2021.
10. **Белоус А. И., Красников Г. Я., Солодуха В. А.** Основы проектирования субмикронных микросхем. М.: ТЕХНОСФЕРА, 2020. ISBN 978-5-94836-603-6.