Труды НИИСИ РАН, Т. 13, № 4, 2023

1. Подход к определению типовых угроз безопасности информации для промышленных контроллеров (24 стр.)

А. А. Асонов[1], А. И. Грюнталь[2], В. Н. Родионов[3]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, asonow@niisi.ras.ru;

[2]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, grntl@niisi.msk.ru;

[3]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, rodionov@niisi.msk.ru

Аннотация. Определение актуальных угроз безопасности информации для некоторого объекта оценки, как правило, должно проводиться по Методике оценки угроз безопасности, утвержденной 5 февраля 2021 года в качестве методического документа ФСТЭК России. В настоящей статье показано, что при условии, когда к основному элементу объекта оценки, например, к ОС (в составе которого реализуются основные механизмы подсистемы защиты информации от несанкционированного доступа) и для которого существует введенный установленным порядком профиль защиты, перечень типовых угроз безопасности также можно получить из анализа данного документа. Сравнение угроз безопасности информации, полученных из профиля защиты операционных систем типа «В» четвертого класса защиты (ИТ.ОС.В4.ПЗ), с перечнем угроз безопасности информации, полученных из Базы данных ФСТЭК России на основе экспертного метода, после оптимизации данного перечня и исключения из него повторных угроз показывает, что оставшиеся из них находятся в определенном соответствии с угрозами из профиля защиты с некоторой детализацией по их реализации.

Ключевые слова: угроза безопасности информации (УБИ), пользователь УПК, АСУ ТП, операционная система

2. Использование аппаратных средств профилирования для обеспечения информационной безопасности критически важных систем (5 стр.)

В. А. Галатенко[1], К. А. Костюхин[2]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, РФ, galat@niisi.ras.ru;

[2]ФГУ ФНЦ НИИСИ РАН, Москва, РФ, kost@niisi.ras.ru

Аннотация. Работа посвящена исследованию возможностей применения аппаратных счетчиков производительности (специальных регистров центрального процессора) для выявления потенциальных угроз безопасности критически важных систем и комплексов. Авторами был доработан открытый прикладной программный интерфейс измерения производительности, с помощью которого осуществляется управление аппаратными счетчиками.

Ключевые слова: счетчики производительности, информационная безопасность, атаки по сторонним каналам, PAPI

3. Низкоуровневые криптографические операции (11 стр.)

Н. Д. Байков[1], А. Н. Годунов[2]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, nknikita@niisi.ras.ru;

[2]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, nkag@niisi.ras.ru

Аннотация. Целью работы является обзор базовых низкоуровневых криптографических операций, лежащих в основе современных криптографических протоколов. Рассмотрены примеры широко применяемых операций криптографического хэширования, шифрования и формирования электронно-цифровой подписи.

Ключевые слова: криптографическая хэш-функция, шифрование, цифровая подпись

4. Введение в разработку и сопровождение систем, реализующих парадигму интернета вещей (5 стр.)

В. А. Галатенко[1], К. А. Костюхин[2]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, РФ, galat@niisi.ras.ru;

[2]ФГУ ФНЦ НИИСИ РАН, Москва, РФ, kost@niisi.ras.ru

Аннотация. В статье рассматривается архитектура типичной системы интернета вещей, выделяется набор требований к ее компонентам, и на основе этих требований формулируются требования к средствам разработки и сопровождения систем, реализующих парадигму интернета вещей.

Ключевые слова: интернет вещей, средства разработки, архитектура, требования

5. Платформа для создания стенда полунатурного моделирования на основе ПЛК «Багет» (9 стр.)

С. Е. Базаева[1], Я. А. Зотов[2]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, bazaeva@niisi.msk.ru;

[2]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, zotov@niisi.ras.ru

Аннотация. В статье описан проект программной платформы, предназначенной для создания стендов полунатурного моделирования и цифровых двойников АСУ ТП, в состав которых входит ПЛК «Багет». Предлагаемый авторами подход к разработке инструментальных средств построения стендов позволяет обеспечить современный набор функциональных возможностей для моделирования и широкую область применения платформы.

Ключевые слова: программная платформа, стенд полунатурного моделирования, АСУ ТП, ПЛК «Багет»

6. Вопросы применения концепции HLA при создании стендов полунатурного моделирования (5 стр.)

С. Е. Базаева[1]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, bazaeva@niisi.msk.ru

Аннотация. В статье рассматриваются вопросы применения концепции распределенного моделирования HLA (High Level Architecture) при создании стендов полунатурного моделирования для АСУ ТП. Дан краткий обзор истории возникновения HLA, преимуществ и недостатков данного стандарта применительно к поставленной задаче, проанализированы функциональные возможности, предоставляемые стандартом HLA. Автором дана оценка целесообразности применения концепции HLA при разработке инструментальных средств для полунатурных стендов на основе ПЛК Багет.

Ключевые слова: полунатурный стенд моделирования, стандарт HLA, распределенное моделирование

7. Архитектура типовой системы автоматизации технологических процессов на базе отечественных СВТ и ПО (4 стр.)

М. С. Аристов[1], А. И. Грюнталь[2], Я. А. Зотов[3], Я. А. Шаповалов[4], Д. В. Яриков[5]

[1] ФГУ ФНЦ НИИСИ РАН, Москва, Россия, aristov@niisi.ras.ru;

[2] ФГУ ФНЦ НИИСИ РАН, Москва, Россия, grntl@niisi.ras.ru;

[3] ФГУ ФНЦ НИИСИ РАН, Москва, Россия, zotov@niisi.ras.ru;

[4]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, shapovalov@niisi.ras.ru;

[5]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, yarikov@niisi.ras.ru

Аннотация. В свете высоких рисков использования зарубежных решений для автоматизации технологических процессов критической инфраструктуры стали особенно актуальны решения на базе отечественной технологической базы. В статье описана архитектура типовой АСУ ТП на базе разработанных в ФГУ ФНЦ НИИСИ РАН программируемых логических контроллеров, операционной системы, средств разработки и другого ПО. Представленные решения поддерживают отраслевые стандарты обмена данными между АСУ ТП и устройствами управления.

Ключевые слова: программируемые логические контроллеры, операционная система, отечественное производство, автоматизированные системы управления, технологические процессы, scada, разработка ПО

8. Развитие языка Си и обзор будущего стандарта C23 (7 стр.)

В. А. Галатенко[1], Г. Л. Левченкова[2], С. В. Самборский[3]

[1] ФГУ ФНЦ НИИСИ РАН, Москва, РФ, galat@niisi.ras.ru;

[2]ФГУ ФНЦ НИИСИ РАН, Москва, РФ, galka@niisi.ras.ru;

[3]ФГУ ФНЦ НИИСИ РАН, Москва, РФ, sambor@niisi.ras.ru

Аннотация. Работа содержит краткий обзор основных этапов развития языка программирования Си с момента его создания. Рассматриваются существующие стандарты этого языка. Пристальное внимание уделяется новому стандарту языка Си – С23. Выделяются его достоинства и недостатки.

Ключевые слова: язык Си, стандарт, С23

9. Оценка сбоеустойчивости топологии СФ блока на разных этапах оптимизации комбинационной логики логического синтеза (5 стр.)

Е. К. Эмин[1], К. А. Петров[2], В. В. Азаров[3], А. П. Скоробогатов[4], А. А. Антонов[5]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, emin@cs.niisi.ras.ru;

[2]ФГУ ФНЦ НИИСИ РАН, Москва, petrovk@cs.niisi.ras.ru;

[3]ФГУ ФНЦ НИИСИ РАН, Москва, azarov_v@cs.niisi.ras.ru;

[4]ФГУ ФНЦ НИИСИ РАН, Москва, skorobog_a@cs.niisi.ras.ru;

[5]ФГУ ФНЦ НИИСИ РАН, Москва, antonov@niisi.msk.ru

Аннотация. Проведен анализ сбоеустойчивости полученных схем СФ-блока с их реальной топологической оценкой. Предложена оценка выходных характеристик полученной схемы при помощи сигмоидальной функции. Данная функция может использоваться для сравнения различных схем, а также для поиска оптимальной схемы заданной логической функции в эвристических алгоритмах, и алгоритмах машинного обучения.

Ключевые слова: сложно-функциональный блок, логический синтез, оптимизация, сбоеустойчивость, одиночные сбои, проектирование СБИС

10. Сокращение энергопотребления СФ-блоков посредством автоматизированного подбора оптимальных параметров проектирования (5 стр.)

Е. С. Кочева[1], Н. В. Желудков[2], Е. В. Ткаченко[3], Н. В. Желудков[2], К. А. Чумаков[5], К. А. Петров[6]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, kocheva@cs.niisi.ras.ru;

[2]ФГУ ФНЦ НИИСИ РАН Москва, Россия, nvgel@cs.niisi.ras.ru;

[3]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, etkachenko@cs.niisi.ras.ru;

[4]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, eboris@cs.niisi.ras.ru;

[5]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, kchumak@cs.niisi.ras.ru;

[6]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, petrovk@cs.niisi.ras.ru

Аннотация. Исследована возможность применения метода автоматизированного подбора оптимальных параметров в процессе проектирования СФ-блоков для оптимизации их энергопотребления. В качестве объектов исследования использовались блок интерфейса ввода/вывода связи процессора и сопроцессора и блок целочисленного умножения-деления 64-разрядных чисел. Полученные результаты позволяют сделать вывод о целесообразности применения исследованного метода в маршруте проектирования СФ-блоков.

Ключевые слова: топологическое проектирование, СБИС, СФ-блок, Optuna, энергопотребление.

11. Реализация функции пространственной фильтрации изображения на векторном сопроцессоре (6 стр.)

С. И. Аряшев[1], П. А. Чибисов[2], В. В. Цветков[3], Д. А. Трубицын[4], К. А. Петров[5]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, aserg@cs.niisi.ras.ru;

[2]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, chibisov@cs.niisi.ras.ru;

[3]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, tsvetkov@cs.niisi.ras.ru;

[4]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, trubitsyn@cs.niisi.ras.ru;

[5]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, petrovk@cs.niisi.ras.ru

Аннотация. Для увеличения быстродействия универсальных микропроцессоров MIPS-подобной архитектуры в НИИСИ РАН был разработан специализированный сопроцессор, позволяющий ускорять операции с комплексными и вещественными числами одинарной и двойной точности. В статье представлены результаты применения 128-го разрядного векторного сопроцессора для задачи фильтрации изображения. На примере двух вариантов векторизации показано повышение эффективности выполнения вычислений при решении этой задачи.

Ключевые слова: векторный сопроцессор, сопроцессор вещественной арифметики, CPV, фильтрация изображений.

12. Оценка карты разводимости при проектировании цифровых блоков СБИС с помощью графовых нейронных сетей (6 стр.)

Н. В. Желудков[1], Я. М. Карандашев[2], Е. С. Кочева[1], М. Х. Сайбодалов[1], З. Б. Сохова[1], А. А. Умнова[1]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, nvgel@cs.niisi.ras.ru;

[2] ФГУ ФНЦ НИИСИ РАН, Москва, Россия, karandashev@niisi.ras.ru

Аннотация. В рамках данной работы рассматривается решение задачи оценки карты разводимости на ранних этапах топологического проектирования цифровых блоков СБИС с помощью применения нейросетевой модели машинного

обучения, основанной на графовой нейронной сети. Раннее предсказание проблемных мест с разводкой позволит разработчику топологии изменить такие характеристики проектируемого блока, как план размещения, расположение макроблоков, а также входных и выходных портов таким образом, чтобы предотвратить возникновение проблем с трассировкой соединений на поздних этапах, тем самым сократив число запусков САПР и общее время проектирования схемы. Применение графовых нейронных сетей позволяет учитывать дополнительную информацию о связях элементов в нетлисте, для более точного предсказания.

Ключевые слова: СБИС, топологическое проектирование, карта разводимости, машинное обучение, графовые нейронные сети

13. Применимость методов машинного обучения для тестирования моделей микропроцессора (8 стр.)

Н. А. Гревцев[1], А. Д. Манеркин[2], П. А. Чибисов[3]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, ngrevcev@cs.niisi.ras.ru;

[2]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, manerkin@cs.niisi.ras.ru;

[3]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, chibisov@cs.niisi.ras.ru

Аннотация. В статье приведен обзор использования методов машинного обучения для различных направлений функциональной верификации. Рассматривается использование машинного обучения в «pre-silicon» верификации, а именно в имитационном тестировании и верификации при помощи UVM. Приводится обзор в области «post-silicon» верификации. Делается вывод об основных областях применения машинного обучения, а также о возможных будущих направлениях исследований.

Ключевые слова: верификация микропроцессоров, машинное обучение, Deep Learning, UVM

14. Оценки вероятности промаха при случайном тестировании кэша (6 стр.)

А. С. Куцаев[1]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, koutsaev@niisi.msk.ru

Аннотация. Вероятность промаха при случайном тестировании системы кэшей зависит в основном от распределения памяти. Оно позволяет ограничить число активных строк, создавая тем самым нагрузку на кэш. Перебор областей памяти в генераторе тестов позволяет сократить вспомогательные действия в тесте, не связанные непосредственно с тестированием. Оценки вероятности промаха в кэшах первого и второго уровня при различных условиях позволяют выбрать параметры для генерации эффективных тестов.

Ключевые слова: случайные тесты, вероятность промаха в кэше, перебор областей памяти

15. Влияние зернистости металлического затвора кремниевых конических GAA нанотранзисторв на флуктуации порогового напряжения (6 стр.)

Н.В. Масальский[1]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, volkov@niisi.ras

Аннотация. Обсуждается влияние зернистости металлического затвора на флуктуацию порогового напряжения кремниевого полевого GAA нанотранзистора. На основе теоремы Пельгорма разработана методика достоверной оценки флуктуации порогового напряжения. В диапазоне длин затворов транзисторов от 11 до 25 нм и средних размеров зерен от 3 до 10 нм получены коэффициенты Пельгорма. Относительные погрешности между модельными значениями стандартного отклонения порогового напряжения и данными полученными из 3D моделирования практически в 95% случаев ниже 5%.

Ключевые слова: перечисление ключевых слов через запятую

16. Тенденции в графических ускорителях для высокопроизводительных вычислений (6 стр.)

А. С. Шмелёв[1]

[1]МСЦ РАН филиал ФГУ ФНЦ НИИСИ РАН, Москва, Россия, guest8993@rambler.ru,

Аннотация. Графические карты, построенные на основе большого количества простых и однотипных исполнительных устройств и обладающие высокой пиковой производительностью уже давно используются в области высокопроизводительных вычислений в качестве ускорителей вычислений. В настоящее время выпускаются отдельные продукты, ориентированные на применение в вычислительных центрах. В данной работе приводится обзор современных ускорителей для вычислительных центров, приведены их показатели производительности, а также приведены анонсы перспективных ускорителей вычислений и показаны тенденции в данной области.

Ключевые слова: высокопроизводительные вычисления, графические ускорители, ускорители вычислений, суперЭВМ, память с высокой пропускной способностью.

17. От критических методов к процессам доказательств (4 стр.)

В. Г. Редько[1]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, vgredko@gmail.com

Аннотация. Построена и проанализирована модель процесса формирования доказательства на основе использования критического мышления. Проведён анализ

методов использования критических рассуждений в научном процессе и в современных схемах искусственного интеллекта. Проанализированная модель вносит вклад в изучение когнитивной эволюции.

Ключевые слова: критическое мышление, доказательство, научное познание

18. О нововведениях в цифровой образовательной платформе Мирера (8 стр.)

И. А. Васильев[1], А. С. Караваева[2], А. Г. Леонов[3], К. А. Мащенко[4], А. В. Шляхов[5]

[1]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, vanya71161@gmail.com;

[2]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, aleksandrakaravaevaa@yandex.ru;

[3]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, МГУ им. М. В. Ломоносова, Москва, Россия, МПГУ, Москва, Россия, Государственный университет управления, Москва, Россия, dr.l@vip.niisi.ru;

[4]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, kirill.mashchenko@vip.niisi.ru;

[5]ФГУ ФНЦ НИИСИ РАН, Москва, Россия, shlyakhov@vip.niisi.ru

Аннотация. При опытной эксплуатации образовательных платформ могут возникать трудности и потребности в нововведениях или исправлениях, которые не были заметны во время разработки и тестирования. Своевременные доработки и изменения способствуют улучшению опыта использования и уменьшают количество сил, затраченных на выполнение неудобных действий в системе, что позволяет лучше сконцентрироваться на выполнении основных задач, таких как преподавание или обучение. В данной статье описываются проблемы, с которыми столкнулись пользователи во время использования комплекта модулей цифровой образовательной платформы Мирера, и методы их решения.

Ключевые слова: цифровая образовательная платформа, цифровая образовательная среда, Мирера, автоматическая проверка, машинное обучение, нейронные сети, трансформеры, семантическая проверка, WebSocket, модульная архитектура