Динара Мирзабековна Калманова* – хат-хабар авторы, педагогика ғылымдарының кандидаты, Л. Гумилев атындағы Еуразия ұлттық университетінің «Ғарыштық технологиялар және технологиялар» кафедрасының доценті, Астана, Қазақстан; e-mail: dinara_kalmanova@mail.ru. ORCID: https://orcid.org/0000-0001-5977-8448.

Өмірзақ Көптілеуұлы Әбдірашев – PhD, Л.Н. Гумилев атындағы Еуразия ұлттық университетінің «Ғарыштық технологиялар және технологиялар» кафедрасының доценті, Астана, Қазақстан; e-mail: omeke_92@mail.ru. ORCID: https://orcid.org/0000-0001-7621-5444.

Асем Адилбекқызы Конырханова – Л.Н. Гумилева ат. ЕҰУ Ақпараттық технологиялар факультетінің Ақпараттық қауіпсіздік кафедрасы доцентінің м.а., Астана, Қазақстан; e-mail: konyrkhanova_aa@enu.kz. ORCID: https://orcid.org/0000-0002-4923-9800.

Поступила в редакцию 11.06.2025
Поступила после доработки 16.06.2025
Принята к публикации 23.06.2025

https://doi.org/10.53360/2788-7995-2025-3(19)-4

МРНТИ: 47.14.07, 81.93.29

Н.С. Глазырина[1], А.К. Шайханова[1*], К.М. Аяпбергенов[1], И.А. Сенюшин[1], Р. Муратхан[2]
[1]ТОО «TSARKA R&D»
[2]ТОО «TSARKA LABS»
010000, Республика Казахстан, г. Астана, проспект Кабанбай Батыра 51/1
*e-mail: igul.shaikhanova@gmail.com

АНАЛИЗ СОВРЕМЕННЫХ СПОСОБОВ ПРОИЗВОДСТВА ИНТЕГРАЛЬНЫХ СХЕМ ДЛЯ СОЗДАНИЯ КРИПТОКОНТРОЛЕРА В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация: *В статье исследуются современные методы производства интегральных схем с целью создания криптоконтроллера в Республике Казахстан. Работа анализирует глобальные тенденции полупроводниковой индустрии, технологические особенности и экономические аспекты производства интегральных схем, а также определяет направления развития полупроводниковой промышленности в Казахстане для разработки аппаратных средств безопасности. Методология исследования включает анализ современных методов проектирования и производства интегральных схем, основанный на сравнении различных технологических процессов, планов и проектов, реализованных в странах, имеющих производственные возможности зрелого, промежуточного и передового интеграции и производительности. Результаты исследований показывают, что для Республики Казахстан, не имеющей собственной производственной базы для интегральных схем, оптимальным подходом является развитие fabless-модели с проектированием внутри страны и производством на сторонних фабриках. Это не требует значительных инвестиций по сравнению с созданием национальных производственных мощностей на зрелых узлах. В работе предлагается поэтапный подход к созданию отечественного криптоконтроллера, начиная с прототипирования на программируемой логике и последующего переноса архитектуры в специализированную интегральную схему. Практическая ценность работы заключается в том, что определены оптимальные возможности для организации производства полупроводниковых микросхем в Казахстане и разработки отечественного криптоконтроллера на уровне, готовом к промышленному производству.*

Ключевые слова: *информационная безопасность, криптоконтроллер, интегральная схема, аппаратная реализация, полупроводниковая промышленность, технологический узел, электронная подпись, FIDO, fabless-модель.*

1 Введение

Полупроводниковые технологии стали неотъемлемой частью современного общества, определяя развитие широкого спектра отраслей. Они играют ключевую роль в миниатюризации электронных компонентов (чипов), повышении производительности и энергоэффективности конечных устройств, что делает технологии доступными для массового применения [1, 2]. Достижения в области проектирования и производства полупроводников

способствуют развитию электронных коммуникаций, искусственного интеллекта, машинного обучения, автоматизированных систем и интернета вещей, тем самым стимулируя технологические инновации [3-6].

Быстрый рост полупроводниковой промышленности в последние годы усилил конкуренцию в глобальной технологической сфере, где передовые разработки тесно переплетаются с экономическим развитием государств. Согласно данным Ассоциации полупроводниковой промышленности (SIA), мировые продажи полупроводников в 2020 году увеличились на 6,5% по сравнению с 2019 годом, составив около 43,9 млрд долларов США [7]. В 2021 году рост продолжился и достиг 26,2%, превысив 55 млрд долларов США. В 2024 году рост мирового сектора полупроводников составил 16,0% в годовом исчислении [8]. При этом две категории интегральных схем станут основными драйверами роста с двузначным приростом: логические схемы (10,7%) и память (76,8%). Зафиксирован значительный рост полупроводниковой промышленности в странах Северной и Южной Америке, Азиатско-Тихоокеанском регионе на 25,1% и 17,5% [8].

Развитие полупроводниковой промышленности сегодня является ключевым фактором научно-технического прогресса, определяющим возможности цифровизации, автоматизации и обеспечения кибербезопасности. Индустрия полупроводников эволюционировала от планарных транзисторов к трёхмерным архитектурам и экстремальной литографии, что позволило достичь рекордных показателей производительности и энергоэффективности. Однако доступ к передовым технологиям концентрируется в ограниченном числе стран, что усиливает технологическую зависимость и формирует новые геополитические риски.

Одновременно возрастает значимость аппаратной информационной безопасности. Традиционные программные решения подвержены широкому спектру атак, тогда как специализированные аппаратные устройства, такие как криптоконтроллеры и аппаратные токены, обеспечивают принципиально более высокий уровень доверия и устойчивости к угрозам [9].

В настоящее время нами выполняются прикладные исследования в рамках научного проекта AP26103891 «Разработка отечественного криптоконтроллера и его имплементация в устройстве хранения ключей», финансируемые Комитетом науки Министерства науки и высшего образования Республики Казахстан. Целью данного проекта является создание отечественного криптоконтроллера с аппаратной реализацией криптографических алгоритмов и разработка на его основе носителя ключевой информации (USB-токена), предназначенного для безопасной аутентификации и защиты данных в системах, поддерживающих стандарт быстрой интернет-аутентификации (Fast Identity Online, FIDO) [10] и алгоритмы электронной цифровой подписи. Планируется выполнить аппаратную реализацию криптографических алгоритмов непосредственно на уровне микросхемы с использованием современных технологий проектирования электронных устройств.

В этой связи ставится задача анализа современных методов проектирования и производства интегральных схем. Такая аналитика необходима для определения оптимальных возможностей организации производства полупроводниковых микросхем в Республике Казахстан, с учётом требований по уровню технологического контроля, локализации процессов и перспектив дальнейшей коммерциализации полученных результатов. Разработка отечественного криптоконтроллера на уровне готовности к промышленному производству будет способствовать укреплению цифрового суверенитета, научного и кадрового потенциала в области микроэлектроники и кибербезопасности Республики Казахстан.

Цель настоящей работы является анализ глобальных тенденций развития полупроводниковой индустрии, изучение технологических особенностей и экономических аспектов производства интегральных схем, а также определение направлений развития полупроводниковой промышленности в Республике Казахстан, в том числе в целях разработки аппаратных средств безопасности.

2 Методы исследования

Анализ современных методов проектирования и производства интегральных схем проведен на основе сравнения типов технологических узлов, используемых в полупроводниковой индустрии. На протяжении десятилетий динамика эволюции узлов описывалась законом Мура, предполагающим регулярное уменьшение размеров транзисторов и рост числа элементов на кристалле [11].

Ранние технологические процессы (process node, процессорный узел или node) именовались по минимальному размеру элемента транзистора Gate Length (Lg) – расстоянию между двумя контактами транзистора (drain и source), которое указывает на то, как быстро и эффективно работает транзистор (рис.1). Однако это перестало соответствовать действительности в 1994-1997 годах [12]. До узла 0,25 мкм Intel начала вводить более агрессивное масштабирование длины затвора. Например, процесс 0,25 мкм имел Lg = 0,20 мкм, а процесс 0,18 мкм имел GL = 0,13 мкм (на узел вперед), то есть «процессный узел» был фактически больше длины затвора. С тех пор термин стал ещё более маркетинговом, теперь даже при описании современных транзисторов может не использоваться термин длина затвора, но при этом техпроцессы продолжают называться 5, 3 или 2 нм.

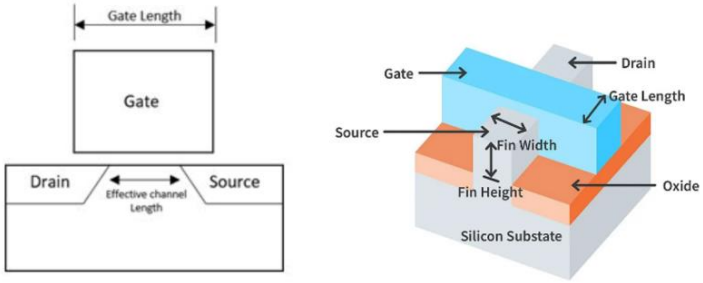

Рисунок – 1 Длина затвора для планарных и 3D транзисторов

На рисунке 1 также представлен вид непланарного FinFET (Fin Field-Effect Transistor), используемого при разработке современных процессоров. Это модификация традиционного металл-оксидного транзистора, которая позволяет преодолеть ограничения планарных CMOS (Complementary Metal-Oxide-Semiconductor) транзисторов, особенно при уменьшении длины затвора.

В настоящее время используются следующие термины, определяющие группы технологических процессов, через которые можно также проследить преемственность технологий типов планарных транзисторов, литографических процессов и архитектурных решений:

– зрелые узлы (mature node, Lg ≥ 28 нм), применяются преимущественно в автомобильной, военной и космической электронике; их ключевыми характеристиками являются низкая стоимость, надёжность и устойчивость к внешним воздействиям [13];

– промежуточные узлы (intermediate, Lg ~10–22/28 нм), связаны с переходом к трёхмерным транзисторным структурам (FinFET) и внедрением усовершенствованных DUV- и EUV-литографических процессов [14];

– передовые узлы (leading-edge, Lg ≤ 7 нм), реализуются на базе FinFET и Gate-All-Around (GAA) FET (рис. 2), обеспечивая максимальную плотность интеграции и производительность при значительном увеличении стоимости и сложности производства [15].

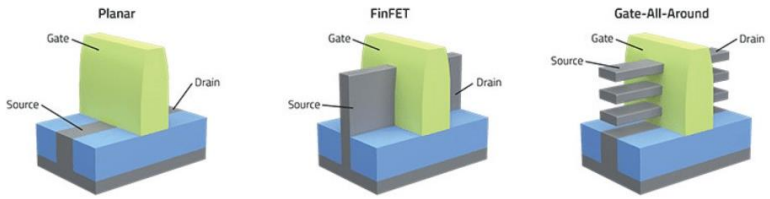

Рисунок 2 – Сравнение архитектур планарных CMOS, FinFET и GAA транзисторов

3 Результаты исследований

Анализ методов проектирования современных электронных узлов показа, что представленной выше разделение на группы технологических узлов отражает не только инженерные особенности масштабирования. Выбор того или иного типа технологического узла зависит от предполагаемой сферы применения (табл. 1), а также глобального распределения производственных компетенций.

Таблица 1 – Распределение технологий в зависимости от сферы применения конечной продукции

Отрасль	Преобладающая технология
Автомобильная	40-90 нм для ECU/MCU; 7-5 нм
Бытовые приборы	180-130 нм MCU/SoC
IoT	50-180 нм
Космос	180-65 нм (радиационно стойкие FPGA/MCU/ASIC)
Военная техника	180-65 нм
Ноутбуки/ПК	5-3 нм (CPU/GPU/SoC); 10-28 нм для отдельных чиплетов/IO
Смартфоны	4-3 нм

Возможности по освоению тех или иных узлов в значительной степени определяются уровнем национальной технологической базы, инвестициями и доступом к современному оборудованию. В результате мировая полупроводниковая промышленность характеризуется высокой степенью географической концентрации, когда лишь ограниченное число стран располагает производственными мощностями на передовых узлах. В результате несколько стран (Тайвань, Южная Корея и США) контролируют узлы 3-2 нм, компании Японии уверенно производят в диапазоне 40 нм и частично на 6/7 нм, а европейские предприятия ограничены уровнем 12-18 нм, Россия располагает производственными возможностями на уровне 90–180 нм. Более подробная информация распределению минимальных возможностей по странам приведена в таблице 2.

Таблица 2 – Минимальные технологии производства планарных транзисторов с распределением по странам

Страна / регион	Минимальный технологический процесс на своей территории
Тайвань	3 нм / 2 нм [16]
Южная Корея	3 нм/ 2 нм – с 2025–2027 гг. [17]
США	3 нм с учетом строящегося завода TSMC в Аризоне [18]
Япония	JASM – 6/7 нм [19], Rapidus – 40 нм [20]
Китай	7 нм [21]
Европа (континент)	16/12 нм [22], 18 нм [23]
Ирландия	3 нм (34Fab Intel node) [24]
Израиль	16/14 нм [25]
Сингапур	22 нм [26]
Россия	90 нм [27]

Приведённые в таблице 2 страны направляют финансирование на усовершенствование технологических процессов, кроме того есть новые страны, которые врываются в индустрию с целью сокращения затрат на потребление чипов внутри страны или на рост ВВП. На основе анализа исследований планов и инвестиционных проектов таких стран как Украина, Индия, Германия и Япония, можно выделить ориентировочные стоимости таких фабрик, данные по которым приведены в таблице 3.

Таблица 3 – Оценка стоимости проектов по старту фабрикации полупроводниковых чипов

Тип завода	Уровень технологии	Инвестиции, $	Ключевые достоинства	Ключевые недостатки
Mature node	~180-28 нм	$1–3 млрд [28]	Полный контроль; нацпроект, развивающий смежные отрасли; независимость (при локализации поставок)	Очень высокие фиксированные затраты; риски недозагрузки и устаревания; потребность в кадрах-экспатах
Intermediate node	< 28 нм	$5-10+ млрд [29]	Доступ к передовым чипам внутри страны; престиж и лидерство; потенциал экспорта глобально	Экстремальные затраты; почти недостижимо без международного консорциума; нужен огромный рынок сбыта

Fabless-модель (от англ. fabrication-less – «без производства») [30] представляет собой бизнес-модель полупроводниковой индустрии, при которой компания специализируется исключительно на разработке и проектировании интегральных микросхем, передавая их производство сторонним фабрикам-подрядчикам (foundries). Данная модель, используемая такими лидерами как Qualcomm, NVIDIA, AMD и Apple, позволяет концентрировать ресурсы на инновационной составляющей, в то время как капиталоёмкое производство осуществляется специализированными фабриками. Важным инструментом для стартапов являются программы MPW (Multi Project Wafer) [31], позволяющие нескольким проектам совместно использовать одну кремниевую пластину для изготовления прототипов по стоимости от $10,000 до $100,000, что делает доступным создание прототипов даже для небольших команд и университетов на передовых процессах до 7 нм и 5 нм.

4 Обсуждение научных результатов

В современных условиях Республика Казахстан не имеет собственной производственной базы, что обусловливает необходимость выбора стратегического пути: развитие fabless-модели, предполагающей проектирование внутри страны и производство за её пределами, либо формирование национальных производственных мощностей на зрелых узлах для обеспечения внутренних потребностей.

Вопрос локализации напрямую связан не только с экономическими показателями, но и с безопастностью, так как необходим контроль производства микросхем, которые непосредственно используются в сфере безопастности. В рамках работы ведется разработка специализированной микросхемы (ASIC – application specific integrated circuit) для выполнения задач реализации аппаратного исполнения криптографических алгоритмов, которые применяются в средствах аутентификации пользователей, ЭЦП и, потенциально, в устройствах обеспечивающих защищенную связь.

Современные протоколы аутентификации (например, FIDO2) и электронная подпись (ЭЦП) могут иметь программную, аппаратную и программно-аппаратную реализацию. Однако аппаратная реализация считается наиболее защищенной и является обязательной для некоторых применений, например SP 800-63B [32], где средства аутентификации и идентификации должны быть аппаратами для уровня AAL3, или FIPS 201-3 [33], где для уровня выше 2 должно обеспечиваться физическая защита уровня 3 по FIPS 140 [34]. Их ключевое преимущество заключается в изоляции криптографических операций от операционной системы и пользовательского окружения, разделение интерфейсов, что существенно снижает риск компрометации ключей.

Мировая практика демонстрирует, что наибольшую надёжность и производительность в области криптографической защиты обеспечивают решения на основе специализированных интегральных схем (ASIC). Такой подход позволяет реализовывать алгоритмы непосредственно на аппаратном уровне, интегрируя их в архитектуру элементарных логических структур (планарных транзисторов микросхем). В отличие от этого, использование микроконтроллеров общего назначения, а также микроконтроллеров с расширенными функциями безопасности не может считаться полностью аппаратным решением. В подобных случаях криптографический алгоритм (например, ГОСТ Р 34.12-2015) хранится в виде программного кода, что теоретически повышает уязвимость системы к различным видам атак. Следует отметить, что на рынке существуют устройства аутентификации, построенные на основе микроконтроллеров. Примерами являются решения компаний Yubico, Google Titan, а также ряд промышленных токенов, используемых в финансовом секторе. Однако зависимость от зарубежных микросхем существенно ограничивает возможности их сертификации по национальным стандартам как средств с аппаратной реализацией криптографических алгоритмов. Более того, отсутствие контроля над цепочкой проектирования, производства и поставки создаёт риски технологической уязвимости. В этой связи ключевым условием обеспечения доверенной инфраструктуры является развитие собственных производственных возможностей по созданию микросхем с криптографическими функциями, которые аппаратно поддерживают необходимые алгоритмы.

Создание отечественного криптоконтроллера предполагает решение комплекса технологических и организационных задач. Во-первых, требуется определить оптимальный класс технологического узла. Для задач безопасности не всегда необходимы узлы ≤7 нм,

зрелые технологии на уровне 90-130 нм остаются востребованными благодаря надёжности, радиационной стойкости и более низким затратам на производство.

Во-вторых, важным направлением является аппаратная реализация криптографических алгоритмов. Переход от программных решений к аппаратным повышает эффективность и стойкость к атакам по сторонним каналам (side-channel attack) на микроконтроллеры, что критично при реализации алгоритмов ЭЦП и протокола FIDO2.

В-третьих, путь к созданию полупроводниковых микросхем (серийный IC или специализированный ASIC) целесообразно строить поэтапно и следует минимально начать с создания собственной архитектуры, которую можно производить на внешних фабриках под своим контролем. При необходимости можно делать приемку 1-5% готовой продукции на рентген контроле для выявления аппаратных закладок.

Проектирование архитектуры, в свою очередь, можно также разложить на этапы: на первом этапе – про Приведённые в таблице 2 страны направляют финансирование на усовершенствование технологических процессов, кроме того есть новые страны, которые врываются в индустрию с целью сокращения затрат на потребление чипов внутри страны или на рост ВВП. На основе анализа исследований планов и инвестиционных проектов таких стран как Украина, Индия, Германия и Япония, можно выделить ориентировочные стоимости таких фабрик, данные по которым приведены в таблице 3.

тотипирование на ПЛИС, на втором – оптимизация архитектуры и перенос в специализированную интегральную схему. Такой подход соответствует мировой практике проектирования и позволяет минимизировать затраты при сохранении высокого уровня надёжности.

5 Заключение

Современное развитие полупроводниковой индустрии и рост киберугроз определяют необходимость создания отечественных решений в области аппаратной криптографии. Криптоконтроллеры и аппаратные токены занимают центральное место в архитектуре доверенной среды, обеспечивая защиту от внешних воздействий и снижение зависимости от зарубежных технологий.

Для Республики Казахстан разработка отечественного криптоконтроллера представляется стратегически значимым направлением. Наиболее реалистичной траекторией развития полупроводниковой промышленности является реализация fabless-модели, что позволит одновременно получить доступ к передовым технологиям и формировать собственный кадровый и научный потенциал. В работе показано, что для задач безопасности не всегда требуются передовые узлы. Аппаратная реализация криптографических алгоритмов на специализированных интегральных схемах (ASIC) считается более надёжной, чем программные решения на микроконтроллерах общего назначения. Предлагается поэтапный подход к созданию отечественного криптоконтроллера, начиная с прототипирования на программируемых логических интегральных схемах и последующего переноса архитектуры в ASIC.

Список литературы

1. A 220-GHz Energy-Efficient High-Data-Rate Wireless ASK Transmitter Array / B. Hadidian et al // IEEE Journal of Solid-State Circuits. – 2022. – Vol. 57, № 6. – P. 1623-1634.
2. Calazans N.L.V. Robust and energy-efficient hardware: the case for asynchronous design / N.L.V. Calazans, T.A. Rodolfo, M.L.L. Sartori // Journal of Integrated Circuits and Systems. – 2021. – T. 16, № 2. – P. 1-11.
3. Matuska S. Internet of Things Platform for Rapid Development and Learning / S. Matuska, R. Hudec, P. Kamencay // 2019 17th International Conference on Emerging eLearning Technologies and Applications (ICETA). – IEEE, 2019. – P. 512-517.
4. Bhalerao S.R. Flexible, solution-processed, indium oxide (In2O3) thin film transistors (TFT) and circuits for internet-of-things (IoT) / S.R. Bhalerao, D. Lupo, P.R. Berger // Materials Science in Semiconductor Processing. – 2022. – Vol. 139. – P. 106354.
5. Survey of photonic and plasmonic interconnect technologies for intra-datacenter and high-performance computing communications / C.A. Thraskias et al // IEEE Communications Surveys & Tutorials. – 2018. – Vol. 20, № 4. – P. 2758-2783.
6. High-brightness, high-speed, and low-noise VCSEL arrays for optical wireless communication / Z. Khan et al // IEEE Access. – 2021. – Vol. 10. – P. 2303-2317.

7. Assessing the contribution of semiconductors to the sustainable development goals (SDGs) from 2017 to 2022 / S. Hsieh et al // Heliyon. – 2023. – Vol. 9, № 11. – P. 1-10.
8. WSTS Semiconductor Market Forecast Spring 2024 [electronic resource]. – 2024. – URL: https://www.wsts.org/76/103/WSTS-Semiconductor-Market-Forecast-Spring-2024 (date of request: 12.03.2025).
9. Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure User Identity / M.I.M. Yusop et al // IEEE Access. – 2025. – Vol. 13. – P. 13919-13943.
10. Okeke F., Pankratyeva A. FIDO2 & Passkeys: The Future of Passwordless Authentication [electronic resource]. – 2025. – URL: https://www.techopedia.com/passwordless-authentication-fido2-passkeys (date of request: 12.03.2025 г.).
11. Song J. The history and trends of semiconductor materials' development / J. Song // Journal of Physics: Conference Series. – IOP Publishing, 2023. – Vol. 2608, № 1. – P. 012019.
12. Moore S.K. A Better Way to Measure Progress in Semiconductors [electronic resource]. – 2020. – URL: https://spectrum.ieee.org/a-better-way-to-measure-progress-in-semiconductors (date of request: 12.03.2025 г.).
13. Theis T.N. The End of Moore's Law: A New Beginning for Information Technology / T.N. Theis, H.-S.P. Wong // Computing in Science & Engineering. – 2017. – Vol. 19(2). – P. 41-50.
14. Yin H. Advanced Transistor Process Technology from 22-to / H. Yin, J. Yao // Complementary Metal Oxide Semiconductor. – 2018. – Chapter 2. – P. 11-26.
15. Das U.K. Opportunities in device scaling for 3-nm node and beyond: FinFET versus GAA-FET versus UFET / U.K. Das, T.K. Bhattacharyya // IEEE transactions on electron devices. – 2020. – V. 67, № 6. – P. 2633-2638.
16. Tung C.-Y. Taiwan and the global semiconductor supply chain [electronic resource]. – 2020. – URL: https://roc-taiwan.org/uploads/sites/86/2024/02/February-2024-Issue.pdf. (date of request: 12.03.2025 г.).
17. Friedman A.History is made! Samsung beats out TSMC and starts shipping 3nm GAA chipsets [electronic resource]. – 2022. – URL: https://www.phonearena.com/news/samsung-first-to-ship-3nm-gaa-chips_id141505 (date of request: 12.03.2025 г.).
18. TSMC to Invest $100B in US Chip Manufacturing Expansion [electronic resource]. – 2025. – URL: https://manufacturing-today.com/news/tsmc-to-invest-100b-in-us-chip-manufacturing-expansion/ (date of request: 12.03.2025 г.).
19. JASM Set to Expand in Kumamoto Japan Expansion [electronic resource]. – 2024. – URL: https://www.sony-semicon.com/en/news/2024/2024020601.html (date of request: 12.03.2025 г.).
20. Grant-Chapman H., McGee T. Japan's Chip Challenge: Semiconductor Policy for the Data Centre Era [electronic resource]. – 2024. – URL: https://cetas.turing.ac.uk/publications/japans-chip-challenge-semiconductor-policy-data-centre-era (date of request: 12.03.2025 г.).
21. Castellano R. How China Is Reaching 5nm Without EUV, and How That Impacts ASML [electronic resource]. – 2025. – URL: https://drrobertcastellano.substack.com/p/how-china-is-reaching-5nm-without (date of request: 12.03.2025 г.).
22. European Semiconductor Manufacturing Company (ESMC). What we do [electronic resource]. – 2025. – URL: https://www.esmc.eu/en/who_we_are.html (date of request: 12.03.2025 г.).
23. France Must Attain 2–10nm Advanced Semiconductor Manufacturing Capabilities [electronic resource]. – 2025. – URL: https://www.trendforce.com/news/2025/06/18/news-macron-france-must-attain-2-10nm-advanced-semiconductor-manufacturing-capabilities/ (date of request: 12.03.2025 г.).
24. Gerstl S. Ireland introduces 3-nanometer process in Europe [electronic resource]. – 2025. – URL: https://www.all-about-industries.com/ireland-introduces-3-nanometer-process-in-europe-a-2c64c062331ab02d49ffc1c49f65a9f2/ (date of request: 12.03.2025 г.).
25. Challenges for Israeli Semiconductor Startups Manufacturing on Advanced Nodes [electronic resource]. – 2025. – URL: https://arnontl.com/news/challenges-for-israeli-semiconductor-startups-manufacturing-on-advanced-nodes/ (date of request: 12.03.2025 г.).
26. Grasping the Trend: Chip Wars Escalate In The AI Era, Singapore's Semiconductor Sector Emerges Strong [electronic resource]. – 2025. – URL: https://www.a-star.edu.sg/News/astarNews/news/features/singapore-semiconductor-rise-ai-chip-wars (date of request: 12.03.2025 г.).

27. Shilov A. Russia on track to manufacture 28nm chips in domestic fabs by 2030, 19 years after tech first debuted [electronic resource]. – 2025. – URL: https://www.tomshardware.com/tech-industry/russia-says-its-on-track-to-manufacture-28nm-chips-in-its-own-fabs-by-2030-the-tech-first-debuted-15-years-ago (date of request: 12.03.2025 г.).
28. Microelectronics. Robert Bosch Semiconductor Manufacturing Dresden: Interview with Dr. Christian Koitzsch, Plant Manager [electronic resource]. – 2025. – URL: https://silicon-saxony.de/en/robert-bosch-semiconductor-manufacturing-dresden-interview-with-dr-christian-koitzsch-plant-manager/ (date of request: 12.03.2025 г.).
29. Giant leap for India Semiconductor Mission: Cabinet approves three more semiconductor units [electronic resource]. – 2024. – URL: https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2010132 (date of request: 12.03.2025 г.).
30. Singh K.B. Manufacturing of Semiconductor Chips: From Their Origins to the Current Automotive Chip Crisis / K.B. Singh, S.C. Misra // IEEE Engineering Management Review. – 2024. – P. 1-19.
31. Çeliker H. Multi-project wafers for flexible thin-film electronics by independent foundries / H. Çeliker, W. Dehaene, K. Myny // Nature. – 2024. – V. 629, № 8011. – P. 335-340.
32. Draft nist special publication 800-63b digital identity guidelines / P.A. Grassi et al // National Institute of Standards and Technology (NIST). – 2016. – V. 27. – P. 1-46.
33. PUB F. Personal Identity Verification (PIV) of Federal Employees and Contractors. [electronic resource]. – 2022. – URL: https://csrc.nist.gov/pubs/fips/201-3/final (date of request: 12.03.2025 г.).
34. FIPS 140-3. Security Requirements for Cryptographic Modules [electronic resource]. – 2022. – URL: https://csrc.nist.gov/pubs/fips/140-3/final (date of request: 12.03.2025 г.).

Информация о финансировании

Данное исследование финансируется Комитетом науки Министерства науки и высшего образования Республики Казахстан (грант № AP26103891).

Н. Глазырина[1], А. Шайханова[1]*, К. Аяпбергенов[1], И. Сенюшин[1], Р. Мұратхан[2]
[1]TSARKA R&D ЖШС,
[2]TSARKA LABS ЖШС,
010000, Қазақстан Республикасы, Астана қ., Қабанбай батыр даңғылы 51/1
*e-mail: shaikhanova_ak@enu.kz

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДА КРИПТОБАҚЫЛАУДЫ ҚҰРУ ҮШІН ИНТЕГРАЦИЯЛЫҚ ТІЛБЕЛЕРДІ ӨНДІРУДІҢ ҚАЗІРГІ ӘДІСТЕРІН ТАЛДАУ

Мақалада Қазақстан Республикасында криптографиялық контроллерді құру мақсатында интегралды микросхемалар өндірісінің заманауи әдістері зерттеледі. Жұмыста жартылай өткізгіштер өнеркәсібіндегі әлемдік тенденциялар, интегралдық микросхемалар өндірісінің технологиялық ерекшеліктері мен экономикалық аспектілері талданады, сондай-ақ қауіпсіздік техникасын дамыту үшін Қазақстанда жартылай өткізгіш өнеркәсібінің даму бағыттары айқындалады. Зерттеу әдістемесі дамыған, орта және алдыңғы қатарлы интеграциялық және өнімділік мүмкіндіктері бар елдерде жүзеге асырылатын әртүрлі технологиялық процестерді, жоспарларды және жобаларды салыстыруға негізделген заманауи интегралды схемаларды жобалау және өндіру әдістерін талдауды қамтиды. Зерттеу нәтижелері көрсеткендей, жеке интегралды схемалар өндірісінің базасы жоқ Қазақстан Республикасы үшін оңтайлы тәсіл ел ішінде дизайнмен және үшінші тарап құю зауыттарында өндірілетін фабельсіз модельді әзірлеу болып табылады. Бұл жетілген түйіндерде ұлттық өндірістік қуаттарды құрумен салыстырғанда айтарлықтай инвестицияны қажет етпейді. Бұл мақалада бағдарламаланатын логикада прототиптеуден бастап, кейіннен архитектураны мамандандырылған интегралды схемаға көшіруден бастап, отандық криптоконтроллерді құрудың кезеңдік тәсілі ұсынылады. Жұмыстың практикалық құндылығы Қазақстанда жартылай өткізгіш микрочиптер өндірісін ұйымдастырудың оңтайлы мүмкіндіктерін анықтауда және өнеркәсіптік өндіріске дайын деңгейде отандық криптоконтроллерді әзірлеуде жатыр.

Түйін сөздер: *ақпараттық қауіпсіздік, криптографиялық контроллер, интегралды схема, аппараттық қамтамасыз ету, жартылай өткізгіш өнеркәсібі, технологиялық түйін, электронды қолтаңба, FIDO, fabless модель.*

N. Glazyrina[1], A. Shaikhanova[1]*, K. Ayapbergenov[1], I. Seniushin[1], R. Muratkhan[2]
[1]TSARKA R&D LLP,
[2]TSARKA LABS LLP,
010000, Republic of Kazakhstan, Astana, Kabanbay Batyr Avenue 51/1
*e-mail: shaikhanova_ak@enu.kz

ANALYSIS OF MODERN METHODS FOR PRODUCING INTEGRATED CIRCUITS FOR CREATION OF A CRYPTOCONTROLLER IN THE REPUBLIC OF KAZAKHSTAN

The article explores modern integrated circuit production methods with the aim of creating a crypto controller in the Republic of Kazakhstan. The paper analyzes global trends in the semiconductor industry, technological features and economic aspects of integrated circuit production, and also identifies directions for the development of the semiconductor industry in Kazakhstan for the development of security hardware. The research methodology includes an analysis of modern integrated circuit design and manufacturing methods, based on a comparison of various technological processes, plans, and projects implemented in countries with mature, intermediate, and leading-edge integration and productivity capabilities. Research results show that for the Republic of Kazakhstan, which lacks its own integrated circuit production base, the optimal approach is to develop a fabless model with design within the country and production at third-party foundries. This doesn't require significant investment compared to building national production capacity in mature nodes. The paper proposes a phased approach to creating a domestic crypto controller, starting with prototyping on programmable logic and subsequently transferring the architecture to a specialized integrated circuit. The practical value of the work lies in the identification of optimal opportunities for organizing the production of semiconductor microchips in Kazakhstan and developing a domestic crypto controller at a level ready for industrial production.

Key words: *information security, crypto controller, integrated circuit, hardware implementation, semiconductor industry, technological node, electronic signature, FIDO, fabless model*

Сведения об авторах

Наталья Сергеевна Глазырина – PhD, ассоциированный профессор, координатор научный проектов, ТОО «TSARKA R&D», г. Астана, Республика Казахстан; e-mail: glazyrina_ns_1@enu.kz. ORCID: https://orcid.org/0000-0002-0259-774X.

Айгуль Кайрулаевна Шайханова* – PhD, ассоциированный профессор, координатор научный проектов, ТОО «TSARKA R&D», г. Астана, Республика Казахстан; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Камиль Муратович Аяпбергенов – системный инженер, ТОО «TSARKA R&D», г. Астана, Республика Казахстан; e-mail: ayapbergenov.kamil@gmail.com. ORCID: https://orcid.org/0009-0006-3906-1873.

Игорь Анатольевич Сенюшин – проектный менеджер, ТОО «TSARKA R&D», г. Астана, Республика Казахстан; e-mail: sigor@cybersec.kz. ORCID: https://orcid.org/0009-0008-4479-4478.

Райхан Муратхан – PhD, научный сотрудник ТОО «TSARKA Labs», г. Астана, Республика Казахстан; e-mail: raikhan.muratkhan@mail.ksu.kz. ORCID: https://orcid.org/0000-0002-2030-8948.

Авторлар туралы мәліметтер:

Наталья Сергеевна Глазырина – PhD докторы, доцент, «TSARKA R&D» ЖШС ғылыми жоба үйлестірушісі, Астана қ., Қазақстан Республикасы; e-mail: glazyrina_ns_1@enu.kz. ORCID: https://orcid.org/0000-0002-0259-774X.

Айгүл Қайрулақызы Шайханова* – PhD докторы, доцент, «TSARKA R&D» ЖШС ғылыми жоба үйлестірушісі, Астана, Қазақстан Республикасы; e-mail: igul.shaikhanova@gmail.com. ORCID: https://orcid.org/0000-0001-6006-4813.

Камил Мұратұлы Аяпбергенов – «TSARKA R&D» ЖШС инженер-жүйе жөніндегі инженер, Қазақстан Республикасы, Астана қ.; e-mail: ayapbergenov.kamil@gmail.com. ORCID: https://orcid.org/0009-0006-3906-1873.

Игорь Анатольевич Сенюшин – «TSARKA R&D» ЖШС жоба жетекшісі, Астана, Қазақстан Республикасы; e-mail: sigor@cybersec.kz. ORCID: https://orcid.org/0009-0008-4479-4478.

Райхан Мұратхан – PhD, ғылыми қызметкер, «TSARKA Labs» ЖШС, Астана, Қазақстан Республикасы; e-mail: raikhan.muratkhan@mail.ksu.kz. ORCID: https://orcid.org/0000-0002-2030-8948.

Information about the authors

Natalya Glazyrina – PhD, associate professor, scientific project coordinator, TSARKA R&D LLP, Astana, Republic of Kazakhstan; e-mail: glazyrina_ns_1@enu.kz. ORCID: https://orcid.org/0000-0002-0259-774X.

Aigul Shaikhanova* – PhD, associate professor, scientific project coordinator, TSARKA R&D LLP, Astana, Republic of Kazakhstan; e-mail: igul.shaikhanova@gmail.com. ORCID: https://orcid.org/0000-0001-6006-4813.

Kamil Ayapbergenov – Systems Engineer, TSARKA R&D LLP, Astana, Republic of Kazakhstan; e-mail: ayapbergenov.kamil@gmail.com. ORCID: https://orcid.org/0009-0006-3906-1873.

Igor Seniushin – Project Manager, TSARKA R&D LLP, Astana, Republic of Kazakhstan; e-mail: sigor@cybersec.kz. ORCID: https://orcid.org/0009-0008-4479-4478.

Raikhan Muratkhan – PhD, Researcher, TSARKA Labs LLP, Astana, Republic of Kazakhstan; e-mail: raikhan.muratkhan@mail.ksu.kz. ORCID: https://orcid.org/0000-0002-2030-8948.

Поступила в редакцию 20.07.2025
Поступила после доработки 20.08.2025
Принята к публикации 21.08.2025

https://doi.org/10.53360/2788-7995-2025-3(19)-5

ҒТАХР: 50.47.29

Қ. Махамбетов*, Б.А. Бельгибаев[1], N. Kunicina[2]
[1]Әл-Фараби атындағы Қазақ ұлттық университеті,
050040, Қазақстан Республикасы, Алматы қ., Аль-Фараби к-сі, 71
[2]Riga Technical University
LV-1048, Latvia, Riga, Ķīpsalas Street, 6A
*e-mail: 1998kaldybek@gmail.com

ТАМАҚ ӨНЕРКӘСІБІНДЕ ЦИФРЛЫҚ ЕГІЗДЕРДІ ҚҰРУ ҮШІН MATLAB PDE TOOLBOX КӨМЕГІМЕН ТЕРМОДИНАМИКАЛЫҚ ПРОЦЕСТЕРДІ МОДЕЛЬДЕУ

Аңдатпа: *Мақалада MATLAB PDE Toolbox көмегімен тамақ өнеркәсібінің өндіріс жүйелеріндегі термодинамикалық процестерді модельдеу тәсілі қарастырылады. Зерттеудің негізгі мақсаты – жылу процестерін имитациялауға және өндірістік операцияларды оңтайландыруға мүмкіндік беретін цифрлық егіздерді құру. Зерттеу барысында модельдеудің дәлдігі мен сенімділігін қамтамасыз ететін Нейман және Дирихле шекаралық шарттарын ескере отырып, жылу өткізгіштік теңдеулерін қолдануға баса назар аударылады. 2D кеңістігіндегі температура өрістерінің динамикалық өзгерістерін көрсететін есептеу эксперименттерінің нәтижелері берілген. Температураның таралуына жылу өткізгіштік, тығыздық және меншікті жылу сыйымдылығы сияқты физикалық параметрлердің әсеріне басты назар аударылады. Алынған мәліметтерді тамақ өнеркәсібіндегі өндірістік процестердің энергия тиімділігі мен сапасын арттыру үшін пайдалануға болады.*

Зерттеу нәтижесінде MATLAB PDE Toolbox жүйесінде температуралық өрістерді сипаттайтын модель әзірленді. Әзірленген модель цифрлық егіздер саласындағы әрі қарай зерттеулерге және SIEMENS NX сияқты өнеркәсіптік модельдеу құралдарымен, сондай-ақ PML платформаларымен интеграциялау үшін негіз болады. Осы зерттеу барысында модельдің оңтайлы параметрлерін анықтау үшін әртүрлі жылу беру коэффициенттері мен шекаралық шарттар сыналған. Мақаланың соңында ұсынылған соңғы нәтиже термодинамикалық процестердің біркелкі және дұрыс таралуын көрсетеді, ұсынылған тәсілдің тиімділігін растайды. Болашақта бұл тәсілді термиялық процестерді талдауға ғана емес, сонымен қатар технологиялық процестердің бейімділігі мен тиімділігін арттыра отырып, термиялық өңдеуді басқарудың интеллектуалды жүйелерін дамытуға мүмкіндік беретін күрделі виртуалды өндіріс жүйелерін құру үшін пайдалануға болады.

Түйін сөздер: *цифрлық егіздер, жылу беру, MATLAB PDE Toolbox, FEM, жылу теңдеуі, шекаралық шарттар, цифрлық модельдеу, температуралық өрісті талдау, энергия тиімділігі, жылулық процесті оңтайландыру.*

Кіріспе

Тамақ өнеркәсібіндегі технологиялық процестерді жобалау және оңтайландырудың заманауи тәсілдері цифрлық егіз тұжырымдамасын белсенді түрде қолданады [1]. Бұл виртуалды модельдер өндіріс жүйелерінің әрекетін нақты уақыт режимінде талдауға және болжауға мүмкіндік береді, осылайша олардың тиімділігін арттыруға, энергия шығындарын азайтуға және өнім сапасын жақсартуға көмектеседі [2].