DOI:10.33942/sit1366 УДК: 004.056

АНАЛИТИЧЕСКИЙ ОБЗОР ТЕХНОЛОГИЙ ПОСТРОЕНИЯ АППАРАТНО-ОРИЕНТИРОВАННЫХ ОБЛАЧНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ С ПРИМЕНЕНИЕМ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Корякин С.В.
Кыргызско-Германский институт прикладной информатики, старший преподаватель,
Институт машиноведения автоматики и геомеханики НАН КР, научный сотрудник, E-mail: srgkoryakin1@gmail.com

Аннотация. *В статье представлен аналитический обзор технологий построения аппаратно-ориентированных облачных систем защиты информации с применением нейросетевых технологий. Рассматриваются основные подходы к интеграции аппаратных средств в инфраструктуру облачных вычислений для повышения уровня информационной безопасности. Специальное внимание уделено применению нейросетевых алгоритмов для автоматизации обнаружения угроз, адаптивного управления доступом и повышения надежности защиты данных в облачных системах. Проанализированы существующие решения, выделены их преимущества и недостатки, а также предложены перспективные направления развития аппаратно-ориентированных систем на основе нейросетевых технологий для обеспечения защиты информации.*

Ключевые слова: *аппаратная безопасность; облачная защита данных; нейронные сети; анализ киберугроз; распределенные вычисления; защита конфиденциальности; адаптивные системы безопасности; методы глубокого обучения; угрозы информационной безопасности; интеллектуальные алгоритмы защиты.*

НЕЙРОНДУК ТЕХНОЛОГИЯЛАРДЫ КОЛДОНУУ МЕНЕН АППАРАТТЫК БАГЫТТАЛГАН МААЛЫМАТТЫ КОРГОО БУЛУТ СИСТЕМАЛАРЫН ТҮЗҮҮ ТЕХНОЛОГИЯЛАРЫ БОЮНЧА АНАЛИТИКАЛЫК ОБЗОРУ

Корякин С.В.
Кыргыз-Герман прикладык информатика институту ага окутуучу,
Кыргыз Республикасынын Улуттук илимдер академиясынын Машина куруу, автоматика жана геомеханика институту, илимий кызматкер, E-mail: srgkoryakin1@gmail.com

Аннотация*. Макалада нейрондук технологияларды колдонуу менен аппараттык багытталган маалыматты коргоо булут системаларын түзүү технологиялары боюнча аналитикалык обзор сунушталат. Маалыматтык коопсуздукту жогорулатуу максатында аппараттык каражаттарды булут эсептөөлөр инфраструктурасына интеграциялоо боюнча негизги ыкмалар каралат. Коркунучтарды автоматтык түрдө аныктоо, адаптивдүү кирүү мүмкүнчүлүгүн башкаруу жана булут системаларында маалыматты коргоо ишенимдүүлүгүн жогорулатуу үчүн нейрондук алгоритмдерди колдонууга өзгөчө көңүл бурулат. Мында учурдагы чечимдер анализденип, алардын артыкчылыктары жана кемчиликтери белгиленип, маалыматты коргоону камсыз кылуу үчүн нейрондук технологияларга негизделген аппараттык багытталган системаларды өнүктүрүүнүн келечектүү багыттары сунушталат.*

Негизги сөздөр: *аппараттык коопсуздук; булутта маалыматты коргоо; нейрондук тармактар; киберкоркунучтарды анализдөө; бөлүштүрүлгөн эсептөөлөр; купуялуулукту коргоо; адаптивдүү коопсуздук системалары; терең үйрөнүү ыкмалары; маалыматтык коопсуздук коркунучтары; интеллектуалдык коргоо алгоритмдери.*

ANALYTICAL REVIEW OF TECHNOLOGIES FOR BUILDING HARDWARE-ORIENTED CLOUD INFORMATION PROTECTION SYSTEMS USING NEURAL NETWORK TECHNOLOGIES

Koryakin S.V.
Kyrgyz-German Institute of Applied Informatics, Research Associate, Senior Lecturer,
Institute of Mechanical Engineering, Automation and Geomechanics National Academy of Sciences of the Kyrgyz Republic, Research Associate, E-mail: srgkoryakin1@gmail.com

Abstract. *This article presents an analytical review of technologies for developing hardware-oriented cloud information security systems using neural network technologies. The primary approaches to integrating hardware solutions into cloud computing infrastructures to enhance information security levels are examined. Special attention is given to the use of neural network algorithms for automating threat detection, adaptive access management, and increasing data protection reliability in cloud systems. Existing solutions are analyzed, highlighting their advantages and disadvantages, and promising directions for the development of hardware-oriented systems based on neural network technologies for ensuring information security are proposed.*

Keywords: *hardware security; cloud data protection; neural networks; cyber threat analysis; distributed computing; privacy protection; adaptive security systems; deep learning methods; information security threats; intelligent protection algorithms.*

Введение. Современное состояние информационной безопасности тесно связано с развитием облачных вычислений, которые предоставляют новые возможности для хранения и обработки данных [1]. В условиях постоянного увеличения масштабов киберугроз и уязвимостей аппаратно-ориентированные облачные системы защиты информации приобретают ключевое значение для обеспечения устойчивости и надежности систем [2]. Интеграция нейросетевых технологий в такие системы позволяет существенно повысить их адаптивность, а также повысить эффективность в обнаружении и предотвращении угроз [3]. В настоящее время необходимость внедрения таких технологий обусловлена значительным ростом объемов данных и усложнением сетевых инфраструктур [4].

На сегодняшний день в качестве основных принципов построения ООСЗИ выделяют:

1. Аппаратная акселерация механизмов безопасности

Одним из важнейших компонентов аппаратно-ориентированных систем является применение специализированных аппаратных средств для выполнения криптографических операций, что повышает устойчивость системы к атакам на низком уровне [5]. В частности, модули **TPM** (Trusted Platform Module) и **HSM** (Hardware Security Module) играют центральную роль в обеспечении изоляции ключевых данных и выполнении операций, связанных с криптографической защитой информации на уровне аппаратуры [6]. Это

существенно снижает вероятность успешной атаки на систему и обеспечивает предсказуемую производительность, что особенно важно в приложениях реального времени.

2. Гибкость облачной инфраструктуры

Аппаратно-ориентированные системы защиты, интегрированные в облачные платформы, обеспечивают динамическое распределение ресурсов, что позволяет адаптировать архитектуру в зависимости от изменяющегося уровня угроз и объема обрабатываемых данных [7]. Такая гибкость архитектуры представляет собой ключевое преимущество, так как позволяет эффективно масштабировать механизмы защиты без ущерба для производительности [8]. Современные облачные провайдеры все чаще предлагают гибридные решения, сочетающие программные и аппаратные компоненты для обеспечения многоуровневой защиты от угроз различного типа.

3. Применение распределенной вычислительной архитектуры

В рамках облачных вычислительных систем необходимо не только эффективно обрабатывать большие объемы данных, но и обеспечивать их безопасность на каждом этапе обработки. Аппаратные модули защиты минимизируют риск уязвимостей даже при успешной атаке на отдельные узлы системы. В этом контексте аппаратная акселерация с использованием **GPU** (Graphics Processing Unit) и **TPU** (Tensor Processing Unit) обеспечивает эффективное выполнение задач анализа данных и обнаружения угроз в реальном времени, что повышает устойчивость всей системы к кибератакам [8].

Считается, что наиболее распространенное применение в системах защиты информации нейросетевые технологии нашли в следующих направлениях:

1) Использование нейросетевых алгоритмов для выявления аномалий,

2) Обучение на больших объемах данных и моделирование угроз,

3) Проактивные меры по предотвращению угроз.

При этом при выявлении аномалий нейросетевые технологии становятся неотъемлемой частью систем анализа трафика и поведенческой активности. Искусственные нейронные сети (ИНС) обучаются на обширных массивах данных и могут обнаруживать сложные шаблоны, которые традиционные методы анализа выявить не могут. Например, алгоритмы глубокого обучения способны обнаруживать сетевые аномалии и адаптироваться к новым типам атак. Это позволяет динамически модифицировать стратегии защиты в зависимости от актуальной ситуации.

Кроме того, следует отметить, что важным аспектом нейросетевых систем является их способность обучаться на больших объемах данных, что дает возможность выявлять даже незначительные отклонения в работе систем. Генеративные модели, такие как **GAN** (Generative Adversarial Networks), используются для моделирования новых типов атак, что расширяет возможности защитных систем по предсказанию потенциальных угроз и позволяет разрабатывать стратегии их предотвращения. Подобные подходы существенно повышают адаптивность систем защиты [7].

Следует отметить, что в процессе функционирования СЗИ, имеющие в своем составе компоненты нейросетевой архитектуры, не ограничиваются лишь реакцией на уже

произошедшие инциденты; они способны предсказывать возможные угрозы на основе анализа поведенческих паттернов. Например, рекуррентные сети и трансформеры позволяют анализировать действия пользователей и устройств в сети, обнаруживая подозрительную активность до их превращения в полноценные кибератаки [7]. Это дает возможность реализовать проактивные меры защиты, такие как изменение политик безопасности в реальном времени и настройка сетевых фильтров, что значительно увеличивает эффективность системы против новых угроз [8].

Считается, что при внедрении нейросетевых технологий в СЗИ как преимущества от их использования, так и сложности в процессе интеграции в архитектуру СЗИ из преимуществ следует выделить высокую точность и адаптивность, поскольку интеграция нейросетевых технологий с аппаратными системами защиты позволяет достичь высокой точности при обнаружении сложных угроз. Использование специализированных вычислительных модулей, таких как **GPU** и **TPU,** способствует ускорению обработки данных и минимизации времени на обнаружение угроз, что критично для быстрого реагирования на инциденты [8].

Кроме того, следует отметить, что одним из основных преимуществ нейросетевых технологий является их способность к автоматизации процессов защиты информации [9]. Нейросети могут автоматически анализировать данные, обновлять правила безопасности и адаптировать стратегии защиты под изменяющиеся условия, минимизируя человеческий фактор и снижая вероятность ошибок. Это особенно важно в моментах, когда киберфизические системы подвержены воздействию масштабных и сложных сетевых атак.

Из недостатков выделяются вычислительные затраты и необходимость в больших объемах данных. Причем, несмотря на высокую эффективность нейросетевых методов, их интеграция в аппаратно-ориентированные системы защиты связана с рядом сложностей. Одна из главных проблем — значительные вычислительные ресурсы, необходимые для обучения нейросетей. Также требуется огромный объем данных для эффективного функционирования подобных систем, что может стать проблемой при недостаточности ресурсов или данных. Кроме того, процесс сбора и обработки данных должен соответствовать требованиям законодательства по защите информации, что может усложнить внедрение системы.

Исходя из вышеизложенного становится очевидным что, разработка аппаратно-ориентированных облачных систем защиты информации с применением нейросетевых технологий представляет собой важный шаг в повышении уровня безопасности данных в условиях роста киберугроз. Интеграция нейросетей с аппаратными компонентами систем защиты позволяет не только повысить точность обнаружения угроз, но и обеспечить высокую адаптивность к новым видам атак, происходящих в реальном времени [9]. Тем не менее, внедрение таких систем требует значительных вычислительных ресурсов, а также соблюдения требований к конфиденциальности данных, что может стать дополнительным вызовом для их эффективной реализации.

Анализ возможностей применения нейросетевых технологий в аппаратно-ориентированных системах защищенного исполнения.

Системы защищенного исполнения (СЗИ) играют ключевую роль в обеспечении информационной безопасности, защищая от угроз как внешнего, так и внутреннего характера. В условиях быстрого роста киберугроз нейросетевые технологии представляют собой прогрессивный подход для повышения функциональности и адаптивности СЗИ. В разделе рассматривается анализ архитектур некоторых типовых нейросетей, их применение в системах защищенного исполнения, а также сравнение имеющихся программно-аппаратных решений, включая технологии программируемой логики (ПЛИС).

На сегодняшний день считается, что Нейросети – это вычислительные структуры, основанные на принципах работы биологических нейронных сетей, способные выявлять и обрабатывать сложные паттерны в многомерных данных. Эффективность различных архитектур нейросетей в задачах классификации, регрессии и анализа временных рядов подтверждается многочисленными исследованиями [10].

Считается, что различные архитектуры нейросетей предназначены для решения специфических задач и обладают уникальными характеристиками. Проводя анализ применения нейросетевых технологий за последние 15 лет можно с уверенностью говорить о том, что разные архитектуры нейросетей разрабатывались для решения специфических задач и имеют свои уникальные особенности (табл.1) [11-13].

В настоящее время наблюдается активный интерес к системам, использующим нейросетевые методы для выявления угроз безопасности киберфизических систем, основными из которых, по мнению экспертов, являются: обнаружение угроз и аномалий, улучшение аутентификации, защита данных.

Таблица 1. Сравнительный анализ архитектур нейросетей

Архитектура	Применение	Преимущества	Недостатки
Сверточные нейросети (CNN)	Обработка изображений	Эффективное извлечение пространственных признаков	Не оптимальны для последовательных данных
Рекуррентные нейросети (RNN)	Анализ временных рядов	Учет контекста и временных зависимостей	Проблема затухающего градиента
Глубокие нейросети (DNN)	Классификация	Моделирование сложных функций	Высокие вычислительные затраты
Сеть прямого распространения	Общие задачи ML	Простота реализации и обучения	Неспособность обрабатывать временные зависимости

Например, в исследованиях процесса обнаружения угроз и аномалий, так называемых MIT исследованиях, применяются сверточные нейросети (CNN) для анализа сетевого трафика с целью выявления аномалий [14].

Из преимуществ следует выделить высокую точность в обнаружении новых, неизвестных ранее типов угроз благодаря глубокому обучению, а также способность адаптироваться к изменениям в сетевом поведении, что обеспечивает про активное реагирование на инциденты, вызванные угрозами информационной безопасности.

В качестве недостатков следует отметить высокие требования к объемам обучающих данных, что, как правило, ограничивает эффективность в условиях недостаточной информации о сигнатурах угроз кибербезопасности КБ, а также значительные вычислительные затраты, особенно при обработке больших объемов данных в реальном времени.

Для улучшения аутентификации применяются различные программно-аппаратные решения, такие как FaceID от Apple и других мировых производителей, и многие другие, которые считаются значительными шагами в улучшении методов аутентификации [15].

Из преимуществ следует выделить возможность повышения уровня безопасности благодаря использованию уникальных биометрических данных, что способствует обеспечению быстрого и удобного процесса аутентификации.

Из недостатков следует выделить уязвимость к подделке биометрических данных, особенно при недостаточной защите СУБД и сетевой инфраструктуры.

Еще одним существенным недостатком является необходимость в качественных обучающих данных для повышения точности распознавания. Для повышения уровня защищенности данных в настоящее время активно разрабатываются алгоритмы шифрования на основе генеративных состязательных сетей (GAN), как, например, решения от IBM Research и многие другие [16]. Из преимуществ данных решений следует выделить динамическое шифрование, способное адаптироваться к изменениям в характере угроз, что улучшает защиту данных потенциальное повышение производительности по сравнению с традиционными методами шифрования.

Недостатками являются сложность реализации и настройки алгоритмов, что как правило требует значительных временных и ресурсных затрат и потребность в высоких вычислительных ресурсах для работы алгоритмов в реальном времени (табл.2).

Считается, что современные решения по обеспечению безопасности киберфизических систем значительно различаются по своим характеристикам и способам реализации. В качестве основных компонентов архитектуры таких решений следует выделить основные, так называемые, программное и аппаратное ядра. В таблице 3 представлены программные решения, применяемые в качестве компонентов программного ядра, выполняющие функции защиты от киберугроз.

В качестве компонентов аппаратного ядра, помимо традиционных способов реализации на базе ЭВМ различного класса, целесообразно использовать решения на базе ПЛИС (FPGA), использование которых предоставляют возможности для реализации

нейросетевых алгоритмов, обеспечивая высокую степень параллелизма и гибкость настройки под конкретные задачи [17]. Например, платформа Xilinx Zynq используется для создания высокопроизводительных аппаратных реализаций CNN. FlexLogix: предлагает программируемую логику для ускорения работы нейросетей с низким энергопотреблением.

Таблица 2. Анализ сравнительных характеристик, применяемых нейросетевых технологий в системах защищенного исполнения

Применение	**Примеры технологий**	**Преимущества**	**Недостатки**
Обнаружение угроз	MIT (CNN)	Высокая точность в обнаружении новых угроз	Значительные требования к обучающим данным
Улучшение аутентификации	FaceID	Повышенная безопасность с использованием биометрии	Уязвимость к подделке данных
Защита данных	IBM (GAN)	Динамическое шифрование, адаптация к угрозам	Сложность реализации алгоритмов

Таблица 3. Сравнительный анализ программно-аппаратных решений в СЗИ

Решение	**Применение**	**Преимущества**	**Недостатки**
Darktrace	Система обнаружения вторжений (IDS)	Автоматическое самообучение, высокая скорость реакции	Возможные ложные срабатывания, зависимость от качества данных
NEC NeoFace	Биометрическая аутентификация	Высокая точность, возможность работы в реальном времени	Необходимость защиты данных, этические вопросы
NVIDIA Jetson	Ускорение нейросетей	Высокая производительность, работа в условиях ограниченных ресурсов	Высокая стоимость, потребность в навыках разработки
Google Coral	Обработка нейросетевых задач	Оптимизация для ML, доступность	Ограниченные возможности по сравнению с FPGA
Xilinx Zynq	Реализация нейросетей на FPGA	Высокая скорость обработки, гибкость конфигурации	Сложность в разработке, высокая стоимость
FlexLogix	Аппаратная реализация ML	Гибкость, адаптивность	Требует специализированных знаний
Achronix	Оптимизация алгоритмов ML	Высокая производительность	Стоимость и сложность разработки

Xilinx: разрабатывает FPGA с высокоскоростными интерфейсами, обеспечивая производительность при выполнении алгоритмов машинного обучения [18].

Преимущества:

- Исключительно высокая скорость обработки данных благодаря параллельной архитектуре.
- Динамическая конфигурация, позволяющая адаптироваться к изменяющимся требованиям.
- Гибкость: ПЛИС позволяют разработчикам адаптировать аппаратное обеспечение под конкретные задачи, оптимизируя производительность и снижая задержки обработки.
- Параллелизм: Высокая степень параллельной обработки данных позволяет существенно увеличить скорость выполнения задач, особенно для ресурсоемких алгоритмов.
- Энергоэффективность: в некоторых случаях FPGA могут обеспечить более низкое потребление энергии по сравнению с традиционными процессорами при выполнении специализированных задач.

Недостатки:

- Сложность проектирования и программирования, что может потребовать значительных усилий и времени.
- Высокие первоначальные инвестиции, что может ограничить использование в небольших проектах.
- Сложность разработки. Процесс проектирования и программирования ПЛИС требует наличия специализированных знаний и навыков, что может стать барьером для многих разработчиков.
- Стоимость. Внедрение ПЛИС может быть дороже по сравнению с другими решениями за счет высокой оплаты труда квалифицированным специалистам, особенно для малых и средних предприятий с ограниченным бюджетом.
- Ограниченная производительность для общих задач. В случаях, когда задачи не требуют высокой параллелизации, производительность ПЛИС может быть ниже, чем у высокопроизводительных процессоров [19].

Таким образом, на современном этапе исследований в области информационной безопасности критически важным становится глубокое понимание особенностей различных технологий. Этот анализ фокусируется на нескольких ключевых параметрах: применение, скорость обработки, обучаемость, гибкость и сложность реализации, что позволяет оценить их эффективность в контексте систем защищенного исполнения (табл.4).

Рассмотрим практические примеры применения технологий, указанных в таблице 4 в СЗИ:

1. CNN в обнаружении угроз: в качестве, примера можно рассмотреть систему Darktrace, использующую CNN для анализа сетевого трафика. Она демонстрирует высокую точность и способность к самообучению, позволяя идентифицировать новые виды угроз на

основе минимального объема исходных данных. Однако, высокие требования к вычислительным ресурсам могут стать узким местом.

- Таблица 4. Сравнительный анализ различных технологий в СЗИ

Параметр	CNN	RNN	ПЛИС
Применение	Обнаружение объектов, видеоанализ	Анализ временных рядов, обработка естественного языка	Аппаратные реализации нейросетей
Скорость обработки	Высокая (при наличии GPU)	Средняя (зависит от длины последовательности)	Очень высокая (параллельная обработка)
Обучаемость	Требует большого объема данных	Требует времени для обучения	Настройка под специфические задачи
Гибкость	Ограниченная (зависит от архитектуры)	Средняя (можно адаптировать)	Высокая (многофункциональность)
Сложность реализации	Умеренная	Высокая	Высокая (требует специфических навыков)

2. RNN в анализе временных рядов: использование рекуррентных нейросетей в анализе логов систем безопасности позволяет выявлять аномалии и предсказывать потенциальные угрозы, основываясь на исторических данных. Тем не менее, время, необходимое для обучения и адаптации модели к новым условиям, может ограничить скорость реакции на инциденты [20].

3. ПЛИС для нейросетей: Платформы, такие как Xilinx Zynq, и другие позволяют реализовывать высокопроизводительные аппаратные решения для нейросетей, обеспечивая динамическую конфигурацию и высокую скорость обработки. Это дает возможность интегрировать нейросетевые алгоритмы в существующие системы безопасности, однако, высокая стоимость и сложность проектирования остаются значительными барьерами.

Заключение. Глубокий сравнительный анализ нейросетевых технологий и технологий ПЛИС в системах защищенного исполнения подчеркивает, что выбор конкретной архитектуры должен основываться на четком понимании задач, требований к производительности и доступных ресурсах. Эффективная интеграция этих технологий в системы информационной безопасности может значительно повысить уровень защиты, однако требует внимательного подхода к архитектурным решениям и оценке потенциальных рисков. Инновации в области нейросетевых технологий и ПЛИС открывают новые горизонты для разработки адаптивных, мощных и эффективных систем защиты информации, которые могут быстро реагировать на изменяющиеся условия киберугроз.

Список использованных источников

1. Таненбаум, Э., Ветс, Х. Современные операционные системы. М.: Питер, 2016. – 1120 с.

2. Stallings, W. Cryptography and Network Security: Principles and Practice. Pearson, 2017.

3. Challenges and directions. IEEE Communications Magazine, 58(1), 2020, pp. 56-62.

4. Bishop, M. Computer Security: Art and Science. Addison-Wesley Professional, 2018.

5. Lippmann, R., Fried, D., Graf, I., et al. Evaluating Intrusion Detection Systems: The 1998 6. DARPA Off-line Intrusion Detection Evaluation. MIT Lincoln Laboratory Technical Report, 2022.

6. Shaikh, R., Sasikumar, M. Security Issues in Cloud Computing: A Survey. International Journal of Cloud Computing and Services Science (IJ-CLOSER*)*, 2(5), 2022, pp. 387-395.

7.Chen, Y., Paxson, V., Katz, R. What's New About Cloud Computing Security? University of California Berkeley, 2019.

8. Zissis, D., Lekkas, D. Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 2012, pp. 583-592.

9. Google Cloud. Tensor Processing Units (TPUs): A Beginner's Guide. Google White Paper, 2020.

10. Гудфеллоу, И., Бенджио, Ю., & Курвиль, А. (2016). Глубокое обучение. МИТ Пресс.

11. Бишоп, С. (2006). Распознавание образов и машинное обучение. Спрингер.

12. Чжан, К., Чжан, З., Ли, З., & Цяо, Ю. (2016). "Совместное обнаружение и выравнивание лиц с помощью многозадачных каскадных сверточных сетей." IEEE Signal Processing Letters, 23(10), 1499-1503.

13. Хохрейтер, С., & Шмидхубер, Ј. (1997). "Долгая краткосрочная память." Neural Computation, 9(8), 1735-1780.

14. Лекун, Й., Ботту, Л., Бенджио, Ю., & Хаффнер, П. (1998). "Обучение на основе градиента для распознавания документов." Proceedings of the IEEE, 86(11), 2278-2324.

15. Ганаи, М. А., & Хусаинов, Р. (2020). "Методы машинного и глубокого обучения в кибербезопасности: обзор." Journal of Cyber Security Technology, 4(4), 291-313.

16. Чжан, Y., & Чжао, Х. (2019). "Обзор глубокого обучения в кибербезопасности." International Journal of Information Security, 18(5), 485-508.

17. Чен, Ц., Чжан, З., & Ху, Ц. (2020). "Обзор ускорителей нейронных сетей на основе ПЛИС." Journal of Field Programmable Logic Applications, 3(1), 1-12.

18. Жанг, Х., & Ли, Ц. (2019). "Генеративные состязательные сети: обзор." IEEE Transactions on Neural Networks and Learning Systems, 30(1), 1-22.

19. Xilinx Inc. (2021). Zynq-7000 SoC: Технический справочник. Доступно по адресу: Документация Xilinx.

20. Коккоз М. М Методы борьбы с угрозами информационной безопасности государства/ Коккоз М. М, Альжанова А. У., Аубакиров А. М., Жарилхасинова Д. К. // Молодой ученый 8(142). - С-237-240.