УДК 004.056.5

АППАРАТНОЕ ОБЛАКО МЕЖСЕТЕВЫХ ЭКРАНОВ КАК КОМПОНЕНТ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СИСТЕМ КИБЕРЗАЩИТЫ

С.В. Корякин[1], И.В. Бочкарев[2], В.Р. Храмшин[3]

[1] Институт машиноведения, автоматики и геомеханики Национальной академии наук Кыргызской Республики, ул. Скрябина, д. 23, 720055, Кыргызстан. E-mail: srgkoryakin1@gmail.com

[2] Кыргызский государственный технический университет имени И. Раззакова, пр. Ч. Айтматова, д. 66, г. Бишкек, 720044, Кыргызстан

[3] Магнитогорский государственный технический университет имени Г. И. Носова, пр. Ленина, д. 38, г. Магнитогорск, 455000, Россия

Анотация: современные автоматизированные информационные системы характеризуются ростом вычислительных нагрузок и усложнением киберугроз, что требует развития аппаратно-программных средств информационной безопасности. Особый интерес представляет применение аппаратно-ориентированных подходов и облачных архитектур для повышения производительности, масштабируемости и устойчивости средств защиты информации. Цель: разработка принципов организации аппаратного облака в системах защиты информации и создание архитектуры облачной системы межсетевых экранов, обеспечивающей адаптивную защиту автоматизированных информационных систем от киберугроз. Результаты: рассмотрены методы аппаратно-программного обеспечения информационной безопасности автоматизированных информационных систем и принципы организации аппаратного облака на основе функциональных элементов микроэлектронных систем. Представлен прототип облачной системы межсетевых экранов/брандмауэров, функционирующей в рамках аппаратно-ориентированной сети. Предложен подход к формированию конфигурации функциональных возможностей межсетевых экранов, объединённых аппаратным облаком под управлением нейронной сети. Разработаны архитектура и алгоритм работы аппаратного межсетевого экрана, реализующего принципы аппаратно-ориентируемых сетей. Введены определения аппаратной облачной сети и аппаратного облака. Практическая значимость: полученные результаты могут быть использованы при проектировании и модернизации аппаратно-программных комплексов защиты информации, в том числе в корпоративных и критически важных автоматизированных системах. Предложенные архитектурные решения обеспечивают повышение масштабируемости, адаптивности и эффективности межсетевых экранов в условиях динамически изменяющихся киберугроз.

Ключевые слова: аппаратное облако; системы защиты информации; межсетевой экран (МСЭ); файрвол; функциональное расширение; информационная безопасность; архитектура безопасности; модульность; отказоустойчивость; автоматизированные информационные системы реального времени защищенного исполнения (АИСРВ ЗИ); аппаратные облачные системы (АОС).

Вопросы принципов организации аппаратных облачных систем (АОС) в настоящее время являются одними из сложнейших на пути построения АИСРВ ЗИ. Принято считать, что аппаратно-ориентированные АИСРВ ЗИ представляют собой сложные структуры, которые интегрируют вычислительные ресурсы, физические процессы и сетевую инфраструктуру в единую экосистему. В настоящее время однокристальные ЭВМ (ОКЭВМ) играют центральную роль в формировании таких АОС благодаря своей высокой степени интеграции, энергоэффективности и компактности. С учетом стремительного роста интереса к Интернету вещей (IoT) и умным технологиям, считается, что применение ОКЭВМ в ближайшее время продолжит набирать популярность.

Следует отметить, что ключевыми компонентами АОС так же, как и АИСРВ ЗИ, являются: 1 – датчики и актюаторы, 2 – вычислительные блоки, 3 – системы передачи данных.

С учетом этого возникает необходимость возможности классификации таких систем, как АИСРВИ, АИСРВИ ЗИ и АОАИСРВИ – аппаратные облачные автоматизированные информационные системы реального времени.

Следует отметить, что АОАИСРВ ЗИ представляют собой сложные технологические комплексы, интегрирующие физические процессы с цифровыми средствами управления,

анализа и моделирования. Имитационная модель таких систем служит ключевым инструментом для их проектирования, анализа и оптимизации. Поэтому при построении имитационных моделей АОАИСРВ ЗИ крайне важно учитывать особенности структурных компонентов, входящих в состав такой модели, а также основные узлы функциональной структурной схемы. На рисунке 1 представлена обобщенная структурная схема имитационной модели АОАИСРВИ ЗИ.

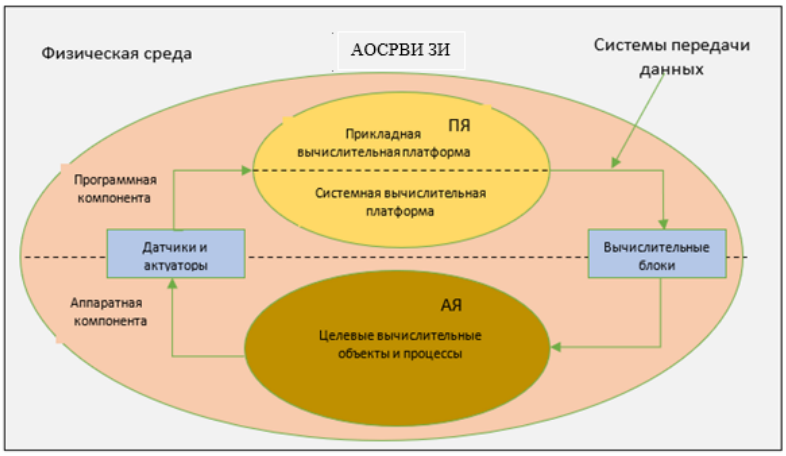

Рисунок 1 – Обобщенная структурная схема имитационной модели АОАИСРВ ЗИ, где : ПЯ – программное ядро АОАИСРВ ЗИ , АЯ – аппаратное ядро АОАИСРВ ЗИ

Как правило, имитационная модель АОАИСРВ ЗИ состоит из ряда взаимосвязанных компонентов, обеспечивающих взаимодействие физических и кибернетических уровней системы таких, как физическая среда, сенсоры, коммуникационная среда, модули сбора и обработки данных, модуль анализа и принятия решений, модуль управления, исполнительные механизмы (актуаторы), интерфейс пользователя, обратная связь.

Ключевой особенностью имитационной модели АОАИСРВ ЗИ является тесная интеграция физических и кибернетических компонентов через коммуникационную среду. Эффективность такой модели зависит от следующих факторов: минимизация задержек передачи данных; точность сенсоров и актюаторов; интеллектуальность алгоритмов анализа и управления. Кроме того, важной частью такой модели является возможность масштабирования системы для обработки больших объемов данных, особенно в условиях сложных физических процессов.

Обобщенная структурная схема модели позволяет наглядно представить взаимодействие элементов, облегчая анализ, проектирование и оптимизацию системы.

Один из возможных вариантов архитектуры АОАИСРВ ЗИ может быть организован на базе ОКЭВМ. АИСРВ ЗИ и представлен несколькими своими уровнями: 1) – аппаратный уровень; 2) – уровень обработки данных; 3) – уровень управления.

Использование ОКЭВМ для создания программируемых и адаптивных файловых систем открывает новые горизонты для обеспечения безопасности в условиях постоянно меняющегося киберпространства. Использование ОКЭВМ позволяет получить такие преимущества, как компактность, энергоэффективность и гибкость архитектуры.

Учитывая увеличение числа подключенных устройств к глобальной сети Internet и растущие киберугрозы, в настоящее время существует острая необходимость в разработке надежных средств защиты, таких как файрволы, которые могут быть реализованы на базе ОКЭВМ. Эти системы способны не только фильтровать трафик, но и защищать от несанкционированного доступа, а также обеспечивать сохранность персональных данных и критически важной информации.

Использование однокристальных ЭВМ для разработки файрволов позволяет значительно сократить затраты на внедрение средств безопасности благодаря высокой степени интеграции и энергоэффективности. Следует подчеркнуть, что такие файрволы

способны реализовывать адаптивные и гибкие правила фильтрации и мониторинга трафика, быстро подстраиваясь под меняющиеся условия угроз [1].

Традиционно применяют аппаратный межсетевой экран, который представляет собой отдельное устройство или часть маршрутизатора. Кроме того, широкое применение нашел также его альтернативный вариант – программный межсетевой экран, примером которого служит брандмауэр, встроенный в Windows.

Существует два основных способа создания наборов правил межсетевого экрана: «включающий» и «исключающий» [1, 2, 3, 4, 5, 6].

Существующие решения имеют следующие недостатки: 1. Недостаток в архитектуре межсетевого экранирования. 2. Применение дорогостоящих, так называемых помощников МСЭ. 3. При реализации традиционной архитектуры МСЭ как подсистема защиты информационных систем, управление всеми процессами осуществляется ядром подсистемы защиты, при этом в процессе функционирования подсистемы защиты вся нагрузка ложится на центральный процессор, который управляет ядром подсистемы защиты.

Это связано с тем, что при построении аппаратной компоненты файрволов – МСЭ, при реализации традиционной архитектуры подсистем защиты информационных систем используются классические серверные микро-ЭВМ (серверы), которые по назначению можно разделить на серверы, рабочие станции, персональные компьютеры, встраиваемые и промышленные микро-ЭВМ (рис. 2) [7,8].

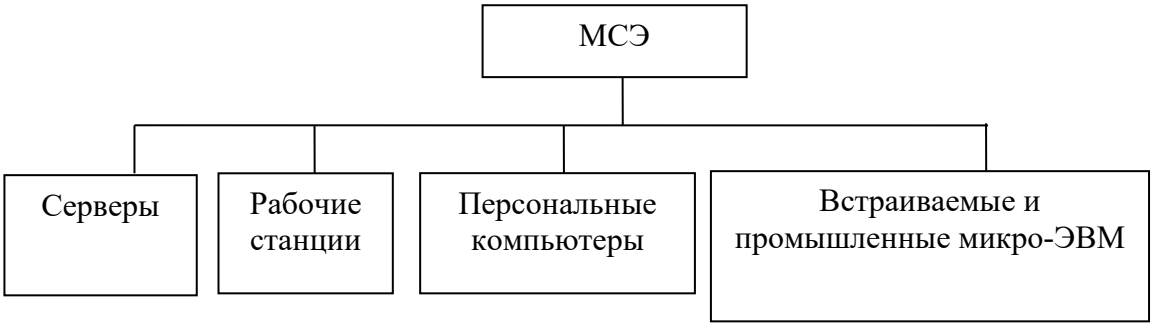

Рисунок 2 – Классификация МСЭ по типу микро-ЭВМ

Следует отметить, что архитектура традиционных МСЭ (ТМСЭ) состоит из двух основных подсистем – аппаратная основная и программная второстепенная подсистемы. Из этого следует, что программная подсистема является неотъемлемой частью аппаратной подсистемы в архитектуре традиционного МСЭ (или файрвола). На рисунке 3 изображена обобщенная структурная схема архитектуры ТМСЭ.

Рисунок 3 – Обобщенная структурная схема архитектуры ТМСЭ

Для построения аппаратной подсистемы традиционных МСЭ используется два основных подхода в реализации архитектуры аппаратного схемотехнического решения: 1. Построение аппаратной архитектуры МСЭ на базе многослойной материнской системной платы. 2. Построение аппаратной архитектуры МСЭ на базе модульных системных плат.

В обоих подходах основная нагрузка в процессе обработки сигналов в системной материнской плате ложится на «чипсет». Именно от него зависит, какой процессор и какой тип оперативной памяти нужно использовать, сколько устройств можно подключить и как быстро и стабильно все они будут работать. [9, 10, 11].

С точки зрения практического применения процессоров для построения архитектуры традиционных МСЭ основной является программная архитектура. На текущий момент актуальные и распространённые архитектуры – это CISC, VLIW, [12].

Исходя из результатов проведенного анализа, для оптимизации функционирования МСЭ предлагается использовать структуру МСЭ, состоящую из дополнительного аппаратного ядра включенную в структуру аппаратной подсистемы МСЭ, основанного на ПЛИС-технологиях и традиционного программного ядра, являющегося центральной частью программной подсистемы МСЭ. В данном случае под аппаратным ядром операционной системы МСЭ понимается функциональный компонент на основе ПЛИС, обеспечивающий приложениям этой операционной системы, координируемый доступ к следующим ресурсам МСЭ: процессорное время, память, внешнее аппаратное обеспечение, внешние устройства ввода-вывода информации, сервисы файловой системы и сетевых протоколов. Подобное аппаратное ПЛИС-ядро ОС МСЭ использует механизмы межпроцессорного взаимодействия и обращения приложений к системным вызовам программного ядра ОС МСЭ. На рисунке 4 изображена обобщенная структурная схема модернизированного МСЭ (ММСЭ) с дополнительными аппаратными и программными ядрами [13].

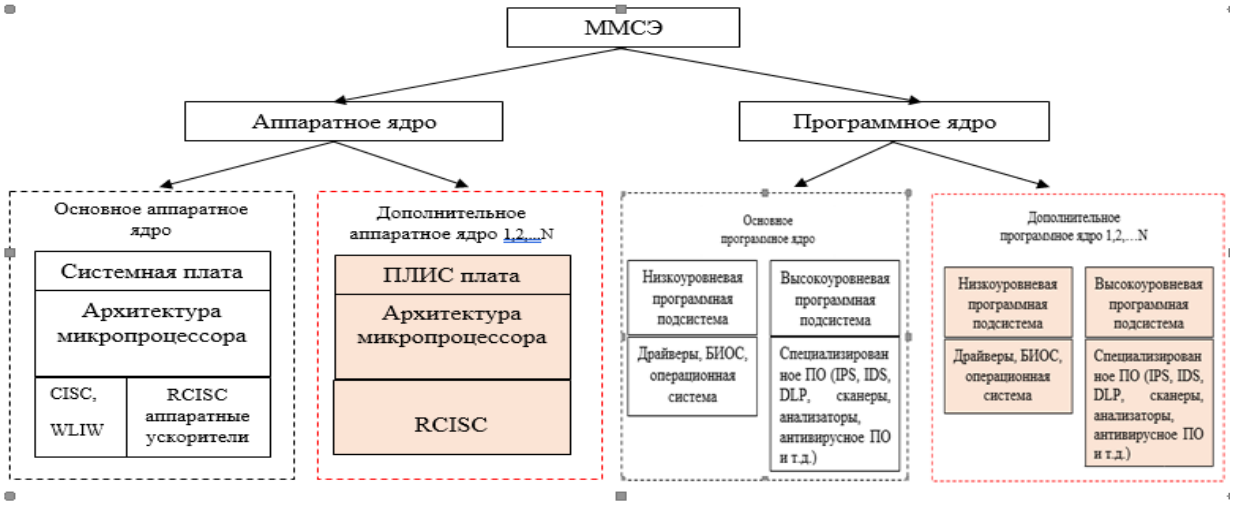

Рисунок 4 – Обобщенная структурная схема архитектуры ММСЭ с дополнительными аппаратными ядрами

В этом случае ПЛИС ядро ОС МСЭ существенно разгружает аппаратный компонент архитектуры МСЭ, обеспечивая при этом многократное повышение быстродействия МСЭ в целом. При этом масштабирование дополнительных аппаратных ПЛИС ядер возможно производить без ограничений за счет уникальных характеристик ПЛИС ядра, таких как:

1. Низкая стоимость. 2. Приемлемые системные характеристики (процессорная память, ОЗУ, интерфейсы ввода вывода), способные повышать производительность ресурсов основного аппаратного ядра МСЭ. 3. Низкая стоимость. 4. Низкое энерго- и теплопотребление. 5. Маленькие габариты. 6. Неограниченные функциональные возможности для конфигурации программной подсистемы МСЭ.

Таким образом предложенный способ конфигурации архитектуры ММСЭ позволяет перераспределять функционал программной подсистемы ММСЭ с целью его адаптации под определенные задачи обеспечения защиты информации. При этом дополнительные ПЛИС ядра забирают на себя часть основного процесса, что позволяет эффективно распределять ресурсы ММСЭ, обеспечивая при этом высокую производительность и быстродействие подсистемы защиты информации в целом [14, 15].

Задачи функционального расширения ММСЭ, масштабирования аппаратных и программных компонентов дополнительных ПЛИС ядер реализуются при помощи нейронной сети, которая объединяет ПЛИС ядра в единое аппаратное облако МСЭ. При этом процесс объединения ПЛИС ядер в группы осуществляется нейронной сетью по неизвестным для злоумышленников алгоритмам, что обеспечивает повышение уровня информационной безопасности и эффективности функционирования ММСЭ в целом.

Интеграция нейросетевых технологий и решений на базе ПЛИС в аппаратно-ориентированные системы защищенного исполнения открывает новые возможности для повышения уровня безопасности. Применение глубоких нейронных сетей и гибких аппаратных решений позволяет адаптироваться к динамично меняющимся киберугрозам, однако требует тщательной проработки архитектурных решений и оценки возможных рисков.

Следует отметить, что предлагаемое использование нейросетевых технологий и технологий ПЛИС в системах защищенного исполнения представляет собой многообещающее направление, которое может привести к созданию более эффективных и адаптивных защитных механизмов киберфизических систем в современных условиях.

Разработка принципа функционального расширения МСЭ-файрволов и брандмауэров

Одним из подходов к решению проблем функционального расширения МСЭ, файрволов и брандмауэров является разработка новой концепции построения системы межсетевых экранов, основанной на облачных и нейросетевых технологиях и технологиях ПЛИС программируемых логических интегральных схем, которые применительно к рассматриваемым проблемам представляют собой аппаратные облачные сети (АОС).

Следует отметить, что в данном случае под АОС понимается сеть передачи данных, в которой определение функционала устройства сети происходит по неизвестному алгоритму в пределах локального аппаратного облака. При этом алгоритмы определения функционала устройств сети и архитектура локального аппаратного облака для каждого частного случая определяются и формируются ядром АОС, управляемым нейронной сетью.

В свою очередь под аппаратным облаком подразумевается модель, обеспечивающая доступ по требованию к общей сети программно-аппаратных устройств для использования алгоритмов определения функциональных возможностей и распределения вычислительных ресурсов. Наряду с этим архитектура, электротехнические составляющие, IT-инфраструктура находятся в «туманной завесе», т.е. в «облаке» и скрыты от объектов глобальной сети Internet. При этом взаимодействие внутри аппаратного облака между устройствами осуществляется по шифрованным каналам передачи информации – облачным кольцевым информационным тоннелям [16].

Другими словами:

«Аппаратное облако» – аппаратно-программный комплекс с гибкой конфигурацией структуры, формируемой и управляемой нейронной сетью с целью обеспечения доступа к общей сети IoT устройств по требованию, а также для оперативной и эффективной технической защиты информации.

«Аппаратная облачная система» – система передачи данных, в которой формирование ее архитектуры и определение функционала сетевого устройства для каждого частного случая осуществляется в пределах аппаратного облака по алгоритму, синтезируемому нейронной сетью [16].

Основными компонентами предлагаемой концепции являются:

Аппаратное облако – объединённая платформа, состоящая из множества межсетевых экранов (МСЭ), управляемых центральной нейронной сетью.

Межсетевые экраны (МСЭ) – программно-аппаратные модули, реализованные на базе программируемых логических интегральных схем (ПЛИС) и работающие в составе аппаратного облака.

Нейросетевая система управления – модуль искусственного интеллекта, осуществляющий анализ сетевого трафика, классификацию угроз и динамическое обновление конфигурации МСЭ.

База данных сигнатур – централизованное хранилище информации об известных угрозах, обновляемое в реальном времени.

Механизмы машинного обучения и интеллектуального анализа данных – алгоритмы оптимизируют работу системы киберзащиты, сокращая количество ложных срабатываний и повышая эффективность обнаружения угроз [17].

В основе функционирования системы межсетевых экранов лежат следующие принципы:

Анализ сетевого трафика. А) Потоки данных проходят через аппаратное облако, где нейросетевая система анализирует пакеты информации. Б) Обнаруженные аномалии и потенциальные угрозы классифицируются в реальном времени.

Динамическая конфигурация правил безопасности. А) Нейросеть автоматически адаптирует параметры межсетевых экранов на основе обнаруженных угроз. Б) Новые правила защиты распространяются на все подключённые устройства [18].

Обновление базы данных сигнатур. Новые угрозы добавляются в базу данных и распространяются в сети для мгновенного реагирования [19].

Оптимизация работы системы с использованием ПЛИС. ПЛИС позволяют ускорить обработку данных и снизить нагрузку на основные вычислительные ресурсы системы [20, 21].

Исходя из вышеизложенного, можно констатировать, что применение искусственных нейронных сетей для детектирования вторжений является сегодня инновационным способом при создании систем защиты информации от НСД. Это обусловлено тем, что нейросети обладают гибкостью, что дает им способность обучаться в режиме реального времени, что повышает вероятность верного срабатывания при детектировании атак [22, 23].

Другими словами, можно говорить о том, что предлагаемые на базе ПЛИС конфигурируемые МСЭ, имеющие в своем составе нейросетевой модуль, обладают функцией самоорганизации, что позволяет им автономно осуществлять конфигурацию функций МСЭ, автономно реагировать на потенциальную угрозу и принимать решение о ликвидации НСД.

При этом по сравнению с традиционными подходами построения сетей МСЭ, где обработка производится процессором ядра подсистемы защиты, использование предлагаемых на базе ПЛИС конфигурируемых МСЭ значительно уменьшает время обработки входящей информации и обнаружения НСД в ИС за счет высокого быстродействия ПЛИС, а обращение к ядру подсистемы защиты будет происходить только в трех случаях:

Получение обновлений о наличии новых сигнатур угроз и конфигураций функций МСЭ. 2. Отправки отчетов неидентифицированных сигнатур угроз. 3. Отправки неидентифицированных сигнатур угроз.

Использование ПЛИС в качестве аппаратной компоненты для создания конфигурируемых облачных аппаратных МСЭ при реализации предлагаемого подхода позволяет решить вопросы, связанные со снижением производительности подсистемы защиты в целом, снижением быстродействия подсистемы защиты, уменьшением времени обнаружения несанкционированного доступа в информационную систему, а также повышением коэффициента защищенности информационной системы.

Основными преимуществами предлагаемой концепции формирования конфигурации межсетевых экранов/брандмауэров являются: адаптивность и самоорганизация – система автономно реагирует на новые угрозы без вмешательства оператора; **высокая производительность** – использование ПЛИС повышает скорость обработки информации; **минимизация ложных срабатываний** – интеллектуальный анализ снижает вероятность ошибок; **масштабируемость** – аппаратное облако позволяет добавлять новые узлы без снижения эффективности работы.

Обобщенная схема АС управления в структуре мониторинга геоэкологической информации с применением концепции формирования конфигурации межсетевых экранов/брандмауэров (КФКМЭ/Б) представлена на рисунке 5.

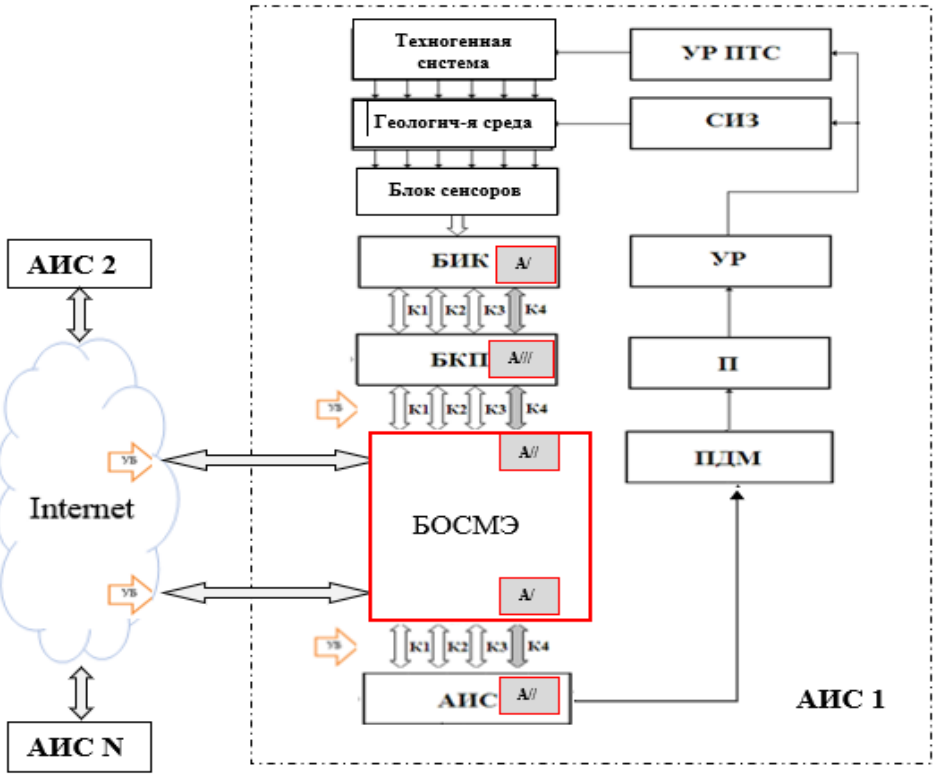

Рисунок 5 – Обобщенная схема АС управления геоэкологического мониторинга с применением КФКМЭ/Б, где ТС – техногенная система; ГС – геологическая среда; БС – блок сенсоров, для регистрации параметров окружающей среды; БИК – блок измерительных каналов; БКП – блок каналов передачи; АИС – автоматизированная информационная система; ПДМ – постоянно действующая модель, являющаяся частью АИС и постоянно пополняющаяся новой информацией по мере функционирования всей системы мониторинга; П – прогноз; УР – управляющее решение; СИЗ – система инженерной защиты; УР ПТС – управление режимами природно-техногенной системы; К1- канал передачи электрическими контрольными кабельными линиями; К2 – канал передачи оптоволоконными кабельными линиями; К3 – канал передачи беспроводными линиями связи; К4 – канал передачи электрическими кабельными линиями распределительных электрических сетей (РЭС); УБ – угрозы информационной безопасности; БОСМЭ – блок облачной системы межсетевых экранов, А/ – адаптер передатчик, А// – адаптер приемник, А///– адаптер приемо-передатчик

Предложенная концепция представляет собой передовой подход к обеспечению кибербезопасности, сочетающий адаптивные алгоритмы ИИ и высокопроизводительные программируемые логические схемы, создавая автономную и эффективную систему защиты.

Для проведения экспериментальных исследований была разработана соответствующая методика, которая представляет собой совокупность трех взаимосвязанных технологических процедур:

1. Определение задач, согласование последовательности проведения эксперимента. 2. Тестирование и сбор данных. 3. Анализ результатов тестирования.

Структурная логическая блок схема методики проведения эксперимента представлена на рисунке 6.

Для выполнения первой задачи необходимо сформулировать основные предъявляемые к МСЭ функциональные и технические характеристики.

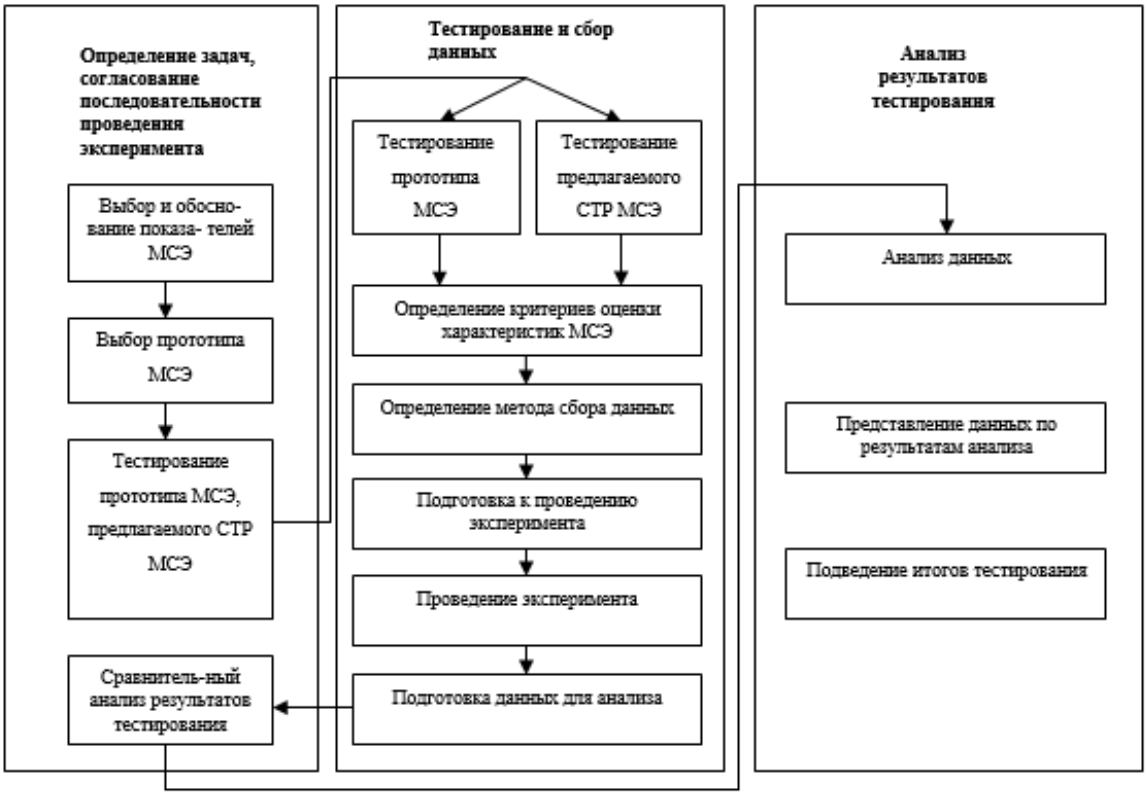

Рисунок 6 – Структурная логическая блок-схема методики проведения эксперимента

Из функциональных следует выделить основные минимальные характеристики: 1. Управление доступом к сегментам сети, контроль и фильтрация трафика. 2. Защита веб-приложений и сервисов. 2. Мониторинг исходящих и входящих пакетов данных. 3. Предотвращение нежелательных соединений и подключений сети. 4. Мониторинг и анализ инцидентов ИБ.

Выбор обоснования аппаратного и программного компонентов экспериментальных исследований

Таким образом, базовая конфигурация современного МСЭ должна состоять из следующих программных подсистем, реализующих функциональные характеристики МСЭ:

1. ПО контроля и фильтрации трафика (NGFW, SolarWinds Network Bandwidth Analyzer, Wireshark, tcpdump, Kismet, EtherApe, KisMAC, решения лаборатории Касперского, решения Позитив Технолоджи, решения Солар и др.). 2. ПО защиты веб-приложений и сервисов (WAF). 3. ПО мониторинга исходящих и входящих пакетов данных (Splunk и др.). 4. ПО IPS/IDS (Snort, Suricata и др.). 5. ПО мониторинга и анализа инцидентов ИБ (Wazuh, стек ELK и др.).

Таким образом, исходя из представленных выше функциональных и технических характеристик, предъявляемых к МСЭ, был выбран прототип МСЭ. Характеристики прототипа МСЭ представлены в таблице 1.

Таблица 1– Характеристики прототипа МСЭ

Функциональные характеристики	
Антивирусное ПО	Антивирус Касперского

ПО контроля и фильтрации трафика	NGFW
ПО защиты веб-приложений и сервисов	WAF
ПО мониторинга исходящих и входящих пакетов данных	Splunk
ПО IPS/IDS	Snort
ПО мониторинга и анализа инцидентов ИБ	Wazuh, стек ELK
Технические характеристики МСЭ до 10 000 событий в секунду	
Версия ОС	ubuntu server 22.04
Кол-во логических ядер в системе виртуализации	20
Память (ОЗУ)	36 ГБ
Твердотельный накопитель	1 000 ГБ
Тип платы аппаратной подсистемы МСЭ	Многослойная материнская плата для ЭВМ
Тип архитектуры процессора	CiSC , WLWL

В таблице 2 представлены характеристики предлагаемого СТР ММСЭ

Таблица 2 – Характеристики предлагаемого СТР ММСЭ

Функциональные характеристики	
Нейросетевой модуль	Модифицированное ПО
Антивирусное ПО	Антивирус Касперского
ПО контроля и фильтрации трафика	NGFW
ПО защиты веб-приложений и сервисов	WAF
ПО мониторинга исходящих и входящих пакетов данных	Splunk
ПО IPS/IDS	Snort
ПО мониторинга и анализа инцидентов ИБ	Wazuh, стек ELK
Технические характеристики основного аппаратного ядра ММСЭ до 10 000 событий в секунду	
Версия ОС	ubuntu server 22.04
Кол-во логических ядер в системе виртуализации	20
Память (ОЗУ)	36 ГБ
Твердотельный накопитель	1 000 ГБ
Технические характеристики дополнительного аппаратного ядра ММСЭ	
Версия ОС	ubuntu модифицированная
Кол-во логических ядер в системе виртуализации	3
Память (ОЗУ)	8 ГБ
Твердотельный накопитель	Встраиваемый микро SSD 64 ГБ
Кол-во дополнительных программных ядер	3
Общие технические характеристики аппаратного ядра ММСЭ	
Версия ОС	ubuntu server 22.04,ubuntu модифицированная
Кол-во логических ядер в системе виртуализации	32
Память (ОЗУ)	60 ГБ
Твердотельный накопитель	1 192 ГБ
Тип платы аппаратной подсистемы МСЭ	Комбинированная (однокристальная система: SoC, многослойная материнская плата для ЭВМ)
Тип архитектуры процессора	ARM Cortex A72

Тестирование и сбор данных

Тестирование образцов будем производить по следующему сценарию:

1. Сравнение технических характеристик образцов. 2. Сравнение распределения компонентов программного ядра на ресурсы аппаратных ядер в процентах. 3. Сравнение общей производительности (количество событий в секунду, количество активов). 4. Сравнение экономических показателей тестируемых образцов.

Результаты сравнения типовых характеристик представлены в таблице 3.

Таблица 3 – Сравнение технических характеристик МСЭ и ММСЭ

Технические характеристики МСЭ до 10 000 событий в секунду		
	Прототип МСЭ	ММСЭ
Версия ОС	ubuntu server 22.04	ubuntu server 22.04,ubuntu модифицированная
Кол-во логических ядер в системе виртуализации	20	32
Память (ОЗУ)	36 ГБ	60 ГБ
Твердотельный накопитель	1 000 ГБ	1 192 ГБ
Тип платы аппаратной подсистемы МСЭ	Многослойная материнская плата для ЭВМ	Комбинированная (однокристальная система: SoC, многослойная материнская плата для ЭВМ)
Тип архитектуры процессора	CiSC , WLWL	ARM Cortex A72
Питание	2x450w	2x450w+3x5w

Исходя из таблицы 3, технические характеристики предлагаемого СТР МСЭ превышают аналогичные характеристики прототипа МСЭ в среднем на 52%. Детальное соотношение тестируемых образцов в процентах представлено на рисунке 7.

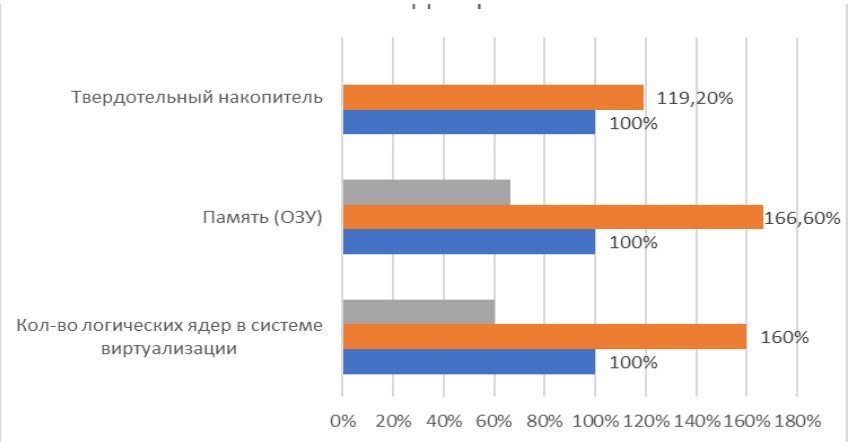

Рисунок 7 – Детальное соотношение тестируемых образцов

Шаг 2. Сравнение распределения компонентов программного ядра на ресурсы аппаратных ядер в процентах.

Для проведения шага 2 сценария тестирования была проведена DDOS атака на порт входящего трафика МСЭ одновременно из 7 хостов для того, чтобы создать максимальную нагрузку в 10 000 событий в секунду и определения состояния загруженности ресурсов аппаратного ядра тестируемых образцов (процессорное время, оперативная память, сервисы файловой системы, процессы внешнего аппаратного обеспечения, процессы устройств ввода вывода информации). Все компоненты программного ядра в ходящие в конфигурацию прототипа МСЭ примем за 100% занимаемых ресурсов аппаратного ядра прототипа МСЭ.

Результаты распределения компонентов программного ядра на ресурсы аппаратного ядра прототипа МСЭ приведены на рисунке 8.

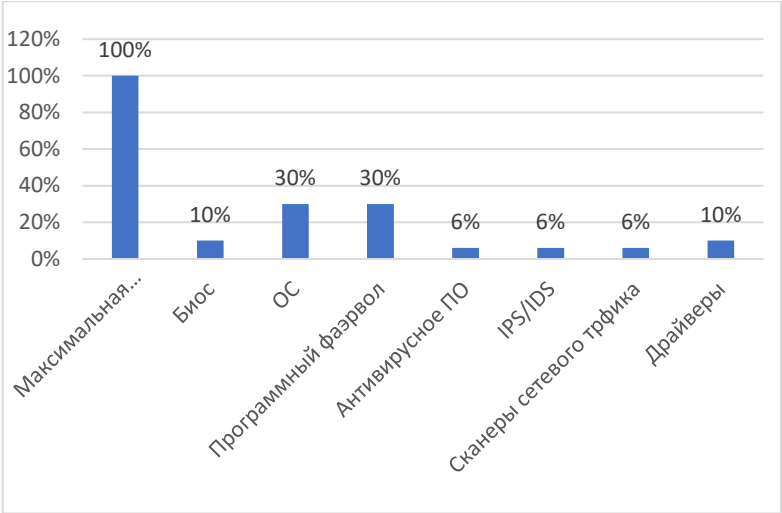

Рисунок 8 – Распределение компонентов ПЯ
на ресурсы АЯ прототипа МСЭ

Следующим действием была проведена аналогичная атака на порт входящего трафика, предлагаемого СТР МСЭ. Схема распределения ресурсов дополнительных ПЛИС ядер, входящих в состав предлагаемого СТР ММСЭ, представлена в таблице 4.

Таблица 4 – Схема распределения ресурсов дополнительных ПЛИС ядер СТР ММСЭ

Компоненты программного ядра, расходующие ресурсы ПЯ	**Ресурсы основного аппаратного ядра ММСЭ**	**Ресурсы Плис ядра 1 ТМСЭ**	**Ресурсы Плис ядра 2 ТМСЭ**	**Ресурсы Плис ядра N ТМСЭ**
Максимальная производительность	100%			
Биос	10%	3%	3%	3%
ОС	30%	5%	5%	3,3%
Программный фаэрвол	30%	5%	нет	3,3%
Антивирусное ПО	6%	Нет	нет	3,3%
IPS/IDS	6%	Нет	2,5%	нет
Сканеры сетевого трафика	6%	Нет	2,5%	нет
Драйверы	10%	3%	3%	3%
Нейросетевой модуль	10%	4%	4%	4%

Результаты распределения компонентов программного ядра на ресурсы аппаратного ядра, предлагаемого СТР ММСЭ, приведены на рисунке 9.

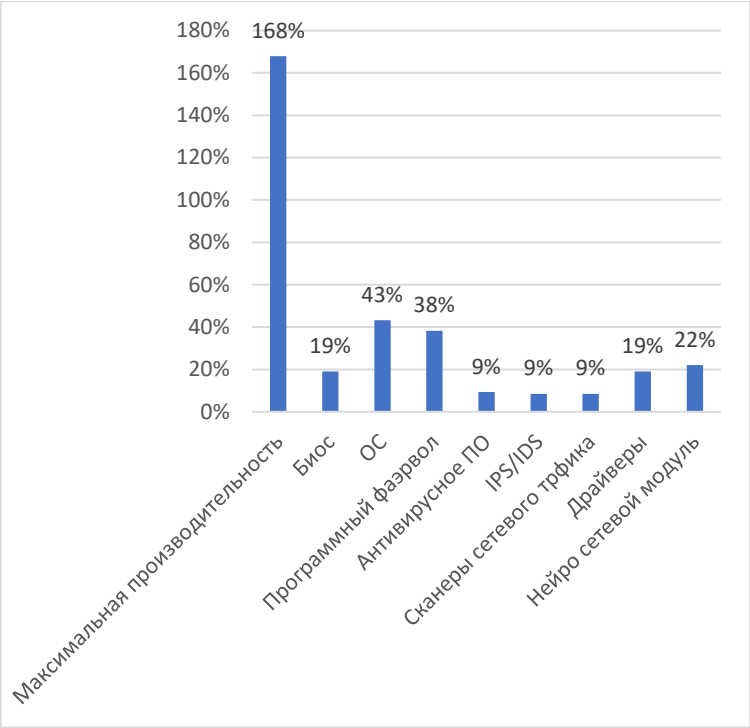

Рисунок 9 – Результаты распределения компонентов ПЯ на ресурсы АЯ СТР ММСЭ

Сравнение результатов распределения компонентов программного ядра на ресурсы аппаратного ядра тестируемых образцов в процентном соотношении приведено на рисунке 10.

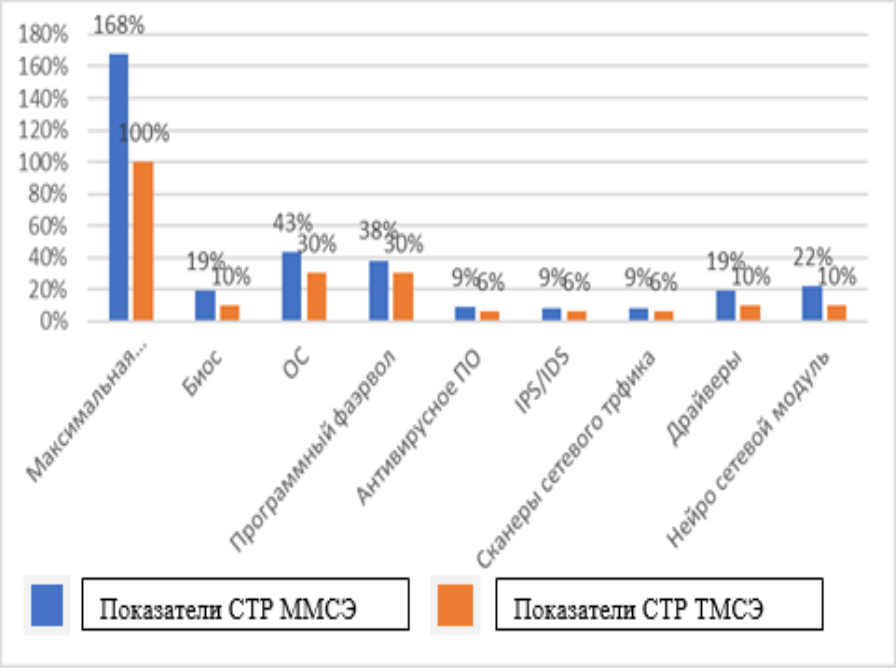

Рисунок 10 – Сравнение результатаов распределения компонентов ПЯ на ресурсы АЯ тестируемых образцов, где синим цветом обазначены характеристики ММСЭ, оранжевым цветом характеристики прототипа МСЭ

Шаг 3. Сравнение общей производительности (количество событий в секунду, количество активов).

Исходя из приведенных выше результатов тестирования следует, что общая производительность ресурсов аппаратного ядра, предлагаемого СТР ММСЭ, превышает

аналогичные показатели прототипа МСЭ на 24%, колличество событий в секунду обрабатываемых предлагаемым СТР ММСЭ при повышении нагрузки на порт входящего трафика составило 12400, в то время как колличество событий в секунду обрабатываемых прототипом МСЭ составляет 10000. Количество активов, обрабатываемых предлагаемым СТР ММСЭ, составило 4340, что на 44% выше рассматриваемого прототипа МСЭ (3000 активов).

Шаг 4. Сравнение экономических показателей тестируемых образцов.

Для сравнения экономических показателей тестируемых образцов был проведен анализ стоимости серверов и компонентов на рынке поставщиков оборудования в КР. По результатам проведенного анализа средняя стоимость тестируемых образцов составила: для прототипа МСЭ – 4200 у.е. (378000 сом.); для предлагаемого СТР ММСЭ – 4500 у.е (405000 сом.). Следовательно стоимость предлагаемого СТР ММСЭ на 7 % больше, чем у прототипа МСЭ.

Анализ основных результатов экспериментальных исследований

Учитывая показатели производительности предлагаемого СТР ММСЭ, а именно превышение на 24% аппаратных ресурсов, 24% количество событий в секунду обрабатываемых предлагаемым СТР ММСЭ и 44% количества обрабатываемых активов, необходимо рассчитать, во сколько денежных средств обойдутся показатели прототипа ММСЭ.

Следует отметить, что для повышения производительности прототипа МСЭ из-за требований, предъявляемых компонентами программного ядра, потребуется установка полноценного сервера с характеристиками, предъявляемыми в качестве минимальных для МСЭ (таблица 5.1). Соответственно стоимость прототипа МСЭ возрастет в 2 раза и составит 756 000 сом. Максимальные показатели производительности при этом составят: 20 000 событий, обрабатываемых в секунду, 6000 активов. Для сравнения следует отметить, что стоимость СТР ММСЭ с аналогичными показателями производительности составит: 486 000 сомов, что на 36% дешевле стоимости прототипа (плюс 12 дополнительных аппаратных ядер), при этом количество событий, обрабатываемых в секунду, составит 19600, 8360 активов, 100% соответствует показателям прототипа МСЭ.

В таблице 5 приведены общие сравнительные характеристики результатов тестирования образцов.

Таблица 5 – Общие сравнительные характеристики результатов тестирования

Технические характеристики прототипа МСЭ до 20 000 событий в секунду		Технические характеристики ММСЭ до 20 000 событий в секунду		Повышение характеристики в процентах %
Количество логических ядер в системе виртуализации шт.	40	Количество логических ядер в системе виртуализации шт.	68	+ 70%
Память (ОЗУ) ГБ	72	Память (ОЗУ) ГБ	132	+ 83,30%
Твердотельный накопитель ГБ	2 000	Твердотельный накопитель ГБ	1 768	-11,60%
Количество серверов шт.	2	Количество серверов шт.	1	+ 50%
Количество дополнительных аппаратных модулей шт.	0	Количество дополнительных аппаратных модулей шт.	12	не сравнивается
Потребляемая электроэнергия Ватт/час (4*450)	1800	Потребляемая электроэнергия Ватт/час (2*450+9*5)	950	+ 52,80%
Общая стоимость сом. (378 000*2)	756 000,00	Общая стоимость сом. (378 000 + 108 000 (12 шт*9000 сом.)	486 000,00	+ 64,80%

Количество активов (хостов)	6000	Количество активов (хостов)	8360	+ 39,80%
Количество событий, обрабатываемых в секунду	20 000	Количество событий, обрабатываемых в секунду	19 600	-2%

Таким образом, обобщая проведенные сравнительные характеристики тестируемых образцов, можно с уверенностью говорить о том, что предлагаемое СТР ММСЭ в среднем на 30% процентов эффективнее прототипа МСЭ.

Кроме того, предлагаемое СТР обладает рядом преимуществ, а именно: возможностью гибкого масштабирования; возможностью территориального распределения дополнительных аппаратных ядер; низким энергопотреблением; возможностью реализации систем анализа и обработки информации, а также конфигурацией программного ядра при помощи нейронных сетей.

Обобщая результаты экспериментальных исследований, можно констатировать, что *концепция формирования конфигурации межсетевых экранов/брандмауэров с расширенными функциональными возможностями, объединённых аппаратным облаком под управлением нейронной сети,* – это инновационный метод организации механизмов киберзащиты, основанный на использовании программируемых логических интегральных схем (ПЛИС) и искусственных нейронных сетей для автоматической конфигурации и управления межсетевыми экранами (МСЭ).

Ключевой особенностью концепции является адаптивный подбор и динамическое обновление конфигурации правил защиты на основе анализа сетевого трафика, что позволяет минимизировать вероятность ложных срабатываний и повышает вероятность обнаружения угроз. МСЭ, работающие в рамках аппаратного облака, управляются нейросетевым модулем, который идентифицирует угрозы, классифицирует их, обновляет базы данных сигнатур и оперативно распространяет новые правила безопасности на все подключённые устройства.

Предложенный подход включает методы интеллектуального анализа данных и машинного обучения, что ускоряет обработку больших потоков информации, характерных для виртуальных центров обработки данных. Использование ПЛИС в составе конфигурируемых МСЭ повышает быстродействие системы, снижает нагрузку на ядро подсистемы защиты и сокращает время обнаружения несанкционированного доступа. Фактически концепция позволяет создать самоорганизующуюся систему сетевой безопасности, способную автономно адаптироваться к новым угрозам, обеспечивая высокий уровень защиты информационных систем.

Заключение

Разработанные на основе комплексного подхода методы и аппаратно-программные средства защиты информации для автоматизированных систем продемонстрировали высокую эффективность в условиях реальных угроз. В ближайшей перспективе планируется дальнейшее развитие этих решений, ориентированных на создание автономных систем защиты информации. Кроме того, материалы исследования могут быть использованы для дальнейшего совершенствования методов и средств многоцелевого контроля параметров технологических процессов различных видов производств.

Литература

1. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153–1176.
2. Kohonen, T. (2001). *Self-organizing maps* (3rd ed.). Springer.
3. Советов, Б. Я. Моделирование систем [Текст] / Б. Я. Советов. – М.: Высш. шк., 2001. – 343 с.
4. Болодурина, И. П. Исследование моделей нейронной сети для обеспечения безопасности и качества обслуживания мультиоблачной платформы

[Текст] / И. П. Болодурина, Д. И. Парфенов // Информационные и математические технологии в науке и управлении. – Оренбург, 2018. – С. 18–26.

5. Bishop, C. M. (2006). *Pattern recognition and machine learning*. Springer.

6. Курзыкина, А. В. Проблемы внедрения автоматизированной информационной системы [Текст] / А. В. Курзыкина // Молодой ученый. – 2017. – № 4. – С. 124–167. – Режим доступа: URL https://moluch.ru/archive/138/38806/. – Загл. с экрана. – Дата обращения: 16.09.2025.

7. Корякин, С. В. Разработка программно-аппаратного ядра универсальной среды проектирования автоматизированных систем защищенного исполнения [Текст] / С. В. Корякин // Проблемы автоматики и управления. – Бишкек, 2020. – № 1 (38). – С. 60–69.

8. Hennessy, J. L., & Patterson, D. A. (2019). *Computer architecture: A quantitative approach* (6th ed.). Morgan Kaufmann.

9. Stallings, W. (2017). *Network security essentials* (6th ed.). Pearson.

10. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *Proceedings of the IEEE Symposium on Security and Privacy* (pp. 305–316). IEEE.

11. Tehranipoor, M., & Wang, C. (2012). *Introduction to hardware security and trust*. Springer.

12. Sivarama, P. Dandamudi. Guide to RISC Processors [Text]: For Programmers and Engineers / P. Sivarama. – USA: Springer Science+Business Media, Inc., 2005. – 387 p.

13. Vesanto, J., & Alhoniemi, E. (2000). Clustering of the self-organizing map. *IEEE Transactions on Neural Networks, 11*(3), 586–600.

14. Шматок, А. Аппаратные ускорители на базе ПЛИС [Текст] / А. Шматок // Современная электроника. – 2007. – № 6. – С. 60–63.

15. Zhang, Q., Chen, M., & Li, Y. (2018). FPGA-based acceleration for machine learning applications. *IEEE Transactions on Circuits and Systems*, 65(3), 1–12.

16. Корякин, С. В. Облачная система межсетевых экранов / С. В. Корякин, Ю. С. Корякина // Вестник Кыргызско-Российского Славянского университета. – 2023. – Т. 23, № 4. – С. 67–78. – DOI 10.36979/1694-500X-2023-23-4-67-78. – EDN ZWRQES.

17. Cheswick, W. R., Bellovin, S. M., & Rubin, A. D. (2003). *Firewalls and Internet security*. Addison-Wesley.

18. Vinayakumar, R., et al. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access, 7*, 41525–41550.

19. Buczak, A. L., & Guven, E. (2016). Machine learning for cybersecurity. *Pattern Recognition Letters, 101*, 3–10.

20. Information Technologies and Automation 2021. (2021). *Procedia Computer Science, 190*, 1–8.

21. Students' motivation and engagement during distance learning. (2021). *Procedia Computer Science, 192*, 247–256.

22. Methods and algorithms of multidimensional data analysis. (2014). In *Neuro-fuzzy methods in intelligent systems* (pp. 9–72).

23. Gruzdeva, L. M. (2015). *Models for improving corporate telecommunication networks under information security threats* (Doctoral dissertation).