Обнаружение вторжений на основе биометрической аутентификации с ИИ и IoT

Дмитрий Швецов

В настоящее время во всём мире растёт потребность в обеспечении информационной безопасности и своевременном обнаружением вторжений в сети во время передачи данных. Для подобных мероприятий существуют методы применения искусственного интеллекта (ИИ) с поддержкой технологий Интернета вещей (IoT), входящих в архитектуру Умных городов, позволяющие принимать решения практически без вмешательства человека. В статье рассматривается новый метод для безопасной передачи данных и обнаружения злоумышленника в системе биометрической аутентификации.

Введение

Обнаружение злонамеренных действий осуществляется путём сбора биометрической базы данных Умного здания на основе IoT. Функции обработанных биометрических данных извлекаются для анализа с использованием основных компонентов ядра системы. Затем обработанные биометрические признаки классифицируются с помощью свёрточной нейросети VGG 16. Затем вся сеть защищается с помощью протокола детерминированной доверительной передачи (DTTP). Производительность предложенного метода рассчитывалась с использованием нескольких показателей, таких как точность (f-оценка), полнота и среднеквадратическая ошибка. Результаты моделирования показали, что предложенный метод обеспечивает лучшие результаты обнаружения вторжений.

Биоидентификация с применением ИИ

Современные методы биометрической аутентификации пользователей должны обладать высокой точностью, универсальностью и высокой производительностью (практически в реальном времени). Биометрическая аутентификация подразделяется на две категории: физическая и поведенческая. Физическая биометрия основывается на определённых индивидуальных физических характеристиках людей и сочетает в себе следующие методы: сканирование лица, рисунка вен ладоней, голоса, радужной оболочки глаза и отпечатков пальцев. Поведенческая биометрия работает исходя из того, что поведение человека при выполнении определённых задач обычно достаточно отчётливо повторяется, чтобы его можно было использовать для аутентификации пользователя. В качестве примера можно привести динамику касания сенсорного экрана смартфона, нажатия клавиш клавиатуры и динамику движения и кликов мыши. Если сравнивать поведенческую биометрию с физической биометрией для аутентификации, поведенческая биометрия привлекла больше внимания из-за её более широкой применимости, меньшей навязчивости и отсутствия внешних датчиков. Кроме того, было продемонстрировано, что динамика мыши является непрерывным, портативным и ненавязчивым решением для аутентификации пользователя. Кроме того, методы машинного обучения (ML) и глубокого обучения (DL) могут извлечь выгоду из огромных объёмов данных динамики движения мыши, доступных в доменном пространстве. Когда методы ML и DL объединяются, работа с большим количеством данных показывает удивительные результаты. ML оказалось достаточно сильным, чтобы его можно было применять к различным проблемным областям, и использует неявные шаблоны на больших объёмах данных, которые слишком сложны для восприятия людьми. Тем не менее этот метод всё же требует большого ручного труда для извлечения нужных признаков из большого количества данных. Найти наилучшее сочетание гиперпараметров, извлекаемых функций и методов подготовки данных для конкретной задачи очень сложно. Аутентификация с помощью ИИ может решать ряд задач в сочетании с машинным обучением и глубокими нейронными сетями. Рассмотрим текущее состояние аутентификации с применением ИИ. Аутентификация с использованием связки логина и пароля больше не являются единственным методом аутентификации. ИИ успешно работает с распознаванием изображений, таких как отпечатки пальцев, рисунки вен ладоней и распознавание лиц, а также хорошо верифицирует пользователей по динамике нажатия клавиш и движения мыши.

Важным шагом в развитии биометрической идентификации является решение о том, какие данные следует комбинировать и как их комбинировать. На данный момент исследователи предложили большое количество мультибиометрических комбинаций. В мультимодальных методах биометрического распознавания, использующих два подхода

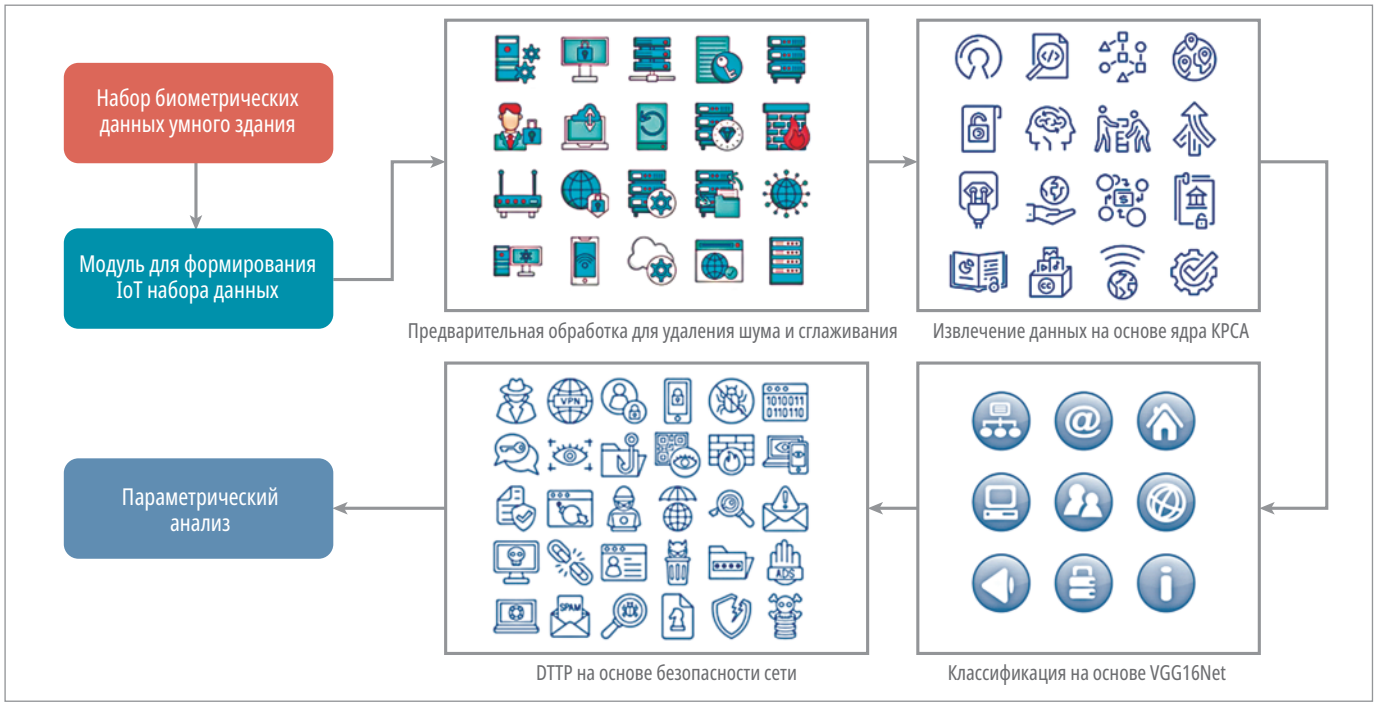


Рис. 1. Общая архитектура безопасной передачи данных

на уровне признаков: первый – оптимизация по алгоритму светлячков, а второй – сочетание теории фракталов и алгоритма светлячков, также для выполнения предварительной обработки применяется метод быстрого преобразования Фурье (FFF) и метод опорных векторов (SVM). В последние годы эта тенденция была определяющей, а методы аутентификации с помощью ИИ лидируют с точки зрения безопасности и совместимости с максимально возможным количеством реальных систем.

Рассмотрим метод безопасной передачи данных и обнаружение злоумышленников в системе биометрической аутентификации. Новый метод безопасной передачи данных при биометрической аутентификации основан на технологиях извлечения признаков с последующей их классификацией. Здесь злоумышленник обнаруживается путём сбора биометрической базы данных умного здания на основе IoT. Функции обработанных данных извлекаются с помощью анализа основных компонентов на основе ядра (KPCA). Затем обработанные признаки классифицируются с использованием свёрточной архитектуры VGG 16. Затем вся сеть защищается с помощью протокола детерминированной доверительной передачи (DTTP). Общая архитектура предлагаемого метода представлена на рис. 1.

Чтобы получить более точные и качественные данные, необходимо провести нормализацию данных для масштабирования характеристик, чтобы они соответствовали заданному максимальному и минимальному значению, обычно между единицей и нулем, как показано в уравнении (1). Это является одним из подходов к предварительной обработке данных.

$$f_{\text{norm}}(x) = \frac{x - x_{\min}}{x_{\max} - x_{\min}}. \quad (1)$$

В уравнении (1) приведена техника преобразования значений (MMN, MMS) так, что они располагаются в диапазоне от 0 до 1. Далее использовалась свёрточная нейронная сеть VGG16, результаты работы которой достигают точности 92,7% в задачах распознавания объектов на изображении. Обучение модели проводилось на базе более чем 14 миллионов изображений, принадлежащих к 1000 классам. Безопасная передача данных основана на использовании протокола детерминированного доверия (DTTP). Данный протокол способствует пересылке пакетов для каждого узла с помощью комбинированных значений доверия (CTV).

Каждый сенсорный узел в предлагаемом методе имеет CTV, основанный на следующих факторах оценки доверия:

- идентификация: содержит информацию о местоположении узла, а также его идентификатор;
- чувствительность данных: этот элемент включает в себя сбор данных и определение времени события;
- согласованность: уровень согласованности узла представлен этим фактором.

CTV отражает общую надёжность узла, определяемую с использованием трёх указанных выше параметров. С их помощью можно идентифицировать вредоносные или взломанные узлы на основе этих функций и фильтровать данные из сети. Понижая или повышая CTV, узел исключается или добавляется. Каждый агрегатор идентифицирует пакет, добавляя его хеш-значение к CTV, и передаёт его узлу назначения. Узел назначения проверяет хеш-значение, и проверяется CTV всех узлов. CTV увеличивается, если хеш-значение подтверждается; в противном случае он уменьшается. Соответствующий узел считается вредоносным, если CTV падает ниже уровня доверия. С течением времени значения доверия для соседних узлов непрерывно меняются. Если узел делает несколько незначительных ошибок при приёме или передаче событий, это мало влияет на значение доверия, которое оценивают его соседи. В противном случае, если узел постоянно передаёт неточные данные или редко связывается со своими соседними узлами, его значение доверия падает и приближается к –1. В результате на этом этапе можно обнаружить и классифицировать некоторые вредоносные или скомпрометированные узлы, которые регулярно передают противоречивые или недостоверные данные.

Ниже приведён алгоритм, который демонстрирует работу безопасной передачи данных на основе DTTP.

Для проверки надёжности предложенных алгоритмов распознавания ис-

```
Algorithm 1: DTTP
For every sensor node, S, I = 1, 2, . . . ,n
    Calculate identification factor Idi
    Calculate sensing result SR
    Calculate consistency value CVi
    Evaluate CTVi
End for
Select aggregator node Aj with highest CTVi
For every aggregator Aj, j = 1, 2, . . . .n
    When Ai receives data packet from node
    Si, it measures its trust value CTVi
        If CTVi < CTVi then Ai will not
        aggregate packet
        Else
        Aj aggregates packet and increment
        its counter CTj as Ctj = Ctj +a
        Where a is the number of packets
        successfully aggregated by Aj
        End if
    Aj produces a random hash value
[MAC (agg, Ctj]
    Aj transmits [MAC (agg, Ctj] to the sink
End for
When all aggregated data from Ai reaches sink,
it checks the counter value Ctj
    If Ctj > Ctj , then
    Aj is well behaving
    Else
    Aj is misbehaving
End if
Aj is prohibited from further transmissions
```

Таблица 1. Сравнительный анализ точности

Количество изображений	RBM	CNN	KPCA_VGG-16-DTTP
100	68	75	81
200	72	77	85
300	75	79	88
400	79	85	92
500	83	90	96

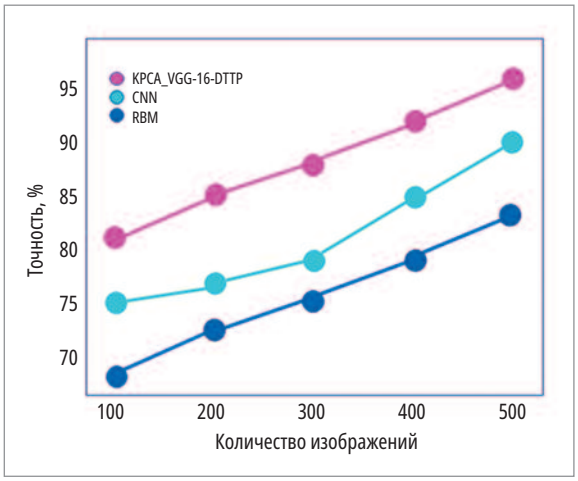


Рис. 2. Сравнение точности

Таблица 2. Сравнительный анализ F-показателя

Количество изображений	RBM	CNN	KPCA_VGG-16-DTTP
100	65	68	73
200	68	71	76
300	72	75	79
400	77	78	81
500	79	81	85

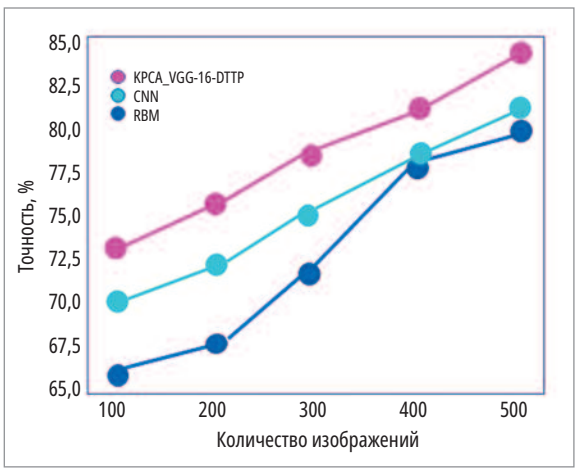


Рис. 3. Сравнение F-оценки

пользовались две открытые базы данных. Шаньдунский университет собрал базу данных рисунков вен фаланг пальцев (FV). Каждое изображение хранится в формате «BMP», который имеет размерность 320×240 пикселей.

Гонконгский политехнический университет собрал базу данных 3D-изображений суставов пальцев (FKP), и в эту базу данных включено 7920 фотографий, состоящих из 12 изображений указательных и средних пальцев обеих рук 165 человек. Поскольку в базе данных FKP больше участников, чем в базе данных FV, для сравнения были выбраны только 106 из них. Такой подход был необходим для слияния модальностей FV и FKP на этапе обучения и тестирования. В выбранных унимодальных и мультимодальных методах классы каждой базы данных были разделены на две отдельные подбазы данных, 60% из которых использовались для обучения, а 40% – для тестирования. После двух перекрестных проверок была рассчитана точность распознавания путём чередования обучающего и тестового изображений.

В табл. 1 и на рис. 2 показан сравнительный анализ точности между предложенными и существующими методами. В данном случае был проведён сравнительный анализ различных наборов биометрических данных на основе количества обработанных изображений. Расчёт точности выполнялся с помощью метода прогнозирования на основании технологий глубокого машинного обучения (DL). Предложенный метод достиг 96% точности для 500 изображений на основе их итераций, в то время как существующий RBM достиг 83%, а CNN достиг 90% точности.

В табл. 2 и на рис. 3 показаны различные сравнения биометрических изображений на основе наборов данных с точки зрения F-показателей. Для расчёта F-показателя количество обработанных изображений составило 500 изображений как для существующей, так и для предлагаемой методики. F-оценка показывает способность различать каждый признак независимо от других признаков. Для первого признака генерируется одна оценка, а для второго признака получается другая оценка. Однако в нём ничего не говорится о том, как эти два элемента работают вместе. Здесь вычисление F-показателя с использованием эксплуатации определило эффективность прогнозирования. Он создаётся путём рассмотрения гармонического компонента отклика и точности. Если расчётный балл равен 1, это считается отличным результатом, тогда как 0 баллов указывает на плохой результат. Фактическая отрицательная ставка не принимается во внимание F-измерениями. Предложенный метод достиг 85% F-оценки для 500 изображений на основе их итераций, в то время как существующий RBM получил 79%, а CNN – 81% F-оценки.

В табл. 3 и на рис. 4 показано сравнение расчётных значений точности биометрических данных предлагаемых и существующих методов на основе 500 изображений. Точность класса рассчитывается путём деления общего количества элементов, классифицированных как принадлежащие к положительному классу, на количество истинно положительных результатов. Вероятность состоит в том, что класси-

Решения на DIN-рейку от Delta Electronics

- Источники питания от 7 до 960 Вт с выходными напряжениями 5, 12, 24, 48 В
- ИБП постоянного тока 24 В/24 В с током нагрузки до 40 А
- Модули резервирования N+1, 1+1
- Буферные модули со временем удержания питания от 200 мс до 8 с
- Батарейные модули (для монтажа двух батарей 7-9 Ач)

DELTA

фикационная функция будет давать положительный показатель, если она присутствует. Предложенный метод достиг 92% точности для 500 изображений, в то время как существующий RBM получил 85%, а CNN – 89%.

В табл. 4 и на рис. 5 показан сравнительный анализ полноты, основанный на количестве изображений из набора входных данных. В этом контексте полнота описывается как отношение общего количества компонентов, которые действительно попадают в положительный класс, к нескольким истинно положительным. Процент положительных образцов, которые были правильно идентифицированы как положительные, из всех положительных образцов – это то, как оценивается полнота. Насколько хорошо метод может распознавать положительные образцы, рассчитывается по полноте. Полнота увеличивается по мере того, как определяется больше положительных образцов. В данном случае предложенный метод достиг 80% отзыва для 500 изображений на основе их итераций, в то время как существующий RBM получил 65%, а CNN достиг 72% отзыва.

В табл. 5 и на рис. 6 показан сравнительный анализ RMSE, который указывает на то, что при обработке 500 изображений произошла ошибка. При обучении моделей регрессии или временных рядов RMSE является одним из наиболее широко используемых показателей для оценки того, насколько точно модель прогнозирования предсказывает значения по сравнению с реальными или наблюдаемыми значениями. Квадратный корень MSE используется для расчёта RMSE. RMSE вычисляет изменение каждого пикселя в результате обработки. Предложенный метод достиг 46% RMSE для 500 изображений на основе их итераций, в то время как существующий RBM получил 55%, а CNN достиг 48% RMSE.

Таблица 3. Сравнительный анализ точности

Количество изображений	RBM	CNN	KPCA_VGG-16-DTTP
100	77	81	83
200	79	83	85
300	81	86	89
400	83	87	91
500	85	89	92

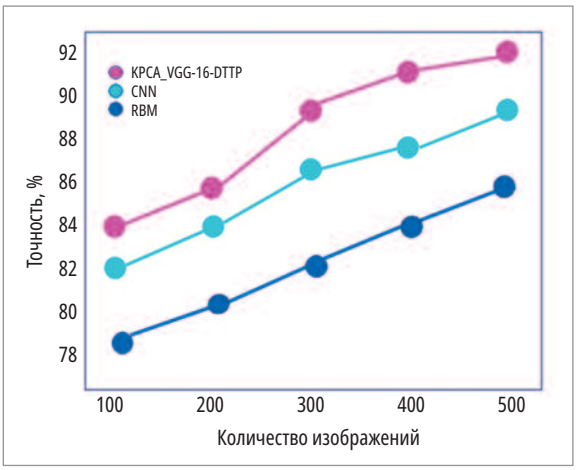


Рис. 4. Сравнение точности

Таблица 4. Сравнение отзыва

Количество изображений	RBM	CNN	KPCA_VGG-16-DTTP
100	55	61	65
200	58	63	69
300	61	67	73
400	63	70	75
500	65	72	80

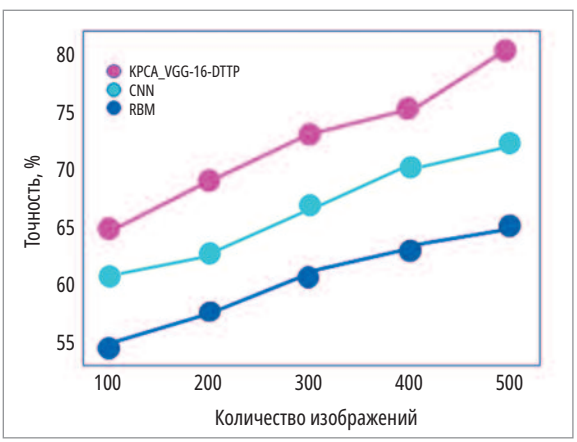


Рис. 5. Сравнение полноты

Таблица 5. Сравнительный анализ RMSE

Количество изображений	RBM	CNN	KPCA_VGG-16-DTTP
100	65	61	58
200	62	55	55
300	60	52	52
400	58	51	51
500	55	48	46

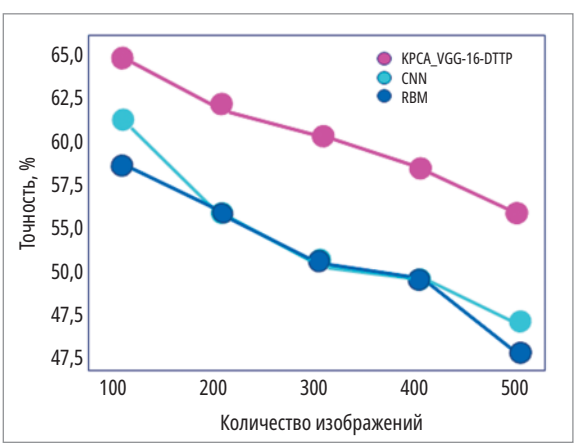


Рис. 6. Сравнение RMSE

Заключение

В этом исследовании был предложен новый метод безопасной передачи данных и обнаружения злоумышленника в системе биометрической аутентификации путём извлечения признаков с классификацией. В данном методе обнаружение злоумышленника реализовано на основе собранной биометрической базы данных умного здания на основе IoT. Эти биометрические данные обрабатываются для удаления шума, сглаживания и нормализации. Функции обработанных данных извлекаются с использованием анализа основных компонентов на основе ядра (KPCA). Затем обработанные признаки были классифицированы с использованием свёрточной архитектуры сети VGG-16. Затем вся сеть была защищена с помощью протокола детерминированной доверительной передачи (DTTP). Экспериментальные результаты достигли таких параметров, как точность 96%, F-показатель 85%, точность 92%, полнота 80% и среднеквадратическая ошибка 46%. Развитием этого метода может быть использование его в облачной системе кибербезопасности. Дальнейшее развитие этого метода может быть реализовано на основе набора данных, полученных в реальном времени с повышенной точностью, с использованием технологии блокчейна и методами машинного обучения. ●

Автор – сотрудник фирмы ПРОСОФТ
Телефон: (495) 234-0636
E-mail: info@prosoft.ru

УСТРОЙСТВА ВВОДА ДЛЯ ЭКСТРЕМАЛЬНЫХ УСЛОВИЙ

KEY TECHNOLOGY (CHINA) LIMITED
深圳市键特电子有限公司
iKey
NSi KEYBOARDS & POINTING DEVICES for the most demanding jobs

- Множество вариантов исполнения и установки
- Различные варианты интерфейсов
- Степень защиты до IP68
- Устройства, соответствующие IEC 60945
- Опциональная регулируемая подсветка
- Возможность кастомизации

ProSoft®

ОФИЦИАЛЬНЫЙ ДИСТРИБЬЮТОР

(495) 234-0636
INFO@PROSOFT.RU

WWW.PROSOFT.RU

Обновление линейки процессорных модулей PC104 Fastwel

Индустриальные процессорные модули разработки и серийного производства Fastwel – уникальное явление на рынке РФ. Изделия проектируются российскими разработчиками от уровня схемотехники и серийно выпускаются на мощностях, расположенных в Москве, для системных интеграторов в высокоответственных сферах применения. Все модули соответствуют как международным стандартам (форм-факторы PC104, CPCI 3U и другие), так и требованиями российских ГОСТ.

Одним из наиболее популярных форм-факторов у разработчиков прикладных систем является формат PC104 в различных вариантах – PC104-Plus, PC104e, StackPC и т.д. В этом формате Fastwel на сегодняшний день предлагает широкий спектр изделий практически для любых применений. Многие из процессорных модулей выпускаются серийно уже более 10 лет, и их срок жизни подходит к концу.

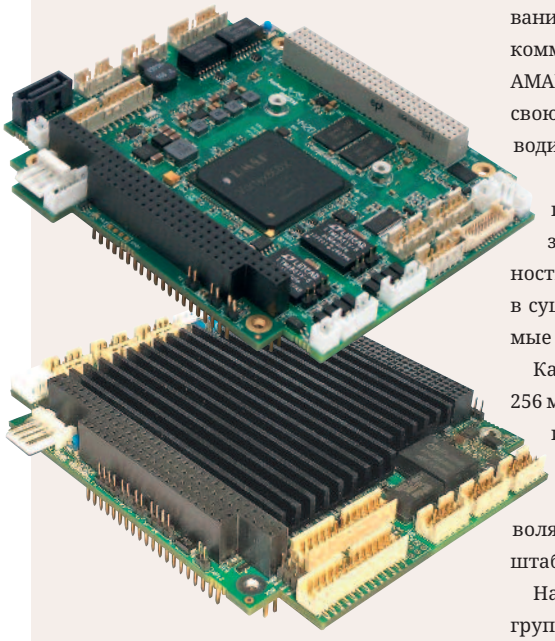
Для плавного перехода от платформ CPC304, CPC306, CPC308 к более современным и долговременно доступным моделям Fastwel предлагает новые одноплатные компьютеры CPC314 и CPC316 стандарта PC104-Plus с процессором Vortex86DX3. Процессор архитектуры x86 разработан и серийно производится в КНР, он не имеет ограничений по поставке на рынок России.

Модули CPC314 и CPC316 отличаются высокой производительностью при небольшом тепловыделении, что особенно важно при разработке безвентиляторных систем и решений в компактных корпусах.

Основной сферой применения одноплатных компьютеров является использование их в качестве вычислительного ядра прикладной системы с широким набором интерфейсов ввода-вывода, расположенных

Основные технические характеристики модулей CPC314 и CPC316 в сравнении с предшественниками

	CPC304-01	CPC308-01	CPC314-01	CPC316-01	CPC316-02
Процессор	AMD Geode LX 800 (500 Мгц)	PineView-M (N450) 1.66Гц	Vortex86DX3 (800 МГц)	Vortex86DX3 (800 МГц)	Vortex86DX3 (800 МГц)
ОЗУ	256 МБ DDR	1 Гбайт DDR2	2 ГБ DDR3	2 ГБ DDR3	2 ГБ DDR3
FLASH-диск напаяный	1 ГБ	4 ГБ	–	8 ГБ	8 ГБ
MicrSD	–	–	1 + карточка 4ГБ	–	–
Compact Flash	1	1	–	1	1
HDD	–	2×SATA	1×SATA	–	–
RS-232	2×RS-233	2×RS-232	2×RS-233	2×RS-232	2×RS-232
RS-485/422	2×RS-422/485 гальв. изолированный	2×RS-422/485 гальв. изолированный	2×RS-422/485 гальв. изолированный	2×RS-422/485 гальв. изолированный	2×RS-422/485 гальв. изолированный
Ethernet	2×10/100 Мбит/с	2×10/100/1000 Мбит/с	2×10/100 Мбит/с	2×10/100/1000 Мбит/с	2×10/100/1000 Мбит/с
USB	2×USB 2.0	4×USB 2.0	2×USB 2.0	4×USB 2.0	4×USB 2.0
KB/Mouse	PS/2	PS/2	PS/2	–	–
Порт GPIO ввод/вывод	8 линий	8 линий	8 линий	8 линий	8 линий
Порт LPT	–	–	LPT	–	–
Цифровой порт ввода/вывода	–	–	–	48×DIO	48×DIO
Audio	Analog IN/Out/Mic	Analog IN/Out/Mic	Analog IN/Out/Mic	Analog IN/Out/Mic	–
VGA	1600×1200 (85 Гц) 1920×1440 (75 Гц 32 бит)	1400×1050 60 Гц (N450)	До 1920×1080, цвет 32 бит	До 1920×1080, цвет 32 бит	До 1920×1080, цвет 32 бит
LVDS	1024×768 (60 Гц)	1280×800 60 Гц (N450)	До 1920×1080, цвет 32 бит	До 1920×1080, цвет 32 бит	–
Шины	ISA / PCI				
Рабочая температура	–40...+85°C				
Электропитание	+5 В / 7,5 Вт	+5 В / 15 Вт	+5 В / 10 Вт		
CPU Mark	61	348	604		
CPU Integer Math	6	24	31		
CPU Floating Point	20	105	25		
CPU Compression	122	802	449.5		
Memory Mark	43	226	80.8		
2D Graphics	86	222	92		
Disk Mark	222	297	388		
Compress (MIPS)	280	1000	600		
Decompress (MIPS)	270	1500	1071		



на самом модуле или на платах расширения Fastwel, сторонних производителей или самостоятельной разработки.

Такое применение актуально для построения систем реального времени, бортовых систем, средств безопасности и связи, контроля производства и других ответственных применений в индустриальном температурном диапазоне (от –40 до +85°C) и с высокими ударно-вибрационными нагрузками.

Приобрести модули или получить изделие на тестирование под проект можно, прислав запрос на адрес *support@fastwel.ru.* ●

AMAX-5070 – улучшает системную интеграцию. Коммуникационный модуль с поддержкой ModBus TCP

Компания Advantech, один из ведущих мировых производителей платформ промышленного Интернета вещей и оборудования для автоматизации, выпустила новый коммуникационный модуль (каплер) – AMAX-5070, тем самым продолжая развивать свою линейку современных высокопроизводительных ПЛК – AMAX-5000.

Модуль AMAX-5070 поддерживает распространённый протокол ModBus TCP, за счёт чего обеспечивается возможность простой и надёжной интеграции как в существующие, так и во вновь создаваемые системы ИТ/ОТ.

Каплер поддерживает подключение до 256 модулей ввода/вывода серии AMAX-5000 и может устанавливаться удалённо от головного устройства на расстоянии до 100 м, что, в свою очередь, позволяет строить распределённые и масштабируемые системы.

Наличие функции идентификатора группы помогает инженерам быстро синхронизировать аппаратное и программное обеспечение своих приложений и позволяет решать проблемы нехватки IP-адресов, так как для каплера требуется всего один IP-адрес.

За счёт нового модуля AMAX-5070 Advantech расширяет коммуникационные возможности ПЛК серии AMAX-5000, которые уже включают поддержку таких шин и протоколов, как EtherCAT, CAN, Profibus, и беспроводные стандарты передачи данных. ●

Имитационная поверка электромагнитных расходомеров NovaMAG

Электромагнитные расходомеры NovaMAG имеют опцию беспроливной (имитационной) поверки. Имитационная поверка выполняется при помощи переносного автономного устройства Артчек.

Беспроливная поверка прибором Артчек имеет ряд преимуществ:

- возможность выполнения поверки по месту эксплуатации приборов;
- удобство и простота поверки расходомеров достигается автономностью прибора, удобным интерфейсом и наличием автоматического режима. ●

Новое гигиеническое исполнение датчиков давления APZ 3420 M, APZ 3420 S, APZ 3410

Разработаны новые резьбовые гигиенические механические присоединения для датчиков APZ 3420 m / APZ 3420 s / APZ 3410. В этих моделях доступны к заказу:

- присоединение с керамическим сенсором и торцевым уплотнением (аналог Aceptoflex Vario);
- присоединение с керамическим сенсором или кремниевым сенсором со стальной мембраной с уплотнением на конус;
- присоединение с торцевой стальной мембраной с периферийным уплотнением.

Новые присоединения разработаны для применения на предприятиях, работающих по строгим гигиеническим стандартам.

Применение датчиков давления с обычными механическими присоединениями может привести к образованию застойных зон с последующим образованием бактерий.

Датчики давления APZ 3420 m, APZ 3420 s, APZ 3410 применяются при производстве молока, мороженого, йогуртов и других пищевых продуктов, в том числе там, где используются CIP- и SIP-мойки. ●

+7 (495) 796-92-20
piezus.ru
e-mail: zakaz@piezus.ru
109316, г. Москва, Волгоградский проспект, дом 42, корпус 5