СКУД: ВЫЙТИ ЗА РАМКИ ФИЗИЧЕСКОГО КОНТРОЛЯ

Векторы развития рынка систем управления доступом в Азии, Европе и Америке в 2026 году

По данным MarketsandMarkets, мировой рынок систем контроля и управления доступом вырастет с $10,62 млрд в 2025 году до $15,80 млрд к 2030 году. Рост обеспечат биометрия и мобильные решения. В Азии высокий спрос на распознавание лиц и бесконтактные технологии, их популярности способствуют господдержка и законодательство в области конфиденциальности данных. Европа уделяет особое внимание соблюдению Общего регламента по защите данных (GDPR) и функциональной совместимости с облачными системами и мобильными учетными данными. В США интегрированные решения, сочетающие контроль доступа с другими мерами, удовлетворяют спрос на безопасность и соответствие требованиям.

asmag.com Security & IoT

Текст:
RUБЕЖ Analytics по материалам A&S Magazine (asmag.com)

ДОСТИЖЕНИЯ В ОБЛАСТИ ИИ

В азиатских странах активно внедряют интеллектуальные системы контроля доступа. Особенно там, где нужны оперативность и безошибочность, например, в аэропортах, медицинских учреждениях и госсекторе с повышенными требованиями к безопасности. Эти системы анализируют каждый случай авторизации, снижая ложные срабатывания и усиливая эффективность работы.

Ханчул Ким, генеральный директор корейской компании Suprema, отмечает, что алгоритмы глубокого обучения обрабатывают миллионы точек данных в реальном времени, поэтому точность распознавания постоянно растет.

Среди интеграторов популярно применение ИИ в сфере управления доступом. Это открывает перспективы для разработки интеллектуальных и надежных систем. Растет спрос на многофакторную аутентификацию, которая объединяет распознавание лиц, отпечатков пальцев и мобильные учетные данные.

ПРОАКТИВНЫЕ ФУНКЦИИ

Американский рынок нацелен на прогнозирование и предотвращение рисков, то есть сочетание систем контроля доступа с ИИ. По словам **Кумара Сокка**, генерального директора американской Acre Security, подобные системы расширяют возможности для мониторинга происшествий, оперативного обнаружения аномалий и беспрепятственной адаптации к новым обстоятельствам. Симбиоз ИИ и облачных решений открывает новую эпоху в сфере контроля доступа, делая его более умным, адаптивным и ориентированным на будущее.

Для профессионалов в области физической безопасности это означает рост автоматизации и улучшение понимания текущей обстановки. Сокка отмечает, что в перспективе службы безопасности станут более зависимыми от технологий из-за необходимости оперативно принимать взвешенные решения и оптимизировать производственные процессы.

ОБЛАЧНЫЕ ТЕХНОЛОГИИ И ОТКРЫТЫЕ ПРОТОКОЛЫ

Облачные решения позволяют компаниям централизованно координировать права доступа и управлять рабочими процессами. По мнению Ханчула Кима, от цифровых платформ ожидают большего, чем простого контроля доступа. «Компании воспринимают системы контроля доступа как часть комплексной экосистемы, включающей видеоаналитику, отслеживание рабочего времени, управление посетителями и обслуживание зданий», — подчеркнул он. Этот тренд стимулирует потребность в платформах, которые поддерживают интеграцию через API и SDK и позволяют объединять их с различными сторонними системами. Для системных интеграторов это сигнал для создания кастомизированных и масштабируемых решений с расширенным функционалом.

Облачные решения позволяют компаниям централизованно координировать права доступа и управлять рабочими процессами

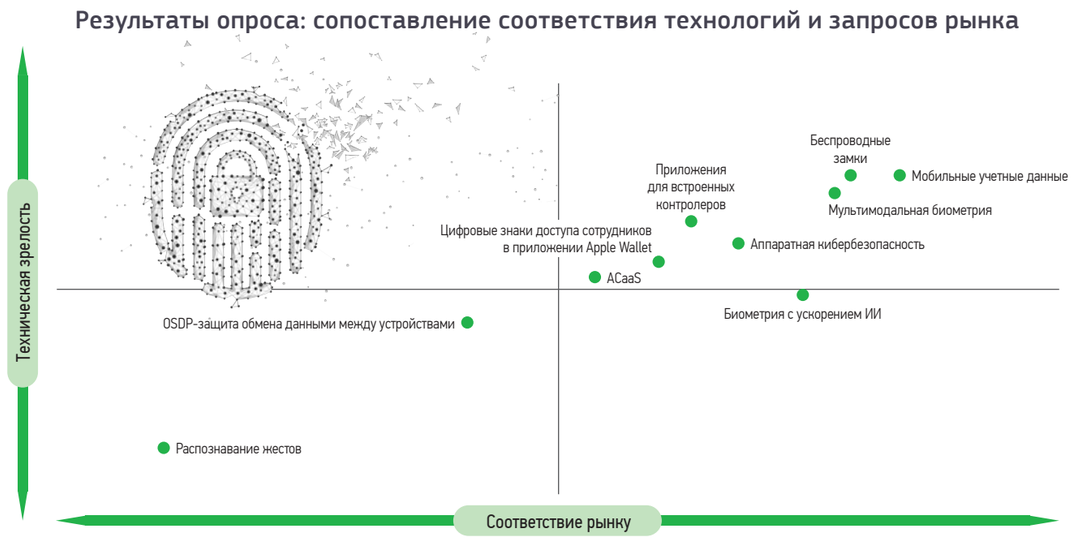
В Европе массово переходят от закрытых систем к открытым. **Джеймс Кларк**, руководитель отдела продаж американской AMAG Technology, уверен, что открытые протоколы, такие как OSDP, завоевывают популярность за счет улучшения совместимости и долгосрочной гибкости. «Организации теперь могут централизованно управлять учетными данными, разрешениями и событиями безопасности из любой точки мира, что одинаково удобно как для администраторов, так и для пользователей», — также убежден и Кумар Сокка.

Облачные платформы способны автоматически обновлять программное обеспечение, гарантировать время безотказной работы и централизовать управление. Такой подход создает благоприятные условия для эффективного масштабирования систем безопасности на множестве объектов.

МОБИЛЬНЫЕ ДАННЫЕ

Тренд на облачные технологии отражает и более масштабную тенденцию — мобильные идентификаторы. Компаниям интересны гибридные форматы работы и доступ из разных локаций. Мобильные учетные данные активируют и деактивируют права доступа дистанционно, что привлекает удобством и уровнем защиты.

«Мобильные технологии доступа — это интеллектуальное, оперативное и безопасное решение для контроля доступа, идеально подходящее для современной мобильной среды, — отмечает Кумар Сокка. — Мобильный доступ и решения на основе идентификационных данных позволяют организациям в режиме реального времени предоставлять, контролировать и блокировать права доступа. Встроенные механизмы защиты устройств, такие как биометрия и пароли, повышают безопасность каждой операции». Стоит отметить, что учетные данные легко переносить и интегрировать с облачными платформами.



МЕЖСИСТЕМНАЯ ИНТЕГРАЦИЯ

В то же время европейский рынок смотрит дальше интеграции исключительно охранных систем. Разработчики заинтересованы в межсистемном взаимодействии. Джеймс Кларк отмечает, что подлинная системная интеграция — это объединение контроля доступа, видеонаблюдения, управления учетными данными с отделами кадров и HR, системами отопления, вентиляции и кондиционирования, корпоративными приложениями и платформами для управления посетителями. Подобная межфункциональная интеграция смещает фокус отрасли в сторону «архитектуры, ориентированной на идентификацию».

Для интеграторов такая тенденция расширит спектр технических компетенций и обеспечит более тесное взаимодействие с ИТ-специалистами и службами эксплуатации зданий. Акцент уходит с традиционной защиты дверных проемов и считывающих устройств к обеспечению безопасности и оптимизации цикла идентификационных данных как в цифровом, так и в физическом пространстве.

СЕРВИСЫ И ПОДПИСКИ

Компании нацелены на стабильную прибыль, а не на единичные сделки. И системные интеграторы держат курс в сторону сервисов и подписок. По словам Кумара Сокки, облачное видеонаблюдение, дистанционная диагностика систем и регулярные обновления софта в ежемесячные пакеты гарантируют прогнозируемый доход и укрепляют связи с клиентами.

Интеграторы внедряют аналитические платформы, позволяющие централизованно управлять системами и настраивать их удаленно. «Такой переход превращает отдельные проекты в долгосрочные контракты, повышает предсказуемость доходов и делает интеграторов надежными партнерами в сфере долговременной безопасности», — подчеркивает Сокка. Подобная трансформация бизнес-модели подразумевает освоение новых компетенций, более тесное взаимодействие с поставщиками и инвестиции в облачные решения.

КОНФИДЕНЦИАЛЬНОСТЬ И ЗАКОНОДАТЕЛЬСТВО

Динамичное развитие законодательства о защите информации в азиатском регионе значительно воздействует на разработку и применение СКУД. Япония и Южная Корея адаптировали свои законы к требованиям Общего регламента ЕС по защите данных (GDPR), а в Индии был принят Закон о защите личных данных в цифровой среде. Законодательные акты акцентируют внимание на согласии пользователей, ограничении объема собираемых данных и обеспечении прозрачности. По словам Ханчула Кима, организации частного и государственного секторов отдают предпочтение надежным системам для защиты

персональных данных по прозрачным схемам и с возможностью контроля.

Джеймс Кларк уверен, что GDPR существенно влияет на системы контроля и управления доступом в ЕС и классифицирует биометрическую информацию как «особую категорию» данных. Это требует четкой правовой базы для реализации проектов, как правило, прямого согласия или законного интереса, а также строгих мер безопасности при сборе, хранении и использовании данных.

Европейским и азиатским интеграторам необходимо соблюдать протоколы конфиденциальности на всех этапах разработки, от проектирования до обслуживания. Неточности в толковании или реализации влекут за собой регуляторные риски для конечных пользователей. Компании, предоставляющие последовательные гарантии конфиденциальности, получают конкурентное преимущество в секторах государственного управления, здравоохранения и финансов.

КИБЕРБЕЗОПАСНОСТЬ

Киберугрозы требуют от поставщиков и разработчиков активнее внедрять международные стандарты для сохранности информации и стабильности работы оборудования. Сертификаты вроде ISO/IEC 27001 по управлению безопасностью данных и ISO/IEC 27701 по контролю конфиденциальной информации стали для сектора эталонными.

> Киберугрозы требуют от поставщиков и разработчиков активнее внедрять международные стандарты для сохранности информации и стабильности работы оборудования

Решения для контроля и управления доступом в перспективе будут соответствовать мировым стандартам информационной безопасности, конфиденциальности и функциональной совместимости. Такова общая тенденция.

В Северной Америке ключевым требованием бизнес-клиентов стали защищенные и соответствующие нормативам продукты. «В наше время безопасность выходит за рамки физических барьеров, — отмечает Кумар Сокка. — Подключение большего количества устройств, платформ и данных стирает различие между охраной физической и цифровой инфраструктуры». На деле платформы обязаны выявлять угрозы независимо от того, вызваны они физическим или цифровым взломом.

ПЕРСПЕКТИВЫ

Согласно исследованию американской Grand View Research, в 2024 году объем рынка Азиатско-Тихоокеанского региона достиг $3,38 млрд. По прогнозам, он вырастет до $6,15 млрд к 2030 году (среднегодовой рост в 10,6%). Слияние ИИ, биометрии и облачных решений превратят контроль доступа в ключевой элемент для поддержания бесперебойной работы предприятий и их цифровой эволюции.

Успех обеспечен тем интеграторам, которые предложат унифицированные платформы, системы которых адаптированы как к местному законодательству и международным стандартам, так и к специфическим операционным задачам клиентов.

Аналогичные тенденции сильны и в Европе. Джеймс Кларк подчеркивает, что лидерами следующей волны инноваций в европейском секторе контроля доступа станут те компании, которые начнут с комплексного решения операционных задач, а не просто с продажи оборудования.

В Северной Америке эволюция рынка СКУД в ближайшее время будет зависеть от способности индустрии адаптировать и применять на практике операционные модели. Направление развития очевидно — переход к более интеллектуальным, взаимосвязанным и устойчивым системам безопасности, от решений на основе ИИ до сервисов по подписке.