

АНАЛИЗ ОТЕЧЕСТВЕННЫХ СИСТЕМ СКУД: ПОИСК АЛЬТЕРНАТИВ ЗАРУБЕЖНЫМ РЕШЕНИЯМ

Аннотация. Системы контроля и управления доступом (СКУД) – важная часть инфраструктуры промышленных объектов. Отечественные решения выгоднее по цене и лучше адаптированы к местным условиям, зарубежные – превосходят по функционалу и эффективности (но разрыв сокращается). Цель работы – изучить особенности российских СКУД и сравнить их с зарубежными аналогами.

Ключевые слова: СКУД, применение, системы, индивидуализация, инновации.

Введение.

Контроль доступа – это набор программных и аппаратных средств, а также ведомственных инструкций, которые позволяют решать управленческие и административные задачи, посещать отдельные объекты и операции, отслеживать перемещения персонала и проводить время на местах.

Исключение сотрудника из рабочей силы особенно важно для обеспечения безопасности объектов, где цена ошибки и иногда элементарные потребности очень высоки. С другой стороны, сотрудник службы безопасности должен получать полную и точную информацию о местных событиях и иметь удобный способ бесперебойной работы и решения проблем [7].

Система контроля доступа обычно содержит идентификационные номера, считыватели карт, контроллеры и серверы ACU [1], а идентификационная карта содержит информацию для идентификации пользователя. Наряду с этим, в исследовании показаны перспективы развития технологий непрерывного контроля доступа в организациях, использующих информационные ресурсы с функциями конфиденциальности, сегодня технологические системы машинного обучения (нейротехнологии) в сочетании (интеграции) с системами искусственного интеллекта.

Основная часть.

Системы контроля и управления доступом часто используются в сложных сооружениях или учреждениях, требующих повышенных мер безопасности. СКУД очень удобна, поскольку автоматически контролирует и регулирует доступ [2].

Система контроля и управления доступом состоит из множества сложных элементов и узлов, к которым предъявляются особые требования. В основе СКУД лежат контроллеры, идентификаторы, считыватели, а также зоны, уровни и точки доступа. От качества системы зависят надежность обеспечения безопасности объекта, контроль персонала и функциональность системы в целом.

Независимо от режима работы работников предприятия, работодатель обязан вести учёт отработанного ими времени. Для этого используется специальный табель, который является обязательным документом для любого предприятия или организации, осуществляющей хозяйственную деятельность.

Системы учета рабочего времени позволяют автоматизировать этот процесс и в любой момент времени получать полную и точную информацию по каждому сотруднику [2].

Крупные учреждения или предприятия с большим скоплением людей используют турникеты для контроля безопасности. Они особенно эффективны, когда необходимо вести ежедневный учёт времени прихода и ухода сотрудников организаций.



Турникеты для контрольно-пропускного пункта исключают любые попытки проникновения в учреждение постороннего человека, даже если он завладел чужим пропуском – информация с него считывается системой управления устройства и передаётся на монитор компьютера службы безопасности. При наличии в базе данных фотопропуска личность нарушителя мгновенно устанавливается [3].

В РФ используется система СКУД Sigur – это программно-аппаратная система контроля доступа, позволяет наблюдать за происходящими событиями, сохранять и анализировать информацию, формировать отчеты, а также взаимодействовать с другими системами, также PASS24.online – это онлайн сервис для автоматизации выдачи пропусков и контроля доступа. Мобильное приложение для сотрудников и гостей.

Плюсы отечественной системы СКУД программное обеспечение Sigur состоит в том, что она имеет клиент-серверную архитектуру. Отдельные рабочие места в системе не лицензируются, что означает, что любое количество пользователей может использовать программное обеспечение с правами, назначенными каждому отдельному пользователю.

Потребуется установить любой из программных модулей на системный сервер только один раз, после чего вы сможете использовать его функционал на всех своих рабочих станциях, подключенных к этому серверу. Расстояние между рабочими станциями и сервером не имеет значения.

Серверное программное обеспечение Sigur и клиентское программное обеспечение Sigur могут работать под управлением Microsoft Windows (для сервера требуется как минимум Windows 7 SP1 или более поздняя версия, рабочая станция должна работать как минимум под управлением Windows XP SP3 или более поздняя версия) независимо от разрядности или Linux (Debian 32 бит) [4].

Заказчики сегодня заинтересованы не в отдельно стоящих СКУД, а в системах, которые легко интегрируются с другими средствами контроля и мониторинга. Это могут быть как комплексные автоматизированные системы управления зданиями, так и системы видеонаблюдения, видеоаналитики, охранно-пожарной сигнализации.

Таблица 1

Рейтинг самых надежных отечественных СКУД.

	Все пользователи	Разработчики, производители	Дистрибуторы, интеграторы и торговые дома	Пользователи
1.	APACS 3000 (AAM Системз)	APACS 3000 (AAM Системз)	APACS 3000 (AAM Системз)	APACS 3000 (AAM Системз)
2.	Lyrix (AAM Системз)	Lyrix (AAM Системз)	Lyrix (AAM Системз)	Lyrix (AAM Системз)
3.	Gate (Равелин)	Parsec (Релвест)	Gate (Равелин)	Gate (Равелин)
4.	PERCo	SIGUR	PERCo	RusGuard
5.	ИСО "Орион" (Болид)	Gate (Равелин)	IronLogic	IronLogic
6.	Parsec (Релвест)	PERCo	SIGUR	PERCo
7.	SIGUR	НЕЙРОСС/Борей (Итриум)	Parsec (Релвест)	SIGUR
8.	IronLogic	IronLogic	ИСО "Орион" (Болид)	Smartec
9.	Smartec	Интегра-СКД (Интегра-С)	Elsys (Электронные системы)	ИСО "Орион" (Болид)
10.	RusGuard	РЕВЕРС 8000 (СКД)	Smartec, RusGuard	RUBEZH

Зарубежные аналоги систем контроля доступа включают ведущие компании из разных стран, такие как Brivo (США), Honeywell (США), Kisi (США), Bosch (Германия) и ButterflyMX (США), и основаны на стандартизованных моделях контроля доступа, таких как управление



доступом на основе атрибутов (ABAC), ролевые игры (Role-Управление доступом на основе данных (RBAC), обязательное управление доступом (MAC) и дискреционное управление доступом (DAC). Они часто изготавливаются в соответствии с международными стандартами, такими как BS EN 60839-11-1.

Сравним по основным характеристикам 2 самые популярные в РФ и в США СКУД, SIGUR и Brivo (США) [5].

Таблица 2

Сравнение СКУД, SIGUR и Brivo (США) по функциональности [5].

Показатели сравнения	SIGUR	Brivo
Функциональное обеспечение	Санкционированный доступ людей, транспорта и других объектов в (из) помещения, здания, зоны и территории, путем идентификации личности по комбинации различных признаков: вещественный код (ключи, карты, брелоки), запоминаемый код (клавиатуры, кодонаборные панели и другие аналогичные устройства), биометрический (отпечатки пальцев, сетчатка глаз и другие);	Предотвращение несанкционированного доступа людей, транспорта и других объектов в (из) помещения, здания, зоны и территории;
Состав работы СКУД.	Устройства ввода идентификационных признаков (УВИП) в составе считывателей и идентификаторов	Устройства управления (УУ) в составе аппаратных и программных средств
Основные функции	Открывание УПУ после считывания идентификационного признака, доступ по которому разрешен в данную зону доступа (помещение или территорию) в заданный временной интервал или по команде оператора СКУД	Санкционированное изменение (добавление, удаление) идентификационных признаков в УУ и связь их с зонами доступа (помещениями) и временными интервалами доступа
Считыватели УВИП обеспечивают	Считывание идентификационного признака с идентификаторов	Формирование сигнала на открывание УПУ при идентификации пользователя

Таким образом, отечественное СКУД состоит из качественного ПО, ключей-идентификаторов, считающих контроллеров, исполнительных устройств, системы видеонаблюдения и сигнализации. Отечественный СКУД разделяют по масштабу системы, способу идентификации пользователей, способу управления, типу объектов контроля, области применения. Системы контроля управления доступом используют, чтобы ограничить доступ в здания, помещения или на территории, повысить уровень безопасности, вести учет рабочего времени, управлять потоком людей или транспорта.

Заключение.

Отечественные системы контроля доступа могут иметь преимущества перед зарубежными за счет лучшей адаптации к местным нормативным актам, более простой и



быстрой интеграции с местной инфраструктурой и потенциально более низких затрат за счет снижения импортных пошлин и транспортных расходов [6].

Хотя конкретные преимущества зависят от производителя и страны, отечественные варианты иногда могут обеспечить более быструю поддержку и более локализованный пользовательский опыт.

Отечественные системы часто разрабатываются в соответствии с конкретными национальными и местными правилами безопасности, конфиденциальности и защиты данных, которые могут существенно отличаться от зарубежных стандартов.

Отечественная система, скорее всего, легко интегрируется с другим доступным на месте оборудованием и программным обеспечением, упрощая настройку и снижая проблемы совместимости.

Отсутствие затрат на импорт, таможенных пошлин и сборов за обмен валюты может привести к снижению общих затрат для конечного пользователя.

Отечественные компании могут предложить более быстрое реагирование на запросы технической поддержки, помощи на месте и запасных частей, поскольку они базируются в одной стране или регионе.

Отечественные системы могут иметь более локализованные пользовательские интерфейсы, документацию и обслуживание клиентов, что упрощает их понимание и использование местной аудиторией. Меньший объем внутреннего рынка может означать меньшие инвестиции в исследования и разработки, что потенциально может привести к меньшему количеству расширенных функций по сравнению с глобальными конкурентами.

Отечественные системы могут не обладать таким же набором функций или таким же уровнем интеграции, как системы компаний, работающих на более крупном и конкурентном международном рынке [7].

Выбор отечественных производителей и продуктов может быть ограничен, что может сузить возможности выбора, доступные потребителям.

В то время как зарубежные системы часто имеют преимущество в доступе к более крупным бюджетам на исследования и разработки и более передовым технологиям, отечественные системы контроля доступа могут предложить значительные преимущества с точки зрения стоимости, соответствия требованиям и поддержки. Наилучший выбор зависит от конкретных потребностей пользователя, бюджета и технических требований.

Список литературы:

1. Средства и системы безопасности. Обзор рынка. URL: <http://stepconsulting.ru/publ/security.shtml>
2. Портной Евгений. О некоторых особенностях систем контроля и управления доступом. Директор по безопасности, 2011, № 10. URL: <http://old.s-director.ru/magazine/archive/viewdoc/2011/10/374.html>
3. Системы безопасности и видеонаблюдения. URL: <http://www.infotel-sec.ru/>
4. Магазин систем безопасности. URL: <http://www.safemag.ru/biometric-systems/>
5. <https://www.advaitgroup.co.in/the-advantages-of-using-acs-wires-for-transmission-lines/>
6. <https://thesecurepass.com/blog/access-control-system-types>
7. <https://researchview.ru/news/blog/rynek-slabotochnyh-sistem-v-rossii-skud-videoonablyudenie-i-pozharotushenie/>

