

Від пластикових карт

до розумної біометрії



Компанія «Конус» розробила систему управління відвідувачами «ЛОГІН», яка використовує біометричні технології і бере на себе чимало додаткових функцій безпеки.

Стандартна система контролю та управління доступом (СКД) вирішує базове завдання — пропускати чи не пропускати людину через турнікет. Вона фіксує події проходів, але не має функцій, необхідних для створення комплексної безпеки великого підприємства: документообігу бюро перепусток, управління життєвим циклом відвідувачів та підрядників, контролю автотранспорту, аналітики переміщень, інтеграції з корпоративними системами.

Ключові «болі» бізнесу:

- черги в бюро перепусток;
- високі витрати часу на обробку заявок на продовження перепусток;
- неможливість оперативно реагувати на події безпеки;
- відсутність єдиного чорного списку для всіх майданчиків підприємства;
- складність інтеграції з корпоративними системами (ERP, HR).

Система управління відвідувачами «ЛОГІН»

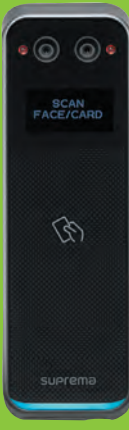
Для вирішення цих завдань замовників було розроблено систему управління відвідувачами (СУВ) «ЛОГІН», яка розширює ядро СКД бізнес-функціями, перетворюючи його на повноцінну платформу безпеки:

- визначає персон за обличчями, відбитками пальців, картками та QR;
- визначає автомобілі за номерами, картками, QR;
- виписує різні види перепусток з урахуванням внесення / винесення, ввезення / вивезення матеріальних засобів;
- автоматично обробляє заявки на введення даних в систему, продовження перепусток, внесення до чорного списку, блокування персон;
- веде журнали обробки та зміни персональних даних;
- веде звіти про час на території підприємства.

Біометричне обладнання

Для ідентифікації облич у СУВ використовуються рішення Suprema FaceStation F2, BioEntry W3 (табл. 1) та BioEntry W2 (табл. 2). Для контролю автотранспорту застосовуються ANPR-камери з автоматичним розпізнаванням номерних знаків.

Таблиця 1. Технічні характеристики Suprema BioEntry W3

	Опції RF (зчитувача)	125 kHz EM & 13.56 MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3, FeliCa • (для APB версії) + HID Prox&iCLASS SE/SR/Seos
	Мобільний доступ	NFC, BLE
	Процесор (CPU)	1.5 GHz Quad Core (4-ядерний)
	Пам'ять	16GB Flash + 2GB RAM
	Крипточип	Підтримується
	Тип РК-дисплея	1.3" PMOLED
	Роздільна здатність дисплея	800 x 1280 пікселів
	Робоча температура	-20°C ~ 50°C (-4°F ~ 122°F)
	Відстань розпізнавання	0.3m ~ 1.0m
	Швидкість зіставлення	19.7" ~ 51.2"
	Визначення живого обличчя	Менше 0.2 сек
	Захист від спуфінгу	Підтримується

Таблиця 2. Технічні характеристики Suprema BioEntry W2

	Опції RF (зчитувача)	125 kHz EM, HID Prox& 13.56 MHz MIFARE, MIFARE Plus, DESFire, DESFire EV1/EV2/EV3 (1), FeliCa
	Мобільна карта	NFC, BLE
	Біометрія	Відбиток пальця
	Тип сенсора	Оптичний сенсор (OP5)
	Процесор (CPU)	1.2 GHz Quad Core
	Пам'ять	2GB Flash + 256 MB RAM
	Макс. кількість користувачів	500,000(2)
	Макс. кількість шаблонів (1:N)	Відбитки пальців: 100,000
	Макс. кількість шаблонів (1:1)	Відбитки пальців: 500,000
	Макс. лог. текстових подій	1,000,000
	Протокол зв'язку	Сумісний з OSDP V2
	PoE	Сумісність з IEEE 802.3af
	Клас захисту корпусу	IP67
	Захист від ударів	IK09
	Датчик розкриття	Підтримується
	Робоча температура	-20°C ~ 50°C (-4°F ~ 122°F)
	Сертифікат	CE, UKCA, KC, FCC, IC, RCM, BIS, ANATEL, SIG, RoHS, REACH, WEEE, сертифікація ETL за стандартом UL 294

Ключові можливості СУВ

Автоматизація бюро перепусток. Система повністю оцифровує документообіг: заявки на перепустки, акти допуску, журнали реєстрації. Співробітнику бюро перепусток достатньо сфотографувати відвідувача та внести мінімум даних — система автоматично створює біометричний профіль та призначає права доступу.

Безконтактна ідентифікація. Розпізнавання облич працює в режимі «вільних рук»: співробітнику не потрібно прикладати картку або зупинятися біля турнікета. Система ідентифікує людину на ходу за 0,5–1 секунду. Це критично важливо для усунення черг у ранкові години.

Єдиний інформаційний простір. Всі дані про осіб, події доступу, транспорт зберігаються централізовано. Служба безпеки в реальному часі бачить, хто і де знаходиться на території, коли заїхав і виїхав. При роботі підрядника на декількох майданчиках холдингу його переміщення відстежуються наскрізним способом.

Єдиний чорний список. Блокування небажаних осіб працює на всіх майданчиках холдингу миттєво. Якщо людину внесено до чорного списку на одному підприємстві, вона автоматично не зможе потрапити на інші об'єкти.

Комплексна аналітика. Система формує звіти за такими показниками:

- час перебування на території для співробітників, підрядників, автотранспорту;
- порушення режиму доступу;
- активність поза зонами та об'єктами;
- робота обладнання та події в системі.

API для інтеграції. REST API дозволяє синхронізувати дані з корпоративними системами, що забезпечує:

- автоматичне завантаження оргструктури, посад, підрозділів з ERP;
- створення та оновлення профілів співробітників;
- блокування доступу при звільненні;
- передача даних про відсутності (відпустки, відрядження, лікарняні);
- вивантаження подій доступу для аналізу в BI-системах.

Якість управління:

- 100% прозорість переміщень людей та транспорту;
- консолідована звітність у реальному часі;
- можливість оперативного реагування на інциденти;
- єдиний чорний список на всіх майданчиках холдингу.

Безпека даних

Враховуючи, що система обробляє біометричні персональні дані, особливу увагу приділено захисту, який забезпечують:

- JWT-токени для автентифікації користувачів з обмеженим часом життя;
- шифрування біометричних шаблонів у базі даних та при передачі по мережі;

- повне логування всіх операцій з персональними даними із зазначенням: хто, коли і що змінив;
- рольова модель доступу — кожен користувач бачить лише ті дані, які необхідні для його роботи;
- відповідність GDPR — можливість видалення даних за запитом, прозорість обробки, мінімізація даних, що зберігаються.

Архітектура рішення

В основі системи лежить мікросервісна архітектура, реалізована на Spring Boot (backend) та Angular (frontend). Такий підхід забезпечує:

горизонтальне масштабування — при зростанні навантаження можна додавати нові екземпляри сервісів без зупинки системи. Критично важливо для підприємства, де в пікові години через КПП проходять тисячі людей;

відмовостійкість — вихід з ладу одного мікросервісу не впливає на роботу всієї системи. Наприклад, тимчасова недоступність сервісу звітності не блокує проходження людей через турнікети;

незалежне розгортання — оновлення окремих компонентів можна виконувати без зупинки всієї системи. Це дозволяє оперативно впроваджувати нові функції та виправляти помилки.

Багатошарова архітектура підтримує роботу з великими обсягами даних:

- рівень представлення (Angular SPA) — інтерфейси для бюро перепусток, служби безпеки, адміністраторів;
- API Gateway — єдина точка входу, маршрутизація запитів, JWT-автентифікація;
- бізнес-логіка (мікросервіси Spring Boot) — обробка подій доступу, управління персонами, формування звітів;
- рівень інтеграції — синхронізація з обладнанням Suprema, інтеграція з ERP через REST API;
- рівень даних — реляційна БД для структурованих даних, логування всіх операцій.

Технологічні переваги

Вибір мікросервісної архітектури виявився стратегічно вірним рішенням. Система легко масштабується під зростаючі потреби.

Обробка пікових навантажень — в ранкові години через КПП проходять до 2000 осіб за 30 хвилин. Мікросервіси автоматично масштабуються, забезпечуючи час відгуку API менше 200 мс.

Модульність — до базової платформи можна підключати нові функції без переробки ядра системи.

Технологічна незалежність — кожен мікросервіс може використовувати оптимальний для його завдань стек технологій. Це дозволяє застосовувати спеціалізовані рішення там, де вони дають максимальний ефект.

Перспективи розвитку

Система управління відвідувачами — не кінцева точка, а платформа для подальшого розвитку. На порядку денному:

- інтеграція з відеоспостереженням — автоматичне зв'язування подій доступу з відеопотоками для швидкого розслідування інцидентів;
- предиктивна аналітика — виявлення аномалій у поведінці (нетипова година приходу, відвідування незвичних зон);
- мобільний застосунок для співробітників — замовлення перепусток для гостей, перевірка своїх переміщень, QR-коди для разових відвідувань;
- IoT-інтеграція — підключення датчиків присутності для оптимізації використання переговорних кімнат та робочих просторів.

Висновки

Перехід від традиційних систем контролю доступу до сучасних біометричних рішень — це не просто заміна обладнання. Це комплексна трансформація процесів, культури безпеки та підходів до управління даними.

Ключові фактори успіху проєкту:

- правильний вибір обладнання — пристрої Suprema показали високу надійність та точність розпізнавання в реальних умовах експлуатації;
- масштабована архітектура — мікросервісний підхід дозволив впоратися з високими навантаженнями та забезпечити відмовостійкість;
- глибока інтеграція — зв'язок з корпоративними системами усунув дублювання даних та ручне введення;
- фокус на користувацькому досвіді — система проєктувалася з урахуванням реальних потреб бюро перепусток та служби безпеки.

Довіртеся професіоналам

Завдяки сучасним технологіям безпека стає не бар'єром, а зручним інструментом, що працює непомітно для працівників і ефективно для бізнесу. Саме цими принципами керуються у своїх проєктах співробітники **компанії «Конус»**.

Наші фахівці мають значний досвід розробки програмних продуктів: банківських систем, систем управління підприємством та корпоративних порталів. Компанія спеціалізується на створенні комплексних систем безпеки для великих промислових підприємств. Експертиза охоплює системи контролю доступу, відеоспостереження та інтеграцію протипожежних і охоронних систем. Усі рішення побудовані на сучасних технологічних стеках із акцентом на масштабованість, відмовостійкість і захист даних.



Андрій РОГОВ,
директор ПП «Конус»
andrey.rogov@gmail.com