



POLSKO-JAPOŃSKA AKADEMIA TECHNIK KOMPUTEROWYCH

Wydział Informatyki

Filia w Gdańsku

Bartosz Bohatyrewicz

Nr albumu s26860

Nazwa specjalizacji: Sztuczna Inteligencja

Łukasz Korycki

Nr albumu s26972

Nazwa specjalizacji: Cyberbezpieczeństwo

Kamil Maliński

Nr albumu s26984

Nazwa specjalizacji: Cyberbezpieczeństwo

Jan Szydłowski

Nr albumu s26978

Nazwa specjalizacji: Cyberbezpieczeństwo

Igor Wojciechowski

Nr albumu s27106

Nazwa specjalizacji: Aplikacje Internetowe

Wdrożenie systemu cyfrowych kluczy do budynku uczelni

Rodzaj pracy
inżynierska

Imię i nazwisko promotora
dr hab. Marek Bednarczyk

Gdańsk, Marzec, 2026

Streszczenie: Celem projektu inżynierskiego jest stworzenie modułu integrującego system zarządzania dostępem "Cyfrowe Klucze" z systemem uczelnianym PJATK. Moduł ten będzie odpowiedzialny za pobieranie danych z planu zajęć oraz wspomaganie zarządzania dostępem do pomieszczeń na podstawie tych danych. Projekt obejmuje również stworzenie aplikacji webowej dla administracji, dziekantu oraz ochrony, umożliwiającej łatwe zarządzanie uprawnieniami dostępu oraz generowanie raportów na podstawie danych z systemu "Cyfrowe Klucze". Ostatecznym celem jest zwiększenie efektywności zarządzania dostępem do pomieszczeń uczelnianych oraz poprawa bezpieczeństwa poprzez automatyzację procesu przydzielania uprawnień.

Słowa kluczowe: czytniki, systemy kontroli dostępu, bezpieczeństwo, karty [RFID](#), integracja systemów



POLSKO-JAPONSKA AKADEMIA TECHNIK KOMPUTEROWYCH

Karta projektu

Temat projektu: Wdrożenie systemu cyfrowych kluczy do budynku uczelni Temat projektu po angielsku: Implementation of a digital key system in a university building	Akronim: EkeyPJATK Data ustalenia tematu 2025-04-01
Promotor: dr hab. Marek Bednarczyk	Konsultanci: 1. Antoni Ulenberg
Cele projektu: Integracja oryginalnego systemu: "Cyfrowe Klucze" z systemem uczelnianym PJATK, wraz z ulepszeniem stworzonych wcześniej rozwiązań.	
Rezultaty projektu: Moduł pobierający i przekazujący dane z systemu uczelnianego PJATK do systemu "Cyfrowe Klucze", wraz z dokumentacją techniczną i użytkową. Aplikacja webowa dla administracji, dziekantu oraz ochrony. Przekazywanie danych z planu zajęć, wspomaganie zarządzania dostępem do pomieszczeń uczelnianych, dla systemu "Cyfrowe Klucze" na podstawie planu zajęć.	
Miary sukcesu: Integracja systemu "Cyfrowe Klucze" z systemem uczelnianym PJATK, umożliwiająca automatyczne zarządzanie dostępem do pomieszczeń na podstawie planu zajęć.	
Ograniczenia: Współpraca z istniejącym systemem uczelnianym PJATK. Wiele osób pośrednich wymaganych do realizacji projektu.	

Wykonawcy	Numer albumu	Specjalizacja	Tryb studiów
Bartosz Bohatyrewicz	s26860	Sztuczna Inteligencja	Stacjonarny
Łukasz Korycki	s26972	Cyberbezpieczeństwo	Stacjonarny
Kamil Maliński	s26984	Cyberbezpieczeństwo	Stacjonarny
Jan Szydłowski	s26978	Cyberbezpieczeństwo	Stacjonarny
Igor Wojciechowski	s27106	Aplikacje Internetowe	Stacjonarny

Data ukończenia projektu: 29 października 2025	Recenzent: —TBA—
--	----------------------------

Spis treści

1 Wstęp	4
2 Słownik pojęć	5
3 Opis problemu	7
3.1 Analiza stanu obecnego	7
3.1.1 Opis aktualnego procesu	7
3.1.2 Zidentyfikowane problemy	7
3.1.3 Analiza problemów	8
3.2 Analiza oryginalnego projektu "Cyfrowe Klucze"	8
3.3 Analiza konkurencji	8
3.3.1 Tritech	9
3.3.2 Logitech Tap Scheduler	10
3.3.3 Vidikom	11
3.4 Propozycja rozwiązania	12
4 Konteksty projektu	14
4.1 Kontekst systemowy	14
4.2 Kontekst biznesowy	14
4.3 Kontekst społeczny	14
4.3.1 Interesariusze i role	14
4.3.2 Zmiany i spodziewane skutki	14
4.3.3 Transparentność i komunikacja	15
4.3.4 Akceptacja społeczna i partycypacja użytkowników	15
4.3.5 Podstawowy scenariusz użycia systemu	15
4.3.6 Miernik wpływu społecznego	15
4.3.7 Ryzyka społeczne i środki zaradcze	15
4.4 Kontekst etyczny	16
4.4.1 Założenia i wartości	16
4.4.2 Prywatność i minimalizacja danych	16
4.4.3 Proporcjonalność i celowość	16

4.4.4	Sprawiedliwość i niedyskryminacja	16
4.4.5	Transparentność i rozliczalność	17
4.4.6	Bezpieczeństwo informacji	17
4.4.7	Dostępność i inkluzywność	17
4.4.8	Zarządzanie ryzykiem i nadzór etyczny	17
4.4.9	Metryki etyczne	17
4.4.10	Podsumowanie	18

Rozdział 1

Wstęp

Dokument opisuje stworzenie systemu weryfikacji uprawnień według rezerwacji z planu zajęć gotowego do wdrożenia. EkeyPJATK nie jest bezpośrednią kontynuacją projektu "Cyfrowe Klucze". System został zaprojektowany z myślą o bezpośredniej współpracy z działającym już systemem na terenie uczelni.

System EkeyPJATK jako uzupełnienie istniejącego już systemu wprowadza weryfikacje uprawnień według rezerwacji z planu zajęć. Ze względu na prototypowy charakter oryginalnego projektu, nasz zespół był również odpowiedzialny za odświeżenie paneli zarządzania dla Ochrony, Dziekanatu i Administracji oraz stworzenia nowej wersji modułu zamka.

Rozdział 2

Słownik pojęć

Pojęcia

API Interfejs programistyczny aplikacji; umożliwia komunikację pomiędzy modułem raportowym a panelami użytkowników oraz systemem kontroli dostępu.

AutoCAD Oprogramowanie do projektowania wspomaganego komputerowo (CAD) używane do tworzenia precyzyjnych rysunków technicznych i modeli 3D.

Cyfrowe Klucze System kontroli dostępu do sal na kampusie uniwersyteckim zbudowany przez zespół Antoniego Ulenberga, Marka Kudły i Kingi Marszałkowskiej.

Czytnik RFID Urządzenie służące do odczytu kart identyfikacyjnych na podstawie fal radiowych, wykorzystywane w systemie EkeyPJATK do kontroli dostępu.

EkeyPJATK System zarządzania dostępem oparty na cyfrowych kluczach, zintegrowany z systemem uczelnianym PJATK.

Elektrozwora Urządzenie służące do mechanicznego blokowania i odblokowywania drzwi w systemie kontroli dostępu.

GAKKO System zarządzania uczelnią, z którego pobierane są dane dotyczące planu zajęć i uprawnień dostępu.

Karta magnetyczna Nośnik identyfikacyjny wykorzystywany przez studentów, wykładowców i gości do autoryzacji dostępu do pomieszczeń uczelni.

Moduł zamka Element systemu kontroli dostępu odpowiedzialny za fizyczne od-blokowywanie drzwi na podstawie weryfikacji uprawnień.

PJATK Polsko-Japońska Akademia Technik Komputerowych.

REST API Interfejs programistyczny oparty na architekturze REST, umożliwia-jący komunikację między modułem integracyjnym a systemem GAKKO.

UI Interfejs użytkownika; graficzne środowisko umożliwiające interakcję z aplik-acją webową.

WebSocket Protokół komunikacyjny umożliwiający dwukierunkową komunikację w czasie rzeczywistym między klientem a serwerem.

Akronimy

AV/UC Audio Video / Unified Communications

BSS Baza Sprzętowo-Systemowa

CAD Computer-Aided Design

IT Information Technology

POE Power over Ethernet

RFID Radio-Frequency Identification

SIS System Informacji o Salach

Rozdział 3

Opis problemu

3.1 Analiza stanu obecnego

3.1.1 Opis aktualnego procesu

Aktualnie Gdańskie oddział PJATK powierza wydawanie odpowiednich kluczy do sal ochronie. Osoba chcącą uzyskać dostęp do danej sali musi najpierw zostać zweryfikowana przez Ochronę i wpisać się do dziennika na recepcji. Po zakończonej rezerwacji klucz należy zwrócić na recepcję.

Pracownicy uczelni, tacy jak wykładowcy, sprzątacze czy administracja budynku, również muszą każdorazowo pobierać klucze do sal. W praktyce oznacza to konieczność częstych wizyt na recepcji lub pobierania kilku kluczy jednocześnie.

3.1.2 Zidentyfikowane problemy

Obecny system generuje szereg trudności. Przede wszystkim proces wymiany kluczy jest uciążliwy, ponieważ każdorazowo wymaga udania się do Ochrony w celu pobrania lub zwrotu klucza. W efekcie dydaktycy, chcąc uproszczyć sobie pracę, często przekazują klucze między sobą bez wpisywania się do dziennika. Powoduje to rozbieżności między stanem faktycznym a zapisanym w dokumentacji.

Kolejnym problemem jest weryfikacja odbytych zajęć. Jeżeli prowadzący nie wpisał się do dziennika, Dziekanat musi kontaktować się z nim bezpośrednio, aby potwierdzić, czy zajęcia rzeczywiście się odbyły. Proces ten jest czasochłonny, nieefektywny i podatny na błędy.

Trudności napotykają również pracownicy techniczni, tacy jak sprzątacze czy administracja budynku. Każdorazowe pobieranie kluczy ogranicza ich elastyczność w

wykonywaniu obowiązków. Jeśli decydują się na pobranie wielu kluczy jednocześnie, rośnie ryzyko ich zgubienia, co dodatkowo komplikuje organizację pracy.

3.1.3 Analiza problemów

Analiza wskazuje, że obecny system oparty na fizycznych kluczach jest mało efektywny i generuje dodatkowe obciążenie organizacyjne. Brak pełnej kontroli nad obiegiem kluczy prowadzi do nieścisłości w dokumentacji i utrudnia rozliczanie odpowiedzialności za poszczególne sale. Proces weryfikacji zajęć jest podatny na błędy ludzkie i wymaga dodatkowych działań administracyjnych, co spowalnia pracę Dziekanatu. Ograniczona elastyczność pracowników technicznych wpływa negatywnie na sprawność obsługi budynku i może prowadzić do opóźnień w realizacji zadań.

3.2 Analiza oryginalnego projektu ”Cyfrowe Klucze”

Przez istniejące problemy aktualnego rozwiązania, zespół Antoniego Ulenberga, Marka Kudły i Kingi Marszałkowskiej zwanego ”Cyfrowe Klucze” zadecydował o stworzeniu prototypu systemu weryfikacji uprawnień przy pomocy czytników zamontowanych na ścianach przy salach oraz kart identyfikacyjnych. Po wielu konsultacjach z głównymi grupami użytkowników potencjalnego nowego systemu, zadecydowali o stworzeniu modularnego systemu.

System został podzielony na parę submodułów, system zarządzania dla administracji i ochrony, moduł sprzętowy, bazę danych, [API autoryzacji użytkowników](#) i [API GAKKO](#). Podczas ich pracy zadecydowali o porzuceniu planu z integracją z [GAKKO](#), na rzecz przedstawienia całokształtu prototypu ówego systemu.

3.3 Analiza konkurencji

Analizę konkurencji podzieliliśmy na dwie grupy. Grupa pierwsza to firmy skupiające się na zaprojektowaniu, wdrożeniu i integracji systemów typu rezerwacji sal konferencyjnych dla firm. Druga grupa, to firmy skupiające się na tworzeniu urządzeń, które są wykorzystywane w takich systemach.

3.3.1 Tritech

Opis

Firma Tritech New Technologies Sp. z o.o. z siedzibą w Warszawie działa na rynku od 2003 roku i specjalizuje się w projektowaniu oraz wdrażaniu systemów **AV/UC**, a także kompleksowych rozwiązań **IT**. Choć w swojej ofercie nie posiada bezpośrednio dedykowanego systemu kontroli dostępu do sal uczelnianych, jest otwarta na współpracę ze szkołami i uczelniami, dostosowując swoje rozwiązania do indywidualnych potrzeb klientów. Tritech kładzie duży nacisk na staranne przygotowanie projektów, wykorzystując narzędzia do modelowania 3D, takie jak **AutoCAD**, GstarCAD czy DraftSight. Na etapie projektowania tworzone są schematy blokowe, plany sieci, rozmieszczenie urządzeń oraz trasy kablowe. Firma prowadzi również konsultacje z klientem, architektem, inwestorem i integratorem, aby zapewnić spójność i funkcjonalność całego rozwiązania. W realizacjach wykorzystuje urządzenia renomowanych dostawców, takich jak Logitech, Cisco, Poly czy Yealink.

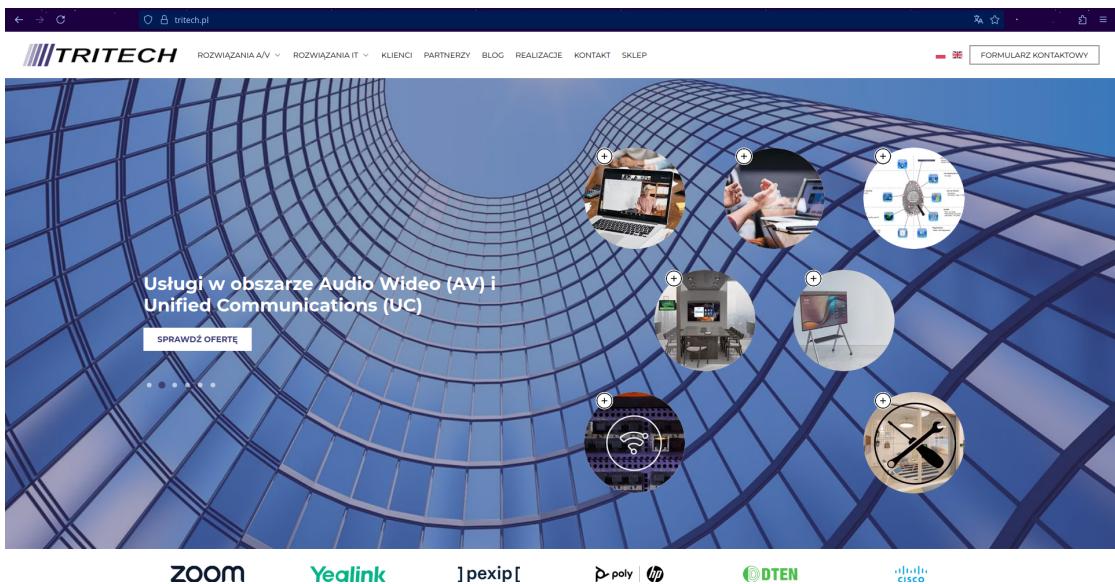
Zalety

Do głównych zalet oferty Tritech należy elastyczność i profesjonalizm w podejściu do klienta. Firma dostosowuje swoje projekty do budżetu oraz wymagań technicznych, co pozwala na tworzenie rozwiązań dopasowanych do specyfiki danej instytucji. Istotnym atutem jest również przygotowywanie pełnej dokumentacji projektowej w formacie **CAD**, co ułatwia późniejszą realizację i integrację systemów. Dzięki współpracy z wieloma dostawcami sprzętu Tritech może zaoferować szeroki wachlarz rozwiązań technologicznych, które odpowiadają różnym potrzebom klientów.

Wady

Do wad oferty Tritech można zaliczyć brak własnych, autorskich urządzeń, które mogłyby być w pełni dostosowane do indywidualnych wymagań klienta. Firma opiera się na sprzęcie dostarczanym przez zewnętrznych producentów, co oznacza, że rozwiązania te często bazują na zamkniętych systemach wymagających dodatkowych licencji lub subskrypcji. Może to generować dodatkowe koszty oraz ograniczać elastyczność wdrożenia w dłuższej perspektywie.

Źródło: <https://tritech.pl/> (Data ostatniego dostępu 29 października 2025)



Rysunek 3.1: Strona główna firmy Tritech.

3.3.2 Logitech Tap Scheduler

Opis

Firma Logitech, znana głównie z produkcji akcesoriów komputerowych, posiada w swojej ofercie również urządzenia do rezerwacji sal konferencyjnych. Jednym z nich jest **Logitech Tap Scheduler**, panel planistyczny montowany na ścianie, wyposażony w 10,1 calowy dotykowy wyświetlacz LCD. Urządzenie jest kompatybilne z wieloma systemami obsługi sal konferencyjnych, takimi jak Microsoft, Zoom, Robin czy też z autorskiego rozwiązania Logitech'a. Tap Scheduler został zaprojektowany z myślą o łatwej instalacji na szkle, futrynie lub ścianie, a kontrolki LED umożliwiają szybkie sprawdzenie statusu dostępności sali z daleka.

Urządzenie może być zarządzane z poziomu platformy **Logitech Sync**, która pozwala na monitorowanie stanu pomieszczeń, wdrażanie aktualizacji oraz konfigurację ustawień. Każdy produkt zakupiony od Logitech objęty jest 2-letnią gwarancją, z możliwością jej przedłużenia.

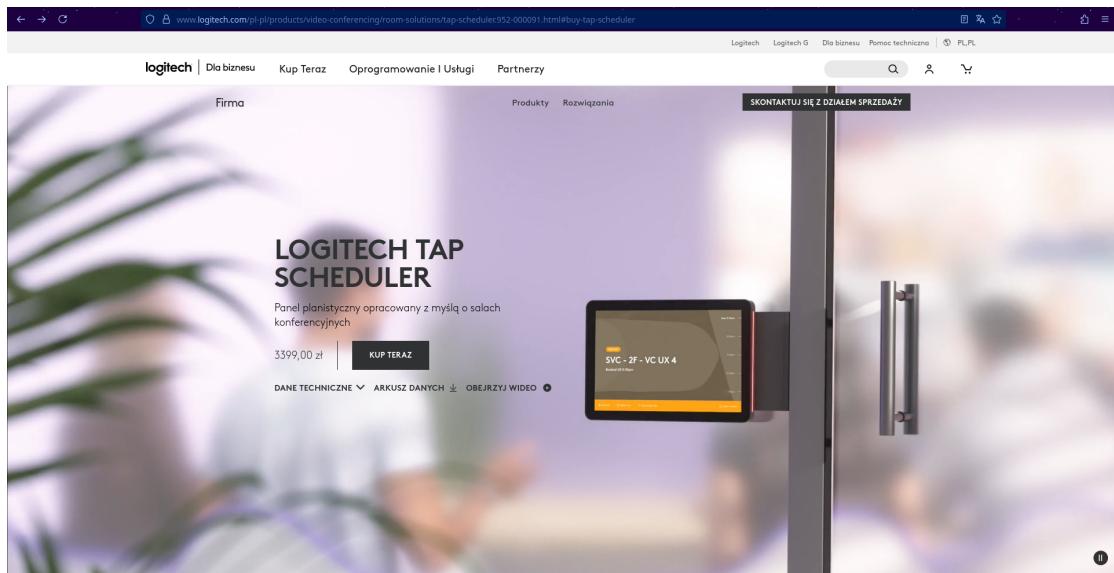
Zalety

Logitech Tap Scheduler wyposażony jest w czytelny ekran dotykowy o przekątnej 10,1 cala. Jest kompatybilny z popularnymi systemami rezerwacji sal, takimi jak Microsoft, Zoom czy Robin, co czyni go rozwiązaniem uniwersalnym. Dzięki kolorowym kontrolkom LED użytkownicy mogą z łatwością sprawdzić status dostępności sali nawet z większej odległości. Urządzenie oferuje elastyczne opcje montażu, może być instalowane na szkle, futrynie lub ścianie, a dodatkowe prowadnice w obudowie ułatwiają estetyczne poprowadzenie okablowania. Kolejną zaletą jest integracja z platformą Logitech Sync, która umożliwia centralne zarządzanie urządzeniami i ich konfiguracją. Standardowa 2-letnia gwarancja z możliwością przedłużenia zwiększa bezpieczeństwo inwestycji.

Wady

Do wad urządzenia należy brak natywnej funkcjonalności blokowania sal oraz brak integracji z systemami kontroli dostępu. Logitech Tap Scheduler nie daje również możliwości

przeprogramowania w ramach dostępnych systemów rezerwacyjnych, co ogranicza jego elastyczność. Cena jednostkowa wynosząca 3399,00 PLN nie obejmuje kosztów dodatkowych licencji ani subskrypcji Logitech Sync, które są wymagane do pełnego wykorzystania możliwości systemu. Dodatkowo, bardziej zaawansowane funkcje analizy i monitorowania w Logitech Sync są dostępne wyłącznie w droższych planach subskrypcyjnych, co może zwiększać całkowity koszt.



Rysunek 3.2: Logitech Tap Scheduler.

Źródło: <https://www.logitech.com/pl-pl/>
(Data ostatniego dostępu 29 października 2025)

3.3.3 Vidikom

Opis

System Informacji o Salach (SIS) (SIS) firmy Vidikom jest rozwiązaniem dedykowanym dla dużych organizacji, takich jak uczelnie, hotele, centra konferencyjne czy urzędy. Vidikom specjalizuje się w kompleksowym wyposażeniu sal konferencyjnych w sprzęt audio-wizualny, oferując również jego instalację i konfigurację. SIS jest autorskim produktem firmy, co umożliwia jego szeroką adaptację zarówno pod względem funkcjonalnym, jak i graficznym.

System oparty jest na tabletach z systemem Android o rozmiarze ekranu zaczynającym się od 10,1 cala, wyposażonych w wyświetlacz IPS o jasności 500 nit, paski LED sygnalizujące stan zajętości sali, zasilanie POE oraz mocowanie VESA. Panel sterowania dostępny z poziomu sieci LAN umożliwia zarządzanie rezerwacjami, konfigurację sal oraz kontrolę dostępu. SIS wspiera integrację z popularnymi kalendarzami takimi jak Google Calendar, Outlook Exchange, Lotus Domino oraz może być połączony z zewnętrznymi niezabezpieczonymi bazami danych.

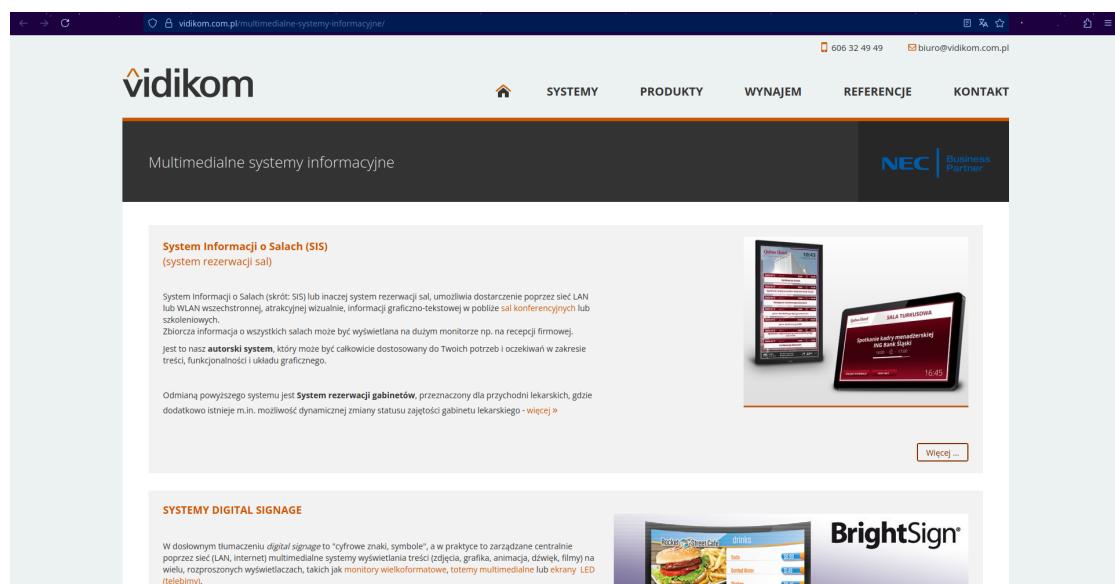
Zalety

System SIS charakteryzuje się otwartą strukturą, co pozwala na szeroką personalizację zarówno funkcji, jak i wyglądu interfejsu użytkownika. Urządzenia wykorzystywane w

systemie są wyposażone w jasne ekrany IPS oraz paski LED, które umożliwiają szybką identyfikację stanu zajętości sali. Zastosowanie zasilania **POE** upraszcza instalację i ogranicza liczbę przewodów. Panel sterowania dostępny przez sieć LAN jest intuicyjny i umożliwia kompleksowe zarządzanie salami, użytkownikami oraz rezerwacjami. System oferuje również możliwość integracji z popularnymi kalendarzami oraz z zewnętrznymi bazami danych, co usprawnia proces rezerwacji i synchronizacji informacji.

Wady

System **SIS** nie posiada natywnego wsparcia dla szyfrowanego dostępu do zewnętrznych baz danych, co może stanowić ograniczenie w kontekście bezpieczeństwa informacji. Główna funkcjonalność systemu koncentruje się na zarządzaniu rezerwacjami i prezentacji informacji, natomiast nie oferuje dedykowanego mechanizmu fizycznej kontroli dostępu, takiego jak identyfikacja użytkowników za pomocą kart **RFID**. Zarządzanie użytkownikami oraz salami odbywa się ręcznie poprzez panel LAN, co może być czasochłonne w przypadku dużych instytucji. Ponadto, zależność od sprzętu z systemem Android może ograniczać elastyczność wdrożenia w środowiskach o innych wymaganiach technicznych lub preferencjach sprzętowych.



Rysunek 3.3: Vidikom System Informacji o Salach

Źródło: <https://vidikom.com.pl/multimedialne-systemy-informacyjne/>
(Data ostatniego dostępu 29 października 2025)

3.4 Propozycja rozwiązania

Proponowane rozwiązanie systemu **EkeyPJATK** różni się od konkurencji poprzez integrację z istniejącym systemem odpowiedzialnym za plan zajęć w uczelni **PJATK**, co umożliwia automatyczne zarządzanie dostępem do pomieszczeń na podstawie harmonogramu. W przeciwieństwie do standardowych rozwiązań oferowanych przez firmy takie jak Tritech czy Logitech, które często opierają się na stałych uprawnieniach dostępu i wymagają ręcznego zarządzania, **EkeyPJATK** automatyzuje ten proces, co zwiększa efektywność i bezpieczeństwo.

Dodatkowo, nasz system oferuje dedykowaną aplikację webową dziekanatu oraz panel ochrony, co pozwala na łatwe zarządzanie uprawnieniami dostępu oraz generowanie raportów na podstawie danych i logów z systemu. Ta funkcjonalność nie jest standardowo dostępna w rozwiązaniach konkurencji i stanowi istotną wartość dodaną dla użytkowników. Oba te panele zostały zaprojektowane z myślą o intuicyjności i łatwości obsługi, współpracując blisko z pracownikami uczelni, aby spełnić ich wymagania i ułatwić pracę.

Dużą zaletą naszego rozwiązania jest duży nacisk na kosz wdrożenia i utrzymania systemu. W przeciwieństwie do komercyjnych ofert, które często wiążą się z wysokimi kosztami licencji i subskrypcji, nasz system zaprojektowany został przez grupę studentów, co pozwala zmniejszyć koszty prototypowania i wdrożenia w porównaniu do komercyjnych ofert.

Rozdział 4

Konteksty projektu

4.1 Kontekst systemowy

4.2 Kontekst biznesowy

4.3 Kontekst społeczny

4.3.1 Interesariusze i role

System [EkeyPJATK](#) będzie miał wpływ na wiele grup: studentów, wykładowców, pracowników administracyjnych, ochronę oraz dział IT uczelni. Wszyscy oni mają odmienne potrzeby i oczekiwania wobec systemu.

- **Wykładowcy:** dostęp do sal zgodnie z harmonogramem, szybka weryfikacja przy czytniku, obsługa wyjątków (zastępstwa). [API](#) decyduje o dostępie, a wejścia są logowane. :contentReference[oaicite:0]index=0
- **Studenci:** wgląd w plan sal, komunikaty o prowadzących i godzinach, brak uprawnień do zamków. :contentReference[oaicite:1]index=1
- **Dziekanat/Administracja:** masowe operacje na uprawnieniach, raporty z dostępów, wsparcie rozliczeń dydaktycznych. :contentReference[oaicite:2]index=2
- **Ochrona:** zdalne otwieranie drzwi, reagowanie na incydenty, przegląd logów w panelu operacyjnym. :contentReference[oaicite:3]index=3
- **BSS:** utrzymanie, integracja z GAKKO, bezpieczeństwo i audyt. :contentReference[oaicite:4]index=4
- **Personel techniczny i sprzątający oraz goście:** elastyczny dostęp czasowy i ewidencja wizyt. :contentReference[oaicite:5]index=5

4.3.2 Zmiany i spodziewane skutki

Wdrożenie systemu [EkeyPJATK](#) przyniesie szereg zmian w codziennych operacjach uczelni. Przede wszystkim, automatyzacja zarządzania dostępem do sal na podstawie planu zajęć zredukuje potrzebę ręcznego rozdawania kluczy przez ochronę.

Dla wykładowców i studentów, system zapewni płynniejszy dostęp do sal, eliminując konieczność fizycznego pobierania kluczy. To zwiększy efektywność korzystania z budynku i poprawi doświadczenie użytkowników. Dziekanat zyska narzędzia do lepszego monitorowania wykorzystania sal oraz generowania raportów, co ułatwi planowanie zasobów i administrację.

Ochrona będzie miała możliwość zdalnego zarządzania dostępem do pomieszczeń, co zwiększy ich zdolność do reagowania na incydenty i poprawi ogólne bezpieczeństwo kampusu. Administracja/ [Baza Sprzętowo-Systemowa \(BSS\)](#) będzie odpowiedzialny za utrzymanie systemu, jego integrację z istniejącymi rozwiązaniami oraz zapewnienie bezpieczeństwa danych, co może wymagać dodatkowych zasobów i szkoleń dla pracowników mających bezpośredni kontakt z [EkeyPJATK](#).

Potencjalne wyzwania mogą obejmować konieczność adaptacji użytkowników do nowego systemu oraz zarządzanie wyjątkami, takimi jak nagłe zmiany w planie zajęć czy sytuacje awaryjne. Ważne będzie zapewnienie odpowiedniego wsparcia technicznego i komunikacji, aby ułatwić przejście na nowe rozwiązanie i maksymalizować jego korzyści dla całej społeczności uczelni.

4.3.3 Transparentność i komunikacja

Niezbędne będzie zapewnienie transparentnej komunikacji z wszystkimi interesariuszami na temat zmian wprowadzanych przez system [EkeyPJATK](#), a także danych gromadzonych i wykorzystywanych przez system. Korzystne może być stworzenie oficjalnej polityki prywatności i bezpieczeństwa danych, która jasno określi, jakie informacje są zbierane, w jakim celu oraz jak są chronione i rozprowadzenie jej wśród użytkowników.

4.3.4 Akceptacja społeczna i partycypacja użytkowników

Aby zapewnić akceptację społeczną dla systemu [EkeyPJATK](#), ważne będzie zaangażowanie użytkowników końcowych w proces projektowania i wdrażania systemu. Dlatego podczas procesu tworzenia systemu, odbywały się konsultacje z różnymi grupami użytkowników, aby zrozumieć ich potrzeby i oczekiwania.

4.3.5 Podstawowy scenariusz użycia systemu

- dodać scenariusze z swojego screeny lub cytaty

4.3.6 Miernik wpływu społecznego

Skuteczność rozwiązania ocenia się przede wszystkim poprzez spadek incydentów związanych z fizycznymi kluczami oraz redukcję interwencji ochrony przy otwarciach awaryjnych. Istotne są także oszczędności czasu użytkowników w porównaniu do poprzedniego systemu.

4.3.7 Ryzyka społeczne i środki zaradcze

Główne ryzyka dotyczą prywatności, wstępnej niechęci użytkowników i możliwości nadużyć administracyjnych. Minimalizuje się je przez projektowanie z poszanowaniem prywatności (ograniczony zakres danych, jasno zdefiniowana retencja, kontrola dostępu do logów), zapewnienie trybów pracy awaryjnej (cache reguł na urządzeniach, procedury

ręczne i wsparcie ochrony) oraz rozdział ról i uprawnień z audytem działań administracyjnych. Kluczowe jest również stałe informowanie społeczności uczelni o zasadach działania systemu i ścieżkach zgłaszania uwag.

4.4 Kontekst etyczny

4.4.1 Założenia i wartości

Projekt opiera się na zasadach: poszanowania prywatności, proporcjonalności środków względem celu, transparentności działania, sprawiedliwego traktowania użytkowników. Celem jest zwiększenie bezpieczeństwa i efektywności, bez nadmiernej ingerencji w autonomię społeczności akademickiej.

4.4.2 Prywatność i minimalizacja danych

System przetwarza dane identyfikacyjne oraz logi czasu wejścia. Zgodnie z zasadą minimalizacji przechowywane są wyłącznie informacje niezbędne do realizacji celu (weryfikacja dostępu, rozliczalność zajęć). Zalecenia:

- ograniczenie zakresu pól w logach (ID karty/rola, sala, timestamp, wynik decyzji),
- domyślna retencja krótka (np. 6–12 miesięcy) oraz anonimizacja po terminie,
- dostęp do logów wyłącznie dla ról uprawnionych, z rejestrowaniem wglądów,
- prawo użytkownika do informacji o przetwarzaniu i wgląd we własne dane.

4.4.3 Proporcjonalność i celowość

Automatyzacja dostępu jest środkiem proporcjonalnym do celu organizacyjnego i bezpieczeństwa tylko wtedy, gdy:

- zakres monitorowania odpowiada planowi zajęć i nie wykracza na sfery prywatne,
- decyzje o dostępie są związane z harmonogramem i uprawnieniami, a nie preferencjami administracyjnymi,
- istnieje tryb wyjątków (zastępstwa, goście) z kontrolowanym, krótkim czasem obowiązywania.

4.4.4 Sprawiedliwość i niedyskryminacja

Mechanizmy podejmowania decyzji nie mogą faworyzować grup użytkowników. Wymagane są:

- spójne reguły nadawania i odwoływania uprawnień oparte na rolach i planie,
- audyt reguł cyklicznie (np. semestralnie) pod kątem uprzedzeń i wykluczeń,
- mechanizmy odwoławcze i ścieżka zgłoszeń dla użytkowników.

4.4.5 Transparentność i rozliczalność

Użytkownicy powinni rozumieć działanie systemu i swoje prawa. Zalecane:

- publiczna polityka prywatności, regulamin działania i FAQ,
- oznaczenia przy drzwiach informujące o kontroli dostępu i logowaniu zdarzeń,
- dzienniki administracyjne (kto, kiedy, jakie reguły zmienił) oraz okresowe raporty z audytów.

4.4.6 Bezpieczeństwo informacji

Ochrona danych jest warunkiem etycznego przetwarzania. Wymagane:

- szyfrowanie w danych, kopie zapasowe,
- kontrola dostępu oparta na rolach, zasada najmniejszych uprawnień,
- testy bezpieczeństwa (przeglądy konfiguracji, testy penetracyjne) i plan reagowania na incydenty.

4.4.7 Dostępność i inkluzywność

System nie może utrudniać korzystania z infrastruktury osobom z niepełnosprawnościami lub gościom. Należy zapewnić:

- alternatywne kanały dostępu (asysta ochrony, kody tymczasowe),
- czytelne komunikaty i interfejsy, ergonomiczne rozmieszczenie czytników,
- procedury na wypadek awarii (tryb degradacji, ręczne otwarcia z rejestrów decyzyjnych).

4.4.8 Zarządzanie ryzykiem i nadzór etyczny

Aby ograniczać ryzyka nadużyć i „pełzającego” rozszerzania celu:

- realizować okresową ocenę skutków dla ochrony danych i etyki,
- wprowadzić komitet nadzoru (przedstawiciele dziekanatu, IT, ochrony, studentów),
- utrzymywać rejestr zmian celu przetwarzania i zakresu danych oraz wymagać zgody interesariuszy na istotne rozszerzenia.

4.4.9 Metryki etyczne

Proponowane wskaźniki:

- odsetek wniosków o wgląd w dane zrealizowanych w terminie,
- liczba incydentów dostępowych i czas ich obsługi,
- czas retencji porównany z oficjalną polityką,
- liczba i wynik audytów (niezgodności, rekomendacje i ich wdrożenie).

4.4.10 Podsumowanie

Etyczne wdrożenie wymaga równowagi między bezpieczeństwem, efektywnością i prawami użytkowników. Kluczowe są: minimalizacja ilości zbieranych danych, przejrzystość, proporcjonalność i ciągły nadzór. Dzięki tym zasadom system może realizować cele uczelni bez naruszania zaufania użytkowników.