

Spis treści

1. Wstęp	6
2. Monitorowanie sygnałów biometrycznych w kontroli użytkowników systemów komputerowych	11
2.1. Problematyka wykorzystania interfejsów człowiek - maszyna	12
2.2. Interfejsy komunikowania się człowieka z komputerem	13
2.3. Biometryczne metody pomocne w realizacji interfejsów człowiek - komputer	15
2.3.1. Elektroencefalografia (EEG)	15
2.3.2. Elektromiografia EMG	20
2.3.3. Okulografia	23
2.3.4. Interpretacja sygnałów bioelektrycznych	25
2.4. Przykłady dostępnych interfejsów człowiek - maszyna zbudowanych na bazie metod biometrycznych	27
2.4.1. Urządzenie Emotiv	29
2.4.2. OCZ - The Neural Impulse Actuator	36
2.4.3. Neuro Sky	37
2.4.4. Interfejsy mózg - komputer firmy g.tec	39
2.4.5. Otwarty modułowy system EEG	41
3. Geolokalizacja użytkowników systemów komputerowych	43
3.1. Metody detekcji geolokalizacji użytkowników systemów komputerowych	44
3.1.1. Geolokalizacja na podstawie dedykowanych urządzeń	45
3.1.2. System geolokalizacji działający w oparciu o sieci bezprzewodowe standardu 802.11	47
3.1.3. Geolokalizacja za pomocą publicznych adresów IP	49
3.2. Interfejs dostępu do danych o geolokalizacji użytkownika	51
3.2.1. Detekcja informacji geolokalizacyjnych za pomocą apletów języka Java	52
3.2.2. Odczyt informacji geolokalizacyjnej w systemie operacyjnym Android	55
3.2.3. Wizualizacja danych związanych z geolokalizacją użytkowników	68
3.2.4. Usługi geolokalizacji w systemach operacyjnych Microsoft Windows	74
3.3. Architektura systemu lokalizacji użytkowników przy użyciu sieci bezprzewodowych	76
4. Określanie tożsamości użytkowników systemów komputerowych	84

4.1. Metody stosowane do uwierzytelniania użytkowników systemów komputerowych	85
4.2. Protokół OpenID	88
4.2.1. Rozszerzenia protokołu OpenID	90
4.2.2. Sprzętowe metody potwierdzania tożsamości użytkowników	93
4.3. Uwierzytelnianie użytkowników portali webowych z użyciem protokołu OpenID	96
4.4. Usługi potwierdzania tożsamości wspierane przez dostawców usług IT	99
4.4.1. Uwierzytelnianie poprzez usługę udostępniana poprzez serwis Facebook	100
4.4.2. Windows Live ID (Microsoft Account)	101
4.4.3. Implementacja standardu OpenID stosowana przez serwis Yahoo	102
4.4.4. Usługa uwierzytelniania firmy Google	104
4.4.5. Profil zaufany i platforma ePuap	105
5. Monitorowanie dostępu użytkowników do zasobów rzeczowych za pomocą technik znacznikowania	107
5.1. Systemy znakowania rzeczy oparte o reprezentacje graficzną	109
5.2. Systemy znakowania produktów działające w oparciu o fale radiowe	113
5.3. Obsługa znaczników za pomocą urządzeń mobilnych na przykładzie standardu NFC	116
6. Wpływ aktywności użytkowników na ciągłość działania systemów komputerowych	122
6.1 Wykrywanie potencjalnie niebezpiecznych zdarzeń dla ciągłości działania systemu komputerowego	124
6.2. Analiza wykorzystania zasobów systemu komputerowego przez użytkowników	126
6.2.1. Monitorowanie stanu systemu komputerowego za pomocą usług instrumentacji i zarządzania systemu operacyjnego Windows	127
7. Monitorowanie dzienników systemu operacyjnego w celu wykrywania zdarzeń generowanych przez użytkownika	130
8. Podsumowanie	134
9. Załączniki	135
10. Literatura	140
11. Streszczenie	143