Streszczenie

W niniejszej rozprawie dokonano analizy istniejących sposobów potwierdzania tożsamości użytkowników z uwzględnieniem rozwiązań opublikowanych w literaturze oraz używanych komercyjnie. Wykazała ona brak kompleksowego podejścia, uwzględniającego zarówno wygodę użytkowników końcowych jak i bezpieczeństwo samego procesu uwierzytelniania, w związku z czym zaprojektowano oraz wykonano całościowy system uwierzytelniający.

Opracowany przez autora rozprawy system, służący potwierdzaniu tożsamości, wykorzystuje niezależne metody uwierzytelniania z obszarów wiedzy, posiadania, cech oraz zachowania użytkownika końcowego. W pracy przedstawiono i wykorzystano także nowe, zaprojektowane przez autora metody oparte na biometrii (analiza składu ciała oraz mierzenie czasu pomiędzy metodami). Praca prezentuje także pierwszy opublikowany w literaturze przykład użycia algorytmów sztucznej inteligencji do podejmowania decyzji o poprawnym uwierzytelnianiu użytkownika końcowego na podstawie wielu różnych metod.

Ponadto zaprojektowano i zrealizowano badania zaimplementowanego systemu z uwzględnieniem znanych metryk mierzenia systemów i metod uwierzytelniania. Wykonano zarówno eksperymenty dla zgodnego z założeniami użycia systemu weryfikując jego skuteczność, jak i zasymulowano różne scenariusze i przypadki innego użycia z uwzględnieniem próby oszukania takiego systemu.

Zbadane rozwiązanie, skupione zarówno na wygodzie użytkowników jak i bezpieczeństwie i ochronie danych, wykazało 100% skuteczność w poprawnym uwierzytelnianiu użytkownika. Uzyskane wyniki pozwalają na kontynuację badań w wielu kierunkach oraz efektywne wykorzystanie takiego systemu komercyjnie.

Słowa kluczowe: uwierzytelnianie użytkownika, uczenie maszynowe, cyberbezpieczeństwo