ISSN 2300-5149

PRZEGLĄD TELEINFORMATYCZNY

TOM 8 (26) **Nr 1-4 (50)**
WARSZAWA **2020**

PRZEGLĄD TELEINFORMATYCZNY
TELEINFORMATICS REVIEW

Dawniej: BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI WAT
(ISSN 1427-3578)
Ukazuje się od 1995 r.

ADRES REDAKCJI
Redakcja Przeglądu Teleinformatycznego
00-908 Warszawa, ul. gen. Sylwestra Kaliskiego 2
tel. 261 83 87 03, fax. 261 83 71 44
e-mail: pt [at] ita.wat.edu.pl

WWW: **http://przeglad.ita.wat.edu.pl/**
https://przegladteleinformatyczny.publisherspanel.com/

Wersją pierwotną czasopisma jest wersja elektroniczna

REDAKTOR NACZELNY:
Antoni Donigiewicz

REDAKTOR WYDANIA
Antoni Donigiewicz

OPRACOWANIE STYLISTYCZNE
Renata Borkowska

PROJEKT OKŁADKI
Barbara Chruszczyk

WYDAWCA: Instytut Teleinformatyki i Cyberbezpieczeństwa WAT

ISSN 2300-5149
ISSN 2353-9836 (on-line)

Ochrona informacji sterującej w sieciach i systemach przemysłowych – propozycja podstaw edukacyjnych

Krzysztof LIDERMAN

Instytut Teleinformatyki i Cyberbezpieczeństwa, Wydział Cybernetyki, WAT
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
krzysztof.liderman@wat.edu.pl

STRESZCZENIE: W artykule przedstawiono problematykę nauczania zagadnień bezpieczeństwa dla przemysłowych systemów sterowania. Po zwięzłym scharakteryzowaniu we wstępie sieci i systemów przemysłowych, w kolejnych punktach krótko opisano podstawowe dla tego obszaru problemowego normy i standardy (IEC 62443 oraz *CIS Critical Security Controls for Effective Cyber Defense*), framework MITRE ATT&CK oraz zbiór „dobrych praktyk" opublikowany przez *Bundesamt für Sichercheit in der Informationstechnik*.

SŁOWA KLUCZOWE: przemysłowe systemy sterowania, IEC 62443, CAG/CIS, MITRE ATT&CK, „dobre praktyki" dla przemysłowych systemów sterowania

1. Wstęp

Eksploatowane we współczesnych organizacjach i – ujmując problem szerzej – infrastrukturze państwowej systemy: transportowe, komunikacyjne, magazynowe i produkcyjne, muszą być *nadzorowane* oraz w części przypadków, dotyczy to głównie systemów produkcji, *sterowane*. Zadania te są realizowane za pomocą przemysłowych systemów sterowania, na które składają się m.in. sieci SCADA (ang. *Supervisory Control And Data Acquisition*), DCS (ang. *Distributed Control Systems*) oraz ich elementy składowe w postaci sterowników programowalnych PLC (ang. *Programmable Logic Controllers*) [5].

Przemysłowe systemy sterowania (ang. *Industrial Control System* – ICS)[1] rozwijały się w zasadzie oddzielnie od teleinformatycznych (biurowych) sieci komputerowych. To oddzielenie, brak połączeń pomiędzy różnymi ICS, stosowanie specjalizowanego sprzętu i protokołów, wydzielonych kanałów komunikacyjnych oraz zwykle dobra ochrona fizyczna centrów sterowania powodowały, że problemy nękające biurowe sieci informatyczne związane z działaniami różnego rodzaju intruzów, możliwościami propagacji niekorzystnych efektów pomiędzy różnymi, połączonymi sieciami, podatność na ataki typu Denial of Services itp. nie dotyczyły praktycznie sieci przemysłowych.

Jednak od lat 90. XX wieku zaczął się zarysowywać trend[2] łączenia wydzielonych dotąd ICS z sieciami biurowymi oraz stosowanie do ICS rozwiązań z „klasycznych" sieci biurowych (komercyjnych systemów operacyjnych i sprzętu komputerowego) oraz wykorzystanie Internetu (protokołu IP) jako medium komunikacyjnego. Wymienione fakty złożyły się na nowy jakościowo obraz współczesnych sieci przemysłowych – pojawiły się w nich nowe problemy z zapewnianiem bezpieczeństwa o tym, że są to zagadnienia istotne dla żywotnych interesów nie tylko poszczególnych firm czy organizacji, ale także państwa, świadczą już wczesne publikacje o tej tematyce i podejmowane działania:

– opublikowane po raz pierwszy we wrześniu 2007 roku rekomendacje NIST (*National Institute of Standards and Technology*) [30],
– przyjęcie przez NERC (*North American Electric Reliability Corporation*) w 2008 roku ośmiu standardów z zakresu „cybersecurity" i ochrony infrastruktury krytycznej (patrz też rozdział 4.3 oraz przypisy dolne z linkami w tym rozdziale) oraz opracowanie [29] listy dziesięciu najgroźniejszych podatności dla ICS wraz ze wskazaniem sposobów ich minimalizacji;
– powołanie w USA, w ramach U.S. Department of Homeland Security, przemysłowego zespołu reagowania (ICS-CERT − *Industrial Control Systems Cyber Emergency Response Team*)[3]. Obecnie na swoich stronach internetowych[4] ICS-CERT prezentuje nie tylko specyfikacje aktualnych

[1] W literaturze anglojęzycznej jest też często używane określenie *Operational Technology* (OT).

[2] Głównie pod wpływem czynników ekonomicznych i nowych koncepcji zarządzania biznesem, w których kadra zarządzająca w celu podwyższenia efektywności i konkurencyjności swoich organizacji korzysta z danych na temat produkcji dostępnych w systemach automatyki.

[3] https://www.us-cert.gov/control_systems/ics-cert/

[4] https://www.us-cert.gov/ics/Recommended-Practices

zagrożeń i podatności wykrytych w systemach przemysłowych, ale także obszernie opisane zalecane praktyki zabezpieczania takich systemów [34].

Najnowsze dane statystyczne pokazują[5], że sieci przemysłowe i przemysłowe systemy sterowania w szczególności mogą być stosunkowo łatwym celem dla intruzów, ponieważ:

- 40% instalacji przemysłowych ma co najmniej jedno bezpośrednie połączenie z Internetem;
- w 53% instalacji przemysłowych używa się przestarzałych systemów Windows, takich jak Windows XP;
- w 69% instalacji przemysłowych używa się nieszyfrowanych haseł do dostępu do ICS;
- 57% instalacji przemysłowych nie ma zainstalowanego oprogramowania antywirusowego z funkcją automatycznej aktualizacji baz sygnatur;
- 16% instalacji przemysłowych ma co najmniej jeden bezprzewodowy punkt dostępowy;
- 84% instalacji przemysłowych ma co najmniej jedno urządzenie z dostępem zdalnym.

W specyfikacjach systemów sterowania używane są często określenia: „czasu rzeczywistego" (ang. *real-time systems*) oraz „systemy wbudowane" (ang. *embedded systems*), wskazujące dokładniej typ systemu sterowania [10], [11]. Zgodnie z definicją IEEE/ANSI Std 729: „ (…) *komputerowym systemem czasu rzeczywistego nazywamy system komputerowy, w którym obliczenia są wykonywane współbieżnie z procesem zewnętrznym (otoczenia) w celu sterowania, nadzorowania lub terminowego reagowania na zdarzenia występujące w tym procesie (otoczeniu)*". Jeżeli oprogramowanie systemu sterowania jest zapisane w pamięci stałej stanowiącej część urządzenia sterującego (tzn. jego zmiana wiąże się z wymianą bądź przeprogramowaniem pamięci PROM), to o takim systemie sterowania mówi się, że jest „wbudowany"[6].

Współczesne środowisko ICS może mieć wbudowanych wiele urządzeń połączonych poprzez protokół IP. Tym urządzeniom brakuje zwykle mocy obliczeniowej do obsługi zabezpieczeń użytkowanych w tradycyjnych systemach informacyjnych. Poza tym używa się w nich specjalizowanego firmware, systemów operacyjnych czasu rzeczywistego oraz firmowych

[5] Patrz np. raport firmy CyberX za rok 2019 dostępny pod: https://cyberx-labs.com/resources/risk-report-2019/ (dostęp 22.05.2020). Dane opracowano na podstawie badania ponad 850 podmiotów z całego świata.

[6] W przypadku instalacji systemów wbudowanych na platformach pływających, latających lub jeżdżących używa się często określenia „systemy pokładowe".

(prawnie zastrzeżonych) protokołów, takich jak Profibus, COTP, TPKT Modbus, czy EtherNet/IP. W odróżnieniu od systemów informacyjnych, pierwszoplanowym zadaniem z zakresu bezpieczeństwa dla systemu składającego się z takich urządzeń jest utrzymanie jego integralności i dostępności, a nie zapewnienie ochrony danych i prywatności.

Zagadnienia bezpieczeństwa ICS związane z przesyłaniem sygnałów sterujących i danych produkcyjnych, w zasadzie od początku ich zaistnienia, są dowiązywane do problemów bezpieczeństwa infrastruktury krytycznej[7], a ostatnio także do modnej tematyki łańcucha dostaw [15]. Ma to odzwierciedlenie w tworzonych rozwiązaniach prawnych, publikacjach naukowych, szkoleniach itp. Przykład takiego podejścia daje chociażby ENISA (*European Union Agency for Network and Information Security*). ENISA w 2014 roku ustanowiła grupę zainteresowanych stron dla problematyki sieci przemysłowych (*ICS Stakeholder Group*). Jej celem jest dostarczenie użytkownikom i ekspertom od ICS/SCADA platformy wymiany poglądów oraz możliwości opracowywania i rozpowszechniania nowych idei podnoszących poziom bezpieczeństwa przemysłowego w UE[8]. Przykłady takich opracowań eksperckich to [13] i [14]. Pierwsze z nich dotyczy wyzwań i rekomendacji związanych z Industry 4.0 Cybersecurity. Drugie z kolei, oprócz przeglądu publikacji i przedsięwzięć ENISY (do roku 2015) w dziedzinie ICS, zawiera wyniki oceny[9] ośmiu krajów UE (w tym Polski) pod względem dojrzałości wdrożonych w infrastrukturze krytycznej państwa rozwiązań z zakresu bezpieczeństwa przemysłowego.

Wzmiankowane powyżej zagadnienia były także przedmiotem zainteresowania już przed ponad dwunastoma latami w ówczesnym Instytucie Automatyki i Robotyki[10] Wydziału Cybernetyki WAT (patrz np. [6]-[9]). Można zatem powiedzieć, że niniejszy artykuł jest powrotem po długiej przerwie do analizowanych kiedyś zagadnień, przy czym powrót ten wiąże się m.in. z przeświadczeniem autora, że opisywane tu zagadnienia powinny zostać włączone do procesu dydaktycznego w obszerniejszym niż dotąd zakresie, szczególnie na takich specjalnościach, jak „bezpieczeństwo systemów teleinformatycznych", „cyberobrona" czy „bezpieczeństwo cybernetyczne". Wiedza przekazywana studentom powinna obejmować:

[7] Patrz np. standardy NERC-CIP (CIP − *Critical Infrastructure Protection*) oraz [32].

[8] *Terms of reference for an ENISA ICS Security Stakeholder Group* − https://resilience.enisa.europa.eu/ics-security/EICSSGTermsofReference.pdf

[9] Ocena bazowała na dziewięciu kryteriach, przydzielonych (po trzy) do trzech grup: prawo lokalne, wsparcie operatorów usług krytycznych przez państwo, lokalne warunki eksploatacji i rozwoju systemów ICS-SCADA.

[10] Obecnie Instytut Teleinformatyki i Cyberbezpieczeństwa.

1. **Zalecenia normatywne**, które powinny być dla inżyniera podstawowymi elementami ukierunkowującymi jego działania przy projektowaniu, konstrukcji, wdrażaniu i ocenie rozwiązań i produktów, w tym przypadku z zakresu bezpieczeństwa *Operational Technology*. Jako podstawę proponuje się zapoznanie studentów z normą IEC 62443 oraz *The CIS Critical Security Controls for Effective Cyber Defense* (w wersji dla sieci i systemów przemysłowych).
2. Znajomość **sposobów realizacji celowych zagrożeń**[11] dla infrastruktury przemysłowej, w tym jej zasobów informacyjnych (w szczególności danych produkcyjnych i sterujących) oraz **znajomość metod i narzędzi** umożliwiających skuteczne przeciwdziałanie takim realizacjom. Jako podstawę proponuje się zapoznanie studentów z rozbudowanym frameworkiem MITRE ATT&CK w wersji dla sieci i systemów przemysłowych. Narzędzie to jest obecnie podstawą działań w zakresie bezpieczeństwa informacyjnego prowadzonych przez wiele uznanych firm z branży „bezpieczeństwa".
3. Tak zwane **„dobre praktyki"** opracowane przez uznane organizacje oraz stosowane i doskonalone w praktyce na całym świecie przez firmy zajmujące się zabezpieczeniem zasobów informacyjnych. Jako podstawę proponuje się zapoznanie studentów z „dobrymi praktykami" dotyczącymi zabezpieczania sieci i systemów przemysłowych, opublikowanymi [16] przez *Bundesamt für Sichercheit in der Informationstechnik*.

Wymienione trzy elementy nauczania: norma IEC 62443 oraz standard *The CIS Critical Security Controls for Effective Cyber Defense*, MITRE ATT&CK w wersji dla sieci i systemów przemysłowych oraz „dobre praktyki" opracowane przez *Bundesamt für Sichercheit in der Informationstechnik* są przedstawione w kolejnych rozdziałach niniejszego artykułu.

2. Normy, standardy i zbiory „dobrych praktyk" dotyczące bezpieczeństwa sieci przemysłowych

Zamieszczona w pracy [2] tabela nr 8: *Top 10 Regulations, Standards, Best Practices Used* przedstawia następujący ranking (z prawej strony procent respondentów, którzy wskazali dany standard, regulację lub zbiór dobrych praktyk):

1. NIST CSF (Cyber Security Framework)	38.1%
2. ISO 27000 series	32.0%

[11] Potocznie nazywanych atakami.

3. **NIST 800-53**	31.4%
4. **NIST 800-82**	30.9%
5. **ISA/IEC 62443**	30.4%
6. CIS Critical Security Controls	29.9%
7. **NERC CIP**	23.7%
8. GDPR	15.5%
9. C2M2 (Cybersecurity Capability Maturity Model)	10.3%
10. NIS Directive (EU)	8.3%.

Badaniem objęto 338 respondentów, przy czym większość (ok. 70%) pochodziła z USA i Kanady i ten fakt należy mieć na uwadze przy dyskusji popularności konkretnych regulacji, standardów czy zbiorów dobrych praktyk. Warto też zauważyć, że do jednego worka wrzucono opracowania o różnych profilach:

- NIST CSF [36] jest opracowaną przez organ standaryzacyjny USA, w odpowiedzi na regulacje prawne administracji rządowej, ogólną metodyką zabezpieczania infrastruktury krytycznej państwa w zakresie „cybersecurity". W jej ramach ICS są jednym z zabezpieczanych elementów[12].
- Seria ISO 27000 dotyczy bezpieczeństwa informacji w systemach informacyjnych, w tym budowania systemów zarządzania bezpieczeństwem informacji (SZBI). Nie dotyczy bezpośrednio ICS.
- NIST 800-53 [31] jest standardem zawierającym zbiór zalecanych przez NIST zabezpieczeń i metodykę ich wdrożenia w systemach informacyjnych. Do ICS standard ten stosuje się przez dodatkowe uregulowania (NIST 800-82 [30]).
- CIS Critical Security Controls są zbiorem 20 dobrych praktyk zabezpieczania systemów informatycznych przed atakami (tylko!). Nie odnoszą się bezpośrednio do ICS – sposób zastosowania tych zaleceń do ICS jest podany w [35][13].
- NIS Directive (EU) jest dyrektywą europejską mającą na celu usprawnienie współpracy (przede wszystkim międzynarodowej) w zakresie incydentów dotyczących infrastruktury krytycznej. Nie odnosi się bezpośrednio do ICS.

[12] W oryginalnej publikacji [36] zapisano: (…) *The Framework offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on* information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), *or connected devices more generally, including the* Internet of Things (IoT).

[13] Patrz też część 5 tego artykułu.

- GDPR (*General Data Protection Regulation*), czyli po polsku RODO, dotyczy tylko jednej kategorii informacji – danych osobowych, które w systemach ICS mają marginalne znaczenie.
- **Tylko ISA/IEC 62443, NIST 800-82, NERC CIP dotyczą w całości i bezpośrednio ICS** (ten ostatni zbiór standardów jest ukierunkowany na ICS w elektroenergetyce).

W rozdz. 2.1 przedstawiono krótką charakterystykę serii norm IEC 62443, ponieważ to one obecnie stanowią światowy standard w dziedzinie bezpieczeństwa sieci i systemów przemysłowych oraz dlatego, że w tabeli 1 jest pokazane mapowanie zaleceń BSI na zalecenia tej serii norm. W rozdz. 2.2 z kolei scharakteryzowano *CIS Critical Security Controls* w wydaniu „przemysłowym".

2.1. Seria norm IEC 62443

Mająca za podstawę serię standardów ISA99 norma ISA/IEC 62443 jest normą wieloelementową [17]-[28] (patrz rys. 5; IACS – ang. *Industrial Automation and Control Systems*)[14]. Jej elementy układają się w następujące cztery „serie":

– Seria 1 zawiera wyjaśnienie używanych terminów, koncepcji oraz proponowane miary „bezpieczeństwa".
– Seria 2 dotyczy bezpieczeństwa czynności operacyjnych i eksploatacji.
– Seria 3 zawiera proponowane poziomy ochrony IACS oraz standaryzuje realizację zadań bezpieczeństwa dla OEM i integracji elementów przygotowywanych na zamówienie klienta.
– Seria 4 dotyczy „bezpiecznego" cyklu życia produktów, takich jak przełączniki, sterowniki, zapory sieciowe itp. oraz technicznych wymagań bezpieczeństwa dla tych produktów.

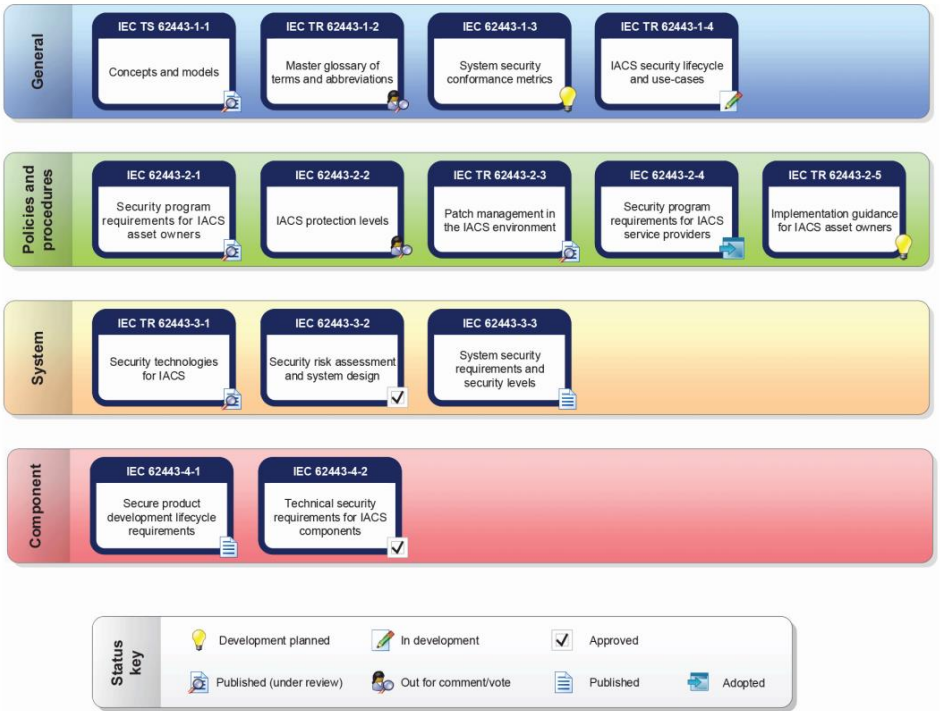
Polski Komitet Normalizacyjny wydał dotychczas (stan na maj 2020) następujące normy polskie serii IEC 62443[15]:

1. **PN-EN IEC 62443-4-1:2018-06 –** wersja angielska: Bezpieczeństwo w systemach sterowania i automatyki przemysłowej − Część 4-1: *Wymagania cyklu rozwoju dotyczące tworzenia bezpiecznego produktu*.

   W tej części normy podano wymagania dla bezpiecznego procesu wytwarzania produktów wykorzystywanych w systemach sterowania i automatyki przemysłowej. Zdefiniowano bezpieczny proces tworzenia

[14] Ułatwia to np. jej aktualizację.
[15] Ale jak widać, nie przetłumaczono tych norm (oprócz tytułów) na język polski!

i rozwoju (SDL) oraz podano definicje wymagań bezpieczeństwa, bezpiecznego projektowania i bezpiecznego wdrożenia (wraz z wytycznymi dla procesów: kodowania, weryfikacji i walidacji, obsługi błędów i wprowadzania poprawek oraz wycofania produktu z użycia). Te wymagania mogą być stosowane do nowych lub istniejących projektów rozwojowych, obsługi i utylizacji sprzętu, programów lub oprogramowania produktów nowych lub istniejących. Wymagania te dotyczą projektantów i serwisantów produktów, nie dotyczą użytkowników produktów. Pełny wykaz wymagań jest podany w załączniku B normy.



Rys. 1. Stan procesu wydawniczego norm serii 62443 na koniec roku 2019 (za IEC 62443-4-2:2019)

2. **PN-EN IEC 62443-4-2:2019-08** – wersja angielska: Bezpieczeństwo w systemach sterowania i automatyki przemysłowej − Część 4-2: *Wymagania techniczne bezpieczeństwa dla komponentów IACS*.

   W tej części normy zamieszczono techniczne wymagania bezpieczeństwa dla komponentów systemów sterowania powiązane z siedmioma podstawowymi

wymaganiami FR (*Foundational Requirement*)) opisanymi w IEC TS 62443-1-1[16]:

- FR-1 – identyfikacja i kontrola autoryzacji (IAC – *Identification and Authentication Control*),
- FR-2 – sterowanie użytkowe (UC – *Use Control*),
- FR-3 – nienaruszalność systemu (SI – *System Integrity*),
- FR-4 – poufność danych (DC – *Data Confidentiality*),
- FR-5 – ograniczenie przepływu danych (RDF – *Restricted Data Flow*),
- FR-6 – dokładna w czasie odpowiedź na zdarzenie (TRE – *Timely Response To Events*),
- FR-7 – dostępność zasobów (RA – *Resource Availability*).

Te wymagania są podstawą określania stopnia bezpieczeństwa systemu za pomocą tzw. poziomów bezpieczeństwa (SL – *Security Level*). Celem tej normy jest definicja przy użyciu kryteriów FR 1-7 bezpieczeństwa systemu sterowania na poziomie komponentu systemu sterowania (SL-C). Poziom bezpieczeństwa (SL-T) oraz poziom bezpieczeństwa osiągnięty (SL-A), nie są objęte zakresem tej normy.

3. **PN-EN IEC 62443-3-3:2020-01 –** wersja angielska: Przemysłowe sieci komunikacyjne − Bezpieczeństwo sieci i systemów − Część 3-3: *Wymagania dla systemu bezpieczeństwa i poziomów bezpieczeństwa*[17].

   W tej części normy zamieszczono techniczne wymagania bezpieczeństwa dla systemów sterowania przy użyciu kryteriów FR 1-7.

4. **PN-EN IEC 62443-2-4:2019-12 –** wersja angielska: Bezpieczeństwo w automatyce przemysłowej i systemach sterowania − Część 2-4: *Wymagania dla programu bezpieczeństwa dla dostawców usług IACS.*

   W tej normie określono wymagania bezpieczeństwa dla dostawców usług dla IACS, które to usługi mogą świadczyć np. podczas konserwacji systemów automatyki. Całość wymagań bezpieczeństwa spełnianych przez dostawcę usługi dla IACS jest nazywana *Programem Bezpieczeństwa*.

Zaproponowane w normie poziomy bezpieczeństwa (SL – ang. *Security Level*) to:

1. **SL 1** – przeciwdziałanie nieautoryzowanemu ujawnieniu informacji poprzez podsłuch lub przypadkową jej ekspozycję. Norma IEC 62443-3-3 specyfikuje

[16] Zawierającymi wymagania dla kompatybilności poziomów bezpieczeństwa SL-C (*Security Level-Control*).

[17] W oryginale: *system security requirements and security levels*. Czyli poprawnie powinno być: *wymagania na bezpieczeństwo systemu i poziomy bezpieczeństwa*.

37 wymagań, które powinny być spełnione, jeżeli jest deklarowany ten poziom bezpieczeństwa.

2. **SL 2** – przeciwdziałanie nieautoryzowanemu ujawnieniu informacji słabo zmotywowanemu i mającemu ogólne umiejętności podmiotowi, który aktywnie jej poszukuje przy użyciu prostych metod i zaangażowaniu niewielkich środków. Norma IEC 62443-3-3 specyfikuje 23 wymagania, które powinny być spełnione, jeżeli jest deklarowany ten poziom bezpieczeństwa.
3. **SL 3** – przeciwdziałanie nieautoryzowanemu ujawnieniu informacji średnio zmotywowanemu i mającemu ukierunkowane na IACS umiejętności podmiotowi, który aktywnie jej poszukuje przy użyciu zaawansowanych metod i zaangażowaniu średniej wielkości środków. Norma IEC 62443-3-3 specyfikuje 30 wymagań, które powinny być spełnione, jeżeli jest deklarowany ten poziom bezpieczeństwa.
4. **SL 4** – przeciwdziałanie nieautoryzowanemu ujawnieniu informacji wysoce zmotywowanemu i mającemu ukierunkowane na IACS umiejętności podmiotowi, który aktywnie jej poszukuje przy użyciu zaawansowanych metod i zaangażowaniu dużych środków (zwykle będzie to podmiot instytucjonalny, np. wojsko lub służby państwowe).

Bardzo dobre wyjaśnienie praktycznego zastosowania koncepcji poziomów bezpieczeństwa jest zaprezentowane w pracy [1].

IEC 62443 *Cybersecurity Certification Programs* prowadzony jest w czterech kategoriach [3]:

1. Certyfikacji procesów – oceniane są procesy projektowania, integracji i testowania urządzeń i sieci ICS.
2. Certyfikacji urządzeń – oceniane są urządzenia, takie jak PLC, bramy sieciowe, zapory sieciowe, DCS.
3. Certyfikacji systemów – oceniane są złożone systemy zawierające różne urządzenia i sieci.
4. Certyfikacji osób:
   - certyfikat 1: *ISA/IEC 62443 Cybersecurity Fundamentals Specialist*;
   - certyfikat 2: *ISA/IEC 62443 Cybersecurity Risk Assessment Specialist*;
   - certyfikat 3: *ISA/IEC 62443 Cybersecurity Design Specialist*;
   - certyfikat 4: *ISA/IEC 62443 Cybersecurity Maintenance Specialist*.

Uzyskanie certyfikatów 1-4 uprawnia do tytułu *ISA/IEC 62443 Cybersecurity Expert*.

2.2. Zalecenia organizacyjne SANS

W 2008 roku administracja rządu USA (w tym m.in. *National Security Agency* oraz *SANS Institute*) w porozumieniu z członkami organizacji biznesowych opracowała zbiór zaleceń o nazwie *Consensus Audit Gudelines* (CAG). Zalecenia te zostały udostępnione publicznie przez instytut SANS w 2009 roku pod adresem *www.sans.org*. Przedstawiony w dokumencie CAG zbiór 20 zalecanych przedsięwzięć z zakresu ochrony przed działaniami intruzów (ang. *Critical Controls*) został uznany przez autorów opracowania za **minimalny, ale łatwy do szybkiego wdrożenia standard zabezpieczenia systemów i sieci komputerowych przed cyberatakami**[18]. Koncepcja CAG/CIS jest zbliżona do metodyki proponowanej przez NIST.

Najnowsza wersja CAG[19] to wersja 7.1. Od wersji 6.1 różni się zmianą miejsc niektórych zaleceń spośród pierwszej szóstki i zmianą nazwy zalecenia 17 na *Implement security Awareness and Training Programs*. Od wersji 6.0 zmieniła się nazwa dokumentu/projektu z *Consensus Audit Gudelines* (CAG) na *The CIS Critical Security Controls for Effective Cyber Defense*[20]. Udostępnianie kolejnych wersji artefaktów projektu odbywa się poprzez stronę *www.cisecurity.org*.

Dalej jest przedstawiona lista (wraz z tłumaczeniami) wszystkich punktów Critical Control dokumentu CAG v.6.1[21] (patrz też rys. 3 dla wersji 7.1). Liczby w nawiasach oznaczają liczbę zalecanych przedsięwzięć w ramach każdego z punktów[22].

1. *Inventory of Authorized and Unauthorized Devices* (6) – inwentaryzacja autoryzowanego i nieautoryzowanego sprzętu.
2. *Inventory of Authorized and Unauthorized Software* (4) – inwentaryzacja autoryzowanego i nieautoryzowanego oprogramowania.
3. *Secure Configurations for Hardware and Software* (7) – utwardzająca konfiguracja sprzętu i oprogramowania na laptopach, stacjach roboczych i serwerach.
4. *Continuous Vulnerability Assessment and Remediation* (8) – ciągłe monitorowanie podatności i ich minimalizowanie.

[18] CAG/CIS został wdrożony m.in. w norweskich elektrowniach – jest to obecnie standard uznany na całym świecie, stąd m.in. jego wybór do programu nauczania.

[19] W czasie przygotowywania niniejszego opracowania, tj. maj 2020 roku. Dostępna pod: https://learn.cisecurity.org/cis-controls-download. CAG jest też krótko opisany w rozdz. 6.1.3 w publikacji [4].

[20] CIS − *Center for Internet Security, Inc.*

[21] Punkty 1-10 dotyczą systemu, punkty 11-13 sieci, a punkty 14-20 aplikacji.

[22] W sumie daje to 149 punktów sprawdzeń do audytu zgodności.

5. *Controlled Use of Administrative Privileges* (9) – nadzór nad kontami administratorów i używaniem przywilejów administracyjnych.
6. *Maintenance, Monitoring, and Analysis of Audit Logs* (6) – utrzymanie, monitorowanie i analiza dzienników bezpieczeństwa.
7. *Email and Web Browser Protections* (8) – ochrona poczty elektronicznej i przeglądarek.
8. *Malware Defenses* (6) – ochrona przed programami i kodami złośliwymi.
9. *Limitation and Control of Network Ports* (6) – ograniczenie i kontrola portów, protokołów i usług sieciowych.
10. *Data Recovery Capability* (4) – zapewnianie zdolności do odzyskiwania danych.
11. *Secure Configurations for Network Devices* (7) – bezpieczna konfiguracja urządzeń sieciowych.
12. *Boundary Defense* (10) – stosowanie ochrony brzegowej.
13. *Data Protection* (9) – ochrona danych.
14. *Controlled Access Based on the Need to Know* (7) – kontrola dostępu na podstawie wiedzy koniecznej.
15. *Wireless Access Control* (9) – nadzór nad dostępem bezprzewodowym.
16. *Account Monitoring and Control* (14) – monitorowanie i kontrola kont użytkowników.
17. *Security Skills Assessment and Appropriate Training to Fill Gaps* (5) – ocena umiejętności personelu w zakresie bezpieczeństwa i odpowiednie szkolenia w celu eliminacji braków.
18. *Application Software Security* (9) – zapewnianie bezpieczeństwa aplikacji.
19. *Incident Response and Management* (7) – reagowanie na incydenty i zarządzanie incydentami.
20. *Penetration Tests and Red Team Exercises* (8) – wykonywanie testów penetracyjnych i ćwiczeń zespołów typu Red Team.

Publikacja [35] jest poradnikiem, jak zalecenia CIS przystosować do ICS. W publikacji tej każde z zaleceń (Critical Controls) jest jednolicie opisane. Na opis składają się zawsze trzy części: uzasadnienie stosowania (*Introduction*), zakres stosowania (*Applicability*) oraz dodatkowe wskazówki/ rozważania (*Considerations*). Przykład jest zamieszczony na rysunku 2.

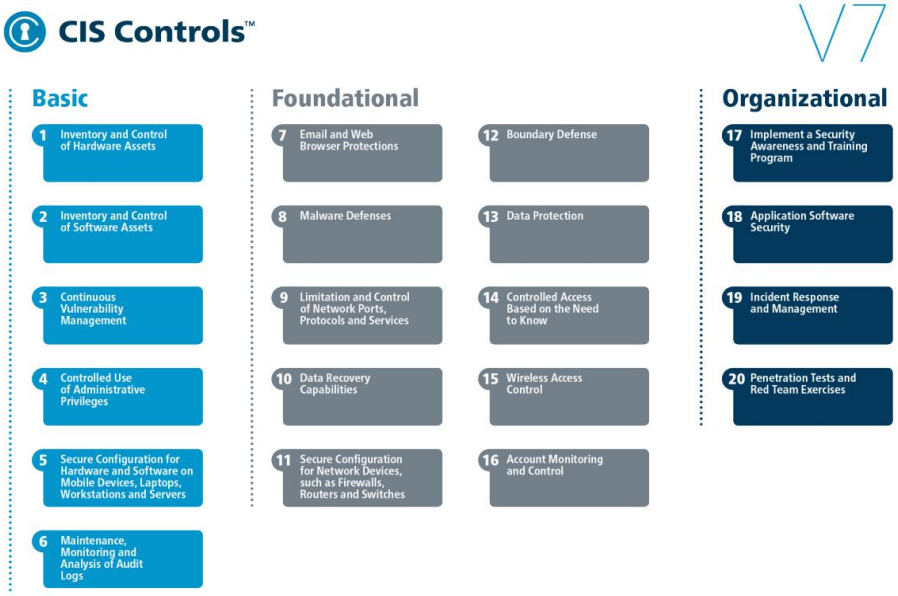
Każde zalecenie, traktowane także z innej perspektywy jako tzw. *punkt kontrolny*, zawiera wszystkie lub część przedstawionych dalej elementów, z których każdy opisuje pewne zagadnienia zabezpieczenia systemu w zakresie danego punktu kontrolnego lub wdrażania w organizacji zaleceń tego punktu:

CIS Control 11 – Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	
ICS Rationale, Applicability, and Considerations	
Introduction	This CIS Control addresses the need to manage the configuration of all network devices using a change control process. The network infrastructure of an ICS network typically carries additional requirements when compared to traditional IT systems. Usually these networks focus on availability and are architected with real-time performance and redundancy requirements. Attack vectors, however, remain the same. Unsecure services, poor firewall configurations, and default credentials remain issues.
Applicability	Due to the availability requirements associated with the ICS environments, Sub-Controls relating to network traffic may not be applicable.
Considerations	For this CIS Control consider the following additional steps: • Ensure firewalls are configured to deny by default. • If a location is unmanned or if critical process data flows through a perimeter device, ensure redundancy exists or device failure won't prevent this data from being received by its intended destination. If the management environment is sufficiently isolated, then multifactor authentication may not be required to manage network devices. Adding multifactor requirements can limit the use of vendor supplied network monitoring solutions.

Rys. 2. Przykład opisu zaleceń CIS w wersji dla ICS [35]

1. *How do Attackers Exploit the Absence of this Control?* – możliwy sposób wykorzystania przez intruza niezabezpieczonej podatności opisanej w danym punkcie.
2. *How to Implement, Automate, and Measure the Effectiveness of this Control?* – zalecenia odnośnie do minimalizowania danej podatności.
3. *Associated NIST Special Publication 800-53 Revision 3, Priority 1 Controls* – powiązania z dokumentami NIST.
4. *Associated NSA Manageable Network Plan Milestones and Network Security Tasks* – powiązania z dokumentami NSA.
5. *Procedures and Tools to Implement and Automate this Control* – opis możliwości wspomagania za pomocą narzędzi i przedsięwzięć organizacyjnych procesu zabezpieczania.
6. *Control xx Metric* – wymagania, jakie musi spełniać system, aby wypełniał założenia zawarte w danym punkcie.

7. *Control xx Test* – propozycje sprawdzeń, jakie muszą być przeprowadzone, aby ocenić implementację danego punktu CAG w praktyce biznesowej organizacji.
8. *Control xx Sensors, Measurements and Scoring* – propozycje sposobu realizacji i oceny sprawdzeń opisanych w punkcie Control xx Test.



Rys. 3. Zbiór zalecanych Critical Control w CAG v.7.1

3. Ataki na sieci i systemy przemysłowe

Podstawowy zbiór zagrożeń dla poprawnego działania sieci i systemów teleinformatycznych oraz sieci i systemów przemysłowych obejmuje:

1. Zagrożenia środowiskowe, tj. oddziaływanie:
   - ognia (np. pożary instalacji przemysłowych wywołanych uderzeniem pioruna),
   - wody (np. wylewy rzek powodujące podtopienia obiektów z infrastrukturą teleinformatyczną),
   - czynników mechanicznych (np. trzęsienia ziemi lub huragany niszczące infrastrukturę telekomunikacyjną),
   - czynników biologicznych (np. wirusów, powodujących braki w personelu obsługującym sieci i systemy teleinformatyczne i przemysłowe) itp.
2. **Zagrożenia celowymi** lub błędnymi **działaniami człowieka.**

3. Tak zwane „siły wyższe” inne niż zagrożenia środowiskowe (np. ustanowienie złych przepisów prawa przez ustawodawcę).

Wspomniane w tytule rozdziału „ataki” to forma realizacji zagrożenia celowymi działaniami człowieka. Cennym źródłem wiedzy o możliwościach ataków na zasoby informacyjne oraz sieci i systemy teleinformatyczne jest strona *https://attack.mitre.org/*[23]. Zawiera ona podstronę:

https://collaborate.mitre.org/attackics/index.php/Main_Page[24]

z tabelą podsumowującą **ataki na sieci i systemy przemysłowe** (jej fragment jest zamieszczony na rysunku 4). Na kolejnych podstronach są szczegółowe opisy:

- 81 technik ataków na systemy ICS;
- 17 narzędzi programowych używanych do ataków na systemy ICS (strona aktualizowana 02.01.2020);
- 10 ujawnionych grup atakujących systemy ICS (strona aktualizowana 02.01.2020).

Należy podkreślić, że opisywany framework (bo tak jest traktowany MITRE ATT&CK) dotyczy jedynie sposobów realizacji (czyli ataków) jednego typu zagrożenia – celowych działań ludzi.

Również w dodatku C (*Threat Sources, Vulnerabilities, and Incidents*) standardu NIST SP 800-82 rev. 2 zamieszczony jest opis 16 incydentów dotyczących ICS (w tym 8 ataków). Opis jest doprowadzony do roku 2013.

Dane statystyczne pokazują także [2], jak grupują się incydenty bezpieczeństwa dla ICS związane z działaniami ludzi (dane na rok 2019). Wyróżnia się incydenty związane z[25]:

1. Dostępem fizycznym (np. poprzez USB lub bezpośredni fizyczny dostęp do urządzenia, w szczególności do jego panelu sterującego) 56,3%.
2. Dostępem zdalnym (obejście zabezpieczeń wbudowanych w architekturę ICS) 40,6%.
3. Zaufanym dostępem zdalnym (dostęp zaufanego podmiotu bez naruszenia zabezpieczeń technicznych) 37,5%.
4. Działaniami serwisowymi i konsultacjami (skutki: nierozpoznane zmiany w konfiguracji) 34,4%.
5. Łańcuchem dostaw (np. oprogramowanie lub sprzęt niezgodne ze specyfikacjami) 18,8%.

[23] Dostęp 16.05.2020.

[24] Dostęp 16.05.2020; strona aktualizowana 04.03.2020.

[25] Podane na końcu każdego punktu wartości procentowe informują, jaki procent respondentów badania prowadzonego przez SANS wskazał na daną grupę.

The MITRE ATT&CK for ICS Matrix is an overview of the tactics and techniques described in the ATT&CK for ICS knowledge base. It visually aligns individual techniques under the tactics in which they can be applied. Some techniques span more than one tactic because they can be used for different purposes.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/ Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View

Rys. 4. Fragment tabeli podsumowującej ataki na systemy ICS (ze strony https://collaborate.mitre.org/attackics/index.php/Main_Page).

4. Kompendium niemieckiego urzędu ds. bezpieczeństwa informacyjnego

Niemiecki urząd ds. bezpieczeństwa informacyjnego (BSI − *Bundesamt für Sichercheit in der Informationstechnik*; https://www.bsi.bund.de) wydał Kompendium [16], w którym, oprócz podstawowych zagadnień bezpieczeństwa ICS, w rozdziale 5 opisano 73 „najlepsze praktyki" w zakresie zapewniania bezpieczeństwa ICS rekomendowane przez ww. urząd. Praktyki te przyporządkowano do pięciu następujących grup:

1. Podstawowe przedsięwzięcia (ang. *first steps*; praktyki 1-6; rozdz. 5.2).
2. Procesy i zasady bezpieczeństwa (ang. *security-specific processes/policies*; praktyki 7-18; rozdz. 5.3).
3. Wybór (zakup) systemów i ich komponentów oraz związanych z nimi dostarczycieli usług serwisowych i integratorów (ang. *selection of the used systems and components as well as of the assigned service providers and integrators*; praktyki 19-30; rozdz. 5.4).
4. Bezpieczeństwo konstrukcyjne i fizyczne (ang. *constructional and physical securing*; praktyka 31; rozdz. 5.5).
5. Przedsięwzięcia techniczne (ang. *technical measures*; praktyki 32-73; rozdz. 5.6).

Te zalecenia zapisano w zwarty sposób w tabeli 7 Kompendium zatytułowanej: *Comparison of the best practices with IEC 62443, VDI/VDE*[26] *2182, NERC CIP*[27] *and DHS*[28] *Best Practices*. Zgodnie z tytułem, rekomendowane „najlepsze praktyki" BSI są w tej tabeli mapowane na zalecenia (nazywane tutaj też „najlepszymi praktykami") wymienionych norm i standardów. Tabela 1 to autorski wariant wspomnianej tabeli 7 z Kompendium, z własnymi komentarzami i mapowaniem na zalecenia normy IEC 62443.

[26] Verein Deutscher Ingenieure/Verband der Elektrotechnik Elektronik Informationstechnik.

[27] North American Electric Reliability Corporation Common Industrial Protocol.

[28] Department of Homeland Security.

Tab. 1. Zalecenia Bundesamt für Sichercheit in der Informationstechnik (BSI) z zakresu zabezpieczania sieci i systemów przemysłowych.

Lp.	Zalecane praktyki (ICS Security Compendium v.1.23)	Odpowiednik w normie IEC 62443	Komentarze
1	Właściciele zasobów powinni ustanowić organizację zarządzania i kontrolowania ról i odpowiedzialności w zakresie bezpieczeństwa elementów ICS.	2-1 chapter A.3.2.3 2-1 chapter 4.3.2.3 2-1 chapter 4.3.2.3	Dotyczy wszystkich aktorów mających styczność z elementami ICS, np. dostawców produktów.
2	Zadbać o właściwe wytwarzanie i zarządzanie dokumentacją ICS.	2-1 chapter A.3.4.4 2-1 chapter 4.2.3.13	Należy opisać cykl życia dokumentacji.
3	Utworzyć SZBI dla informacji wykorzystywanych przez ICS.	Complete 2-1	**S**ystem **Z**arządzania **B**ezpieczeństwem **I**nformacji (SZBI).
4	Utrzymywać plan sieci (fizyczny i logiczny), na którym jest uwidocznione rozmieszczenie elementów ICS.	2-1 chapter A.3.4.2.3.3 2-1 chapter 4.2.3.5	
5	Utrzymywać w celu zapewnienia spójności listę eksploatowanego oprogramowania i listę plików konfiguracyjnych dla elementów ICS.	2-1 chapter 4.2.3.4 3-1 chapter 8.7	
6	Wytworzyć, utrzymywać i udostępniać zainteresowanym dokumentację operacyjną dla administratorów i użytkowników ICS.	2-1 chapter A.3.3.5	Ang. *Administration and user manual*.
7	Wdrożyć wewnętrzne zasady projektowania i integracji (z zakupionymi ICS) samodzielnie wytworzonego oprogramowania.	2-1 chapter 4.3.4.3.1 2-1 chapter 4.3.4.3.3 2-1 chapter 4.3.4.3.4 2-1 chapter 4.3.4.3.5	
8	Zadbać o bezpieczne wycofanie z użycia sprzętu.	2-1 chapter 4.3.3.3.9	Np. twardych dysków.
9	Chronić raporty audytowe.		
10	Właściciele zasobów, integratorzy i dostawcy powinni opracować i udokumentować odpowiednie procedury operacyjne.		Wytwarzania aplikacji, instalowania poprawek, konfigurowania itd.
11	Należy zarządzać zmianami.	2-1 chapter A.3.4.3.6 2-1 chapter 4.3.4.3.2	Np. osoba zalecająca zmianę nie powinna jej implementować
12	Zapewnić nadzór nad bezpieczeństwem i ciągłe monitorowanie stanu bezpieczeństwa.	2-1 chapter A.3.4.5 2-1 chapter 4.3.4.5 2-1 chapter 4.3.3.3.8	Ang. *Security monitoring*.

Lp.	Zalecane praktyki (ICS Security Compendium v.1.23)	Odpowiednik w normie IEC 62443	Komentarze
13	Opracować i wdrożyć plan zapewniania biznesowej ciągłości działania.	2-1 chapter A.3.2.5 2-1 chapter A.3.4.3.8 2-1 chapter 4.3.2.5 2-1 chapter 4.3.4.3.9	Ang. *Business Continuity Plan* (BCP).
14	Dbać o regularne szkolenie personelu.	2-1 chapter A.3.2.4 2-1 chapter 4.3.2.4	
15	Właściwie zarządzać personelem, aby uniknąć związanych z nim naruszeń zasad bezpieczeństwa.	3-1 chapter 10.3, 2-1 chapter A.3.3.2 2-1 chapter 4.3.3.2	Ang. *Personnel security.*
16	Opracować i wdrożyć procedury zatrudniania, zmiany stanowiska i zwalniania pracowników.	2-1 chapter 4.3.3.2	
17	Przeprowadzać regularnie audyty bezpieczeństwa sieci i elementów ICS.	2-1 chapter A.3.4.2.5.4 2-1 chapter 4.2.3.10 2-1 chapter 4.4.2.2	
18	Testować komponenty (ICS) przed instalacją.	2-1 chapter A.3.4.3.5 2-1 chapter A.3.4.2.4.2 2-1 chapter A.3.4.2.4.3 2-1 chapter 4.3.4.3.1	
19	Włączyć do kontraktów z dostarczycielami produktów, zewnętrznymi właścicielami zasobów itp. klauzulę o zachowaniu tajemnicy.		Ang. *Non-disclosure agreement.*
20	Poinformować integratora systemu o obowiązujących wymaganiach bezpieczeństwa.	2-1 chapter A.3.4.2.4 2-1 chapter A.3.4.3	
21	Uwzględnić w analizie ryzyka specyfikację bezpieczeństwa dostarczoną przez integratora systemów ICS.	2-1 chapter A.3.4.2.4 2-1 chapter A.3.4.3	
22	Wymagać od produktów ICS odporności na błędy w oprogramowaniu i sprzęcie.	2-1 chapter A.3.4.2.4.2	W przypadku ujawnienia wady w trakcie działania produktu, musi on zachować się w ustalony sposób.
23	Nabywane produkty ICS muszą być wytworzone zgodnie z uznanymi/obowiązującymi standardami i umożliwiać współdziałanie z innymi produktami zgodnymi z tymi standardami.		Ang. *Compatibility.*

Lp.	Zalecane praktyki (ICS Security Compendium v.1.23)	Odpowiednik w normie IEC 62443	Komentarze
24	Sprzedający powinien dostarczyć produkt ICS z usuniętymi lub dezaktywowanymi funkcjami, które nie były wyspecyfikowane w zamówieniu.		Takie działanie musi być udokumentowane.
25	Dane dostępowe do komponentów ICS, po dostarczeniu przez sprzedającego, muszą być zmienione.	2-1chapter A.3.3.5.3.13	Patrz też 46.
26	Sprzedający powinien dostarczyć produkt z włączonymi funkcjami bezpieczeństwa, odpowiednio skonfigurowany oraz podać status zaktualizowania (ang. *patch status*).		Dostarczony produkt powinien być utwardzony (ang. *hardened*).
27	Wszystkie zainteresowane strony powinny przedstawić strategię długoterminowego zapewniania bezpieczeństwa instalacji przemysłowej.		
28	Nabywane komponenty ICS powinny być wyposażone w oprogramowanie antywirusowe lub powinny wspierać działanie takiego oprogramowania.		
29	**Musi być zachowana zgodność poziomów bezpieczeństwa ICS i systemu zdalnej obsługi tego ICS.**	2-1 chapter A.3.3.6.5.3 3-1 chapter 7.4	Patrz też 32 i 68 **BARDZO WAŻNE ZALECENIE!**
30	Muszą być sprecyzowane i zaimplementowane wymagania bezpieczeństwa dla urządzeń polowych		Urządzenia polowe (ang. *field devices*) – czujniki i elementy wykonawcze.
31	Zapewnić odpowiednią ochronę fizyczną komponentom ICS.	3-1 chapter 10.2 2-1 chapter A.3.3.3 2-1 chapter 4.3.3.3	Dotyczy budynków, pomieszczeń i szaf z urządzeniami.
32	Zapewnić segmentację sieci ICS.	2-1 chapter A.3.3.4 2-1 chapter A.3.4.2.3.3 2-4 chapter 4.3.3.4	Połączenia pomiędzy segmentami mogą być nawiązywane tylko od strony segmentu o wyższym poziomie ochrony.
33	Zabezpieczyć wszystkie zewnętrzne interfejsy do ICS.	2-1 chapter A.3.3.6.5.3	Patrz też: 2, 4, 29, 73.
34	Zaleca się statyczną konfigurację sieci.		
35	Wszystkie komponenty w jednym segmencie sieci powinny być zabezpieczone na tym samym poziomie.	2-1 chapter A.3.4.2.3.3	

Lp.	**Zalecane praktyki** (ICS Security Compendium v.1.23)	**Odpowiednik w normie IEC 62443**	**Komentarze**
36	Dążyć do niezależności operacji w poszczególnych segmentach ICS (utrata połączenia pomiędzy segmentami nie powinna mieć wpływu na produkcję lub wpływ powinien być minimalny).		
37	Poprawnie zabezpieczyć technologie bezprzewodowe używane w sieciach i systemach ICS.		
38	Do logicznej separacji segmentów sieci ICS używać sprzętowych zapór sieciowych.	3-1 chapter 6.2	Ang. *Firewalls.*
39	O ile to możliwe, na każdym komponencie ICS powinna być zainstalowana programowa zapora osobista.	3-1 chapter 6.3	Ang. *Host-based firewalls*.
40	Rozważyć użycie diód danych (ang. *Data diode; one-way gateway*).		
41	Zapewnić odpowiednią separację logiczną za pomocą VLAN-ów i separację fizyczną (na poziomie urządzeń) dla segmentów sieci z różnymi wymaganiami bezpieczeństwa.	3-1 chapter 6.4	
42	Rozważyć zaimplementowanie *Intrusion Detection System* (IDS) i/lub *Intrusion Prevention System* (IPS); zalecane jedynie dla dużych organizacji.	3-1 chapter 8.4	Na każdym urządzeniu ICS powinien być zainstalowany HIDS (*Host-IDS*).
43	Do realizacji zadań administrowania siecią lub zadań krytycznych ze względu na bezpieczeństwo używać tylko bezpiecznych protokołów (np. SSH, SFTP, HTTPS).		Lub protokołów dodatkowo zabezpieczonych kryptograficznie, np. SSL/TLS.
44	W sieciach ICS używać serwera DNS przeznaczonego do obsługi tylko tych sieci, odseparowanego od serwerów DNS z innych sieci (np. biurowych).		W celu utrzymania wysokiej dostępności, serwery DNS powinny być zdublowane.
45	Zapewnić synchronizację czasu (sygnałem czasu z zaufanego źródła).		Zalecane: Network Time Protocol lub IEEE 1588.

Lp.	Zalecane praktyki (ICS Security Compendium v.1.23)	Odpowiednik w normie IEC 62443	Komentarze
46	Zaleca się usuwanie domyślnych kont i zmianę domyślnego hasła natychmiast po instalacji i sprawdzeniu poprawności działania urządzenia lub programu.	2-1 chapter 3.3.5.3.9 2-1 chapter 4.3.3.5.5 2-1 chapter 4.3.3.5.7 2-1chapter A.3.3.5.3.13	
47	Starać się przydzielić osobom obsługującym urządzenia ICS indywidualne konto w celu jednoznacznego rozliczania wykonanych czynności.	2-1 chapter A.3.3.5.3.7 2-1 chapter 4.3.3.5.2	W środowisku ICS jest to często niemożliwe.
48	Usunąć niepotrzebne oprogramowanie i usługi z komponentów ICS.		
49	Odpowiednio zmienić ustawienia domyślne.	2-1chapter A.3.3.5.3.13	
50	Dostroić do potrzeb konfigurację sprzętu.		Niepotrzebne porty USB, napędy CD/DVD itp. usunąć lub zablokować.
51	Zablokować nieograniczony dostęp do Internetu z poziomu sieci ICS.		
52	Opracować i wdrożyć procedurę aktualizacji i wgrywania poprawek do oprogramowania.	2-1 chapter A.3.4.2.4.3 2-1 chapter 4.3.4.3.7 2-1 chapter 4.3.4.5.3 2-1 chapter A.3.4.2.3.5	
53	Opracować i wdrożyć procedurę postępowania w przypadku zakończenia wsparcia produktu przez dostawcę.	2-1 chapter A.3.4.2.3.5	
54	Wybrać, na podstawie wyników analizy ryzyka, sposób i metodę uwierzytelniania w sieciach ICS użytkowników i usług.	2-1 chapter A.3.3.6 2-1 chapter 4.3.3.6 3-1 chapter 5.3 3-1 chapter 5.4 3-1 chapter 5.5 3-1 chapter 5.6 3-1 chapter 5.7 3-1 chapter 5.10	
55	Opracować zasady i wdrożyć procedury techniczne i organizacyjne posługiwania się hasłami.	3-1 chapter 5.9	
56	Zapobiegać nieautoryzowanemu dostępowi do systemu.		Każdy dostęp powinien być udokumentowany i rozliczalny: kto, co, kiedy.

Lp.	**Zalecane praktyki** (ICS Security Compendium v.1.23)	**Odpowiednik w normie IEC 62443**	**Komentarze**
57	W procesie autoryzacji uprawnienia przydzielać podmiotom zgodnie z zasadą „wiedzy koniecznej" i „minimalnego środowiska pracy".	2-1 chapter A.3.3.5 2-1 chapter A.3.3.7 2-1 chapter 4.3.3.5	Inna nazwa: zasada najmniejszych przywilejów.
58	Używać narzędzi/algorytmów kryptograficznych odpowiadających aktualnemu stanowi wiedzy w dziedzinie kryptologii.	3-1 chapter 7.2 3-1 chapter 7.3 3-1 chapter 7.4 3-1 chapter 5.2	
59	Jeżeli jest możliwa i dopuszczalna instalacja oprogramowania antywirusowego na komponentach ICS i dopuszcza to także dostawca produktu (ICS), to takie oprogramowanie należy zainstalować wraz z automatyczną aktualizacją sygnatur wirusów.	3-1 chapter 8.3 2-1 chapter 4.3.4.3.8	
60	Opracować i wdrożyć rozwiązania alternatywne, gdy nie można zainstalować oprogramowania antywirusowego.		Dotyczy to często sterowników, PLC, urządzeń polowych.
61	Bazując na rekomendacjach dostawcy oprogramowania antywirusowego i dostawcy produktu (ICS), zapewnić bezpieczną konfigurację oprogramowania antywirusowego.		Proces instalacji i konfiguracji powinien być udokumentowany dla każdego komponentu ICS.
62	Sygnatury wirusów dla oprogramowania antywirusowego nie powinny być pobierane bezpośrednio z Internetu tylko dystrybuowane przez centralny serwer (usługa dystrybucji sygnatur) umieszczony w DMZ.		
63	Zapewnić niezwłoczne pobieranie uaktualnionych baz sygnatur.	2-1 chapter A.3.4.2.4.2	
64	Rozważyć zastosowanie oprogramowania antywirusowego na zaporze sieciowej (*virus wall*, działający w warstwie 7) w celu sprawdzania ruchu pomiędzy sieciami pod kątem przenoszenia malwaru.		Application Level Gateway zwykle nie wspierają protokołów specyficznych dla ICS.
65	Dopuszczać do użytku tylko to oprogramowanie i tylko te jego działania (*behaviour*), które zostały wcześniej zaakceptowane (ang. *whitelisting*).		Nie jest to zamiennik oprogramowania antywirusowego!

Lp.	Zalecane praktyki (ICS Security Compendium v.1.23)	Odpowiednik w normie IEC 62443	Komentarze
66	Opracować i wdrożyć zasady postępowania z nośnikami wymiennymi.		Te zasady muszą być znane wszystkim pracownikom.
67	Wymienne pamięci przed ich zintegrowaniem z sieciami lub urządzeniami ICS sprawdzić na testowym komputerze, tzw. *quarantine PC*.		
68	Opracować i wdrożyć zasady używania notebooków w celach serwisowych.		
69	Aktywować hasło do BIOS-u i dopuszczać bootowanie tylko z wybranego medium na wszystkich urządzeniach ICS.		
70	Dezaktywować funkcję autorun na wszystkich urządzeniach ICS.		
71	Opracować i wdrożyć strategię i zasady wykonywania kopii bezpieczeństwa.	2-1 chapter 4.3.4.3.9	Proces wykonywania kopii bezpieczeństwa nie może mieć wpływu na produkcję.
72	Opracować i wdrożyć zasady przechowywania kopii bezpieczeństwa.	2-1 chapter A.3.4.3.8	
73	Uaktywnić odpowiednie dzienniki zdarzeń i zapisywać w nich monitorowane zdarzenia.	3-1 chapter 8.2 3-1 chapter 8.6 3-1 chapter 8.7 3-1 chapter 8.8 2-1 chapter 4.3.3.5.8 2-1 chapter 4.3.3.6.4	Dotyczy wszystkich dzienników zdarzeń na wszystkich mających je urządzeniach.

5. Podsumowanie

W artykule przedstawiono te elementy wiedzy techniczno-organizacyjnej, które, zdaniem autora, powinny być podstawą nauczania zagadnień bezpieczeństwa z zakresu sieci i systemów przemysłowych na studiach wyższych. Nauczanie powinno być uzupełnione o podstawowe zagadnienia dotyczące obowiązujących rozwiązań prawnych, takich jak ustawa *o Krajowym Systemie Cyberbezpieczeństwa* [33] (i towarzyszące jej rozporządzenia), która dotyczy operatorów usług kluczowych, czy RODO, żeby studenci mieli świadomość tego, jak nauczane zagadnienia techniczno-organizacyjne wpisują się w system prawny państwa. Należy

bowiem mieć na uwadze, że przy projektowaniu systemów zabezpieczeń, zapisy prawne, formalnie, są dla projektanta ograniczeniami projektowymi, które musi uwzględnić w specyfikacji wymagań projektowanego systemu.

Warto także podkreślić, że zabezpieczenie sieci przemysłowej powinno być elementem szerzej widzianego zabezpieczenia zakładu przemysłowego przed incydentami z zakresu bezpieczeństwa informacyjnego. Oznacza to na przykład, że dostawca zabezpieczeń dla sieci przemysłowej powinien umożliwiać ich integrację z rozwiązaniami nadrzędnymi typu SIEM (ang. *Security Information and Event Management*), w celu uzyskania jednolitego obrazu stanu bezpieczeństwa sieci i systemów teleinformatycznych (tzw. biurowych) oraz przemysłowych. Przekładając to na proces edukacji – nauczanie podstaw bezpieczeństwa informacyjnego powinno poprzedzać nauczanie bardziej specjalistycznych zagadnień, w tym tych związanych z ICS, co niestety nie zawsze ma miejsce w praktyce.

Literatura

1. DESRUISSEAUX D., *Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications*. Schneider Electric White Paper, 2018.
2. FILKINS B., WYLIE D.: *SANS 2019 State of OT/ICS Cybersecurity Survey*. ©2019 SANS™ Institute, June 2019.
3. GOBLE W., *Applying the Global Automation Standard IEC 62443 to protect against cyber threats*. Prezentacja. 2019.
4. LIDERMAN K.: *Bezpieczeństwo informacyjne*. *Nowe wyzwania*. WN PWN SA. Warszawa, 2017.
5. LIDERMAN K., *Bezpieczeństwo informacyjne*. WN PWN SA. Warszawa, 2012.
6. LIDERMAN K., *Ochrona informacji i obiektów w sieciach teleinformatycznych połączonych z systemami przemysłowymi – przegląd zagadnień*. Biuletyn IAiR WAT, nr 25, 2008, s. 85-107.
7. LIDERMAN K., ZIELIŃSKI Z.: *Ochrona informacji w połączonych sieciach przemysłowych i teleinformatycznych*. W: Huzar Z., Mazur Z. (red.): Zagadnienia bezpieczeństwa w systemach informacyjnych. WKŁ, Warszawa, 2008, s. 83-97.
8. LIDERMAN K., *Połączone sieci teleinformatyczne i sieci przemysłowe jako elementy infrastruktury krytycznej – zagrożenia i podstawowe standardy ochrony*. W: Cyberterroryzm – nowe wyzwania XXI wieku. Praca zbiorowa pod red. T. Jemioły, J. Kisielnickiego, K. Rajchela, Wyższa Szkoła Informatyki, Zarządzania i Administracji, Warszawa, 2009, s. 244-260.

9. LIDERMAN K., *Audyt bezpieczeństwa sieci teleinformatycznych połączonych z systemami przemysłowymi − wytyczne do modyfikacji metodyki LP-A*. W: Zieliński Z. (red.): Systemy czasu rzeczywistego. Postępy badań i zastosowania. WKŁ, Warszawa, 2009, s. 299-308.
10. SZMUC T., MOTET G.: *Specyfikacja i projektowanie oprogramowania czasu rzeczywistego*. CCATIE, Katedra Automatyki AGH, Kraków, 1998.
11. ŻURAKOWSKI Z., *Systemy komputerowe w zastosowaniach związanych z bezpieczeństwem*. Informatyka, nr 3, 1995, s. 20-28.
12. *21 Steps to Improve Cyber Security of SCADA Networks*. Office of Energy Assurance, U.S. Department of Energy. http://www.oe.netl.doe.gov/docs/prepare /21stepsbooklet.pdf (dostęp 16.05.2020).
13. ENISA: *Industry 4.0 Cybersecurity: Challenges&Recommendations*. May, 2019.
14. ENISA: *Analysis of ICS-SCADA Cyber Security Maturity Levels In Critical Sectors*. 2015.
15. GAO-04-354, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*. U.S. GAO, 2004. http://www.gao.gov/new.items/d04354.pdf (dostęp 16.05.2020).
16. *ICS Security Compendium*. V. 1.23. Federal Office for Information Security (BSI). Germany, 2013.
17. IEC 62443-1-1: *Industrial communication networks - Network and system security – Part 1-1*: *Terminology, concepts and models* (IEC/TR 62443-1-1:2009).
18. ISA-62443-1-2: *Security for industrial automation and control systems – Master Glossary*. Draft 1. Edit 5. August, 2014 (ISA-TR62443-1-2).
19. ISA-62443-1-3: *Security for industrial automation and control systems – Part 1-3: Cyber security system conformance metrics*. Draft 1. Edit 19. October, 2015.
20. ISA-62443-2-1: *Security for industrial automation and control systems: Part 2-1: Industrial automation and control system security management system*. Draft 7. Edit 5. November 9, 2015.
21. ISA-62443-2-2: *Security for industrial automation and control systems: Implementation Guidance for and IACS Security Management System*. Draft 1. Edit 4. April, 2013.
22. IEC 62443-2-3: *Security for industrial automation and control systems: Part 2-3: Patch Management in IACS environment* (IEC /TR 62443-2-3:2015).
23. IEC 62443-2-4: *Security for industrial automation and control systems: Part 2-4: Security program requirements for IACS providers* (IEC 62443-2-4:2015).
24. ISA-62443-3-2: *Security for industrial automation and control systems: Security risk assessment for system design*. Draft 6. Edit 3. August 5, 2015.

25. IEC 62443-3-3: *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels* (IEC 62443-3-3: 2013).
26. IEC/NP 62443-4-1 *Industrial communication networks – Network and system security – Part 4-1: Product development requirements based on ISA-62443-04-01*. Draft 1. Edit 9. April, 2013.
27. ISA-62443-4-1 *Security for industrial automation and control systems Part 4-1: Secure product development life – cycle requirements*. Draft 3. Edit 11. March, 2016.
28. ISA-62443-4-2 *Security for industrial automation and control systems*. *Technical security requirements for IACS components.* Draft 2. Edit 4. July 2, 2015.
29. NERC: *Top 10 vulnerabilities of control systems and their associated mitigations*. 2006.
30. NIST Special Publication 800-82 Rev. 2: *Guide to Industrial Control Systems (ICS) Security*. May, 2015.
31. NIST Special Publication 800-53 Rev. 5: *Security and Privacy Controls for Federal Information Systems and Organizations*. August, 2017.
32. Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. z dn. 21.05.07).
33. Ustawa z dnia 5 lipca 2018 r. *o Krajowym Systemie Cyberbezpieczeństwa* (Dz. U. 1560).
34. US Industrial Control Systems Cyber Emergency Response Team: *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. September, 2016.
35. *Implementation Guide for Industrial Control Systems*. Version 7. CIS Controls™ https://www.cisecurity.org/controls/ (dostęp 22.05.2020).
36. NIST: *Framework for Improving Critical Infrastructure Cybersecurity* v.1.1. April 16, 2018. https://doi.org/10.6028/NIST.CSWP.04162018 (dostęp 22.05.2020).

ICS security – subject content proposal

ABSTRACT: The paper considers the issue of ICS security teaching. A brief ICS characteristic is given in the introduction. Background chapters present basic norms and standards (e.g.: IEC 62443 and *CIS Critical Security Controls for Effective Cyber Defense*), framework MITRE ATT&CK, as well as a set of „best practices" published by *Bundesamt für Sichercheit in der Informationstechnik*. The considered problem under is based on these elements.

KEYWORDS: Industrial Control System (ICS), IEC 62443, MITRE ATT&CK Framework, „best practices" for Operational Technology (OT)

Praca wpłynęła do redakcji: 16.06.2020 r.

Analiza użyteczności usługi wideokonferencji Microsoft Teams do nauczania zdalnego na uczelni wyższej

Radosław KISTER, Bartosz KONECKI, Jakub SYCHOWIEC, Rafał TWAROWSKI

Instytut Teleinformatyki i Cyberbezpieczeństwa, Wydział Cybernetyki, WAT
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
{radoslaw.kister}, {bartosz.konecki},
{jakub.sychowiec}, rafal.twarowski01@student.wat.edu.pl

STRESZCZENIE: Usługa wideokonferencji, jaką jest Microsoft Teams, jest rodzajem usługi w modelu „cloud computing" typu SaaS (Software as a Service). W ramach tej usługi jej użytkownicy mogą przesyłać obraz ze swoich kamer, dźwięk ze swoich mikrofonów, tekst (chat) i załączniki (pliki). Udostępniane są też różne funkcje zarządzania komunikacją przez organizatora wideokonferencji. W artykule opisano wyniki badania użyteczności wybranych funkcji płatnej usługi, ze względu na przydatność w prowadzeniu nauczania zdalnego na uczelni wyższej.

SŁOWA KLUCZOWE: Microsoft Teams, wideokonferencja, nauczanie zdalne

Wprowadzenie

Niniejszy artykuł został opracowany w związku z rosnącym zainteresowaniem wykorzystania usług wideokonferencyjnych do nauczania zdalnego w placówkach kształcenia. Na rynku dostępnych jest kilka usług wideokonferencyjnych, a wśród przodujących dostawców znajdują się takie firmy, jak: Microsoft (Microsoft Teams), Cisco (Cisco Webex), Zoom (Zoom 5.0). W artykule przedstawiono wyniki badań użyteczności aplikacji Microsoft Teams do nauczania zdalnego na uczelni wyższej. Badania przeprowadzono w ramach przedmiotu „zarządzanie bezpieczeństwem informacji" na I semestrze studiów II stopnia. W artykule zamieszczono także, opracowane przy okazji

badań, instrukcje pomocne w organizacji zajęć przez nauczycieli akademickich.

Wybór do badań Microsoft Teams (a nie np. Zoom) był podyktowany tym, że z firmą Microsoft Wojskowa Akademia Techniczna ma podpisane odpowiednie umowy i ma licencję na to oprogramowanie, co powoduje że właśnie Microsoft Teams są zalecane nauczycielom akademickim WAT do pracy zdalnej. Po „pandemicznym" semestrze zajęć można już stwierdzić, że pewne funkcje wbudowane w narzędzie, jak emotikony, dzienniczki ucznia itp. w pracy na uczelni wyższej są nieprzydatne. Również integracja z różnymi programami ma drugorzędne znaczenie. Istotne natomiast są możliwości wideokonferencyjne: sesje z kamerą i mikrofonem (w różnych wariantach) z grupami liczącymi często powyżej stu uczestników oraz udostępnianie i przechowywanie w ramach Microsoft Teams plików, w tym plików wideokonferencji[1]. Istotne znaczenie ma także łatwość organizacji zajęć, na co składa się wpisywanie uczestników sesji, powiadamianie, dołączanie nowych uczestników itp. Z tego powodu zostały przebadane przede wszystkim możliwości użytkowe narzędzia (stąd w tytule „analiza użyteczności"), a wyniki tych badań wraz z komentarzami przedstawiono w tym artykule. Szeroko rozumiane bezpieczeństwo oferowane w ramach usługi Microsoft Teams [6] będzie przedmiotem innych badań.

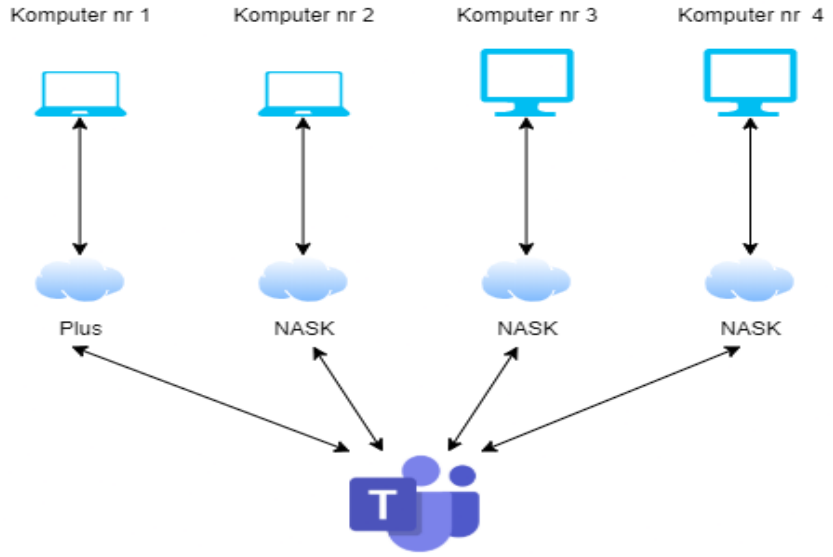
1. Środowisko badawcze

1.1. Przedmiot badania

Przedmiotem badania była aplikacja desktopowa Microsoft Teams w wersji 1.3.00.13565 (64 bity – ostatnia aktualizacja w dniu 02.06.2020 r.) wykorzystywana jako narzędzie komunikacyjne do nauczania zdalnego na uczelni wyższej.

[1] Te ostatnie funkcje są niezbędne do rozliczania zajęć dydaktycznych.

1.2. Schemat środowiska badawczego



Rys. 1. Schemat środowiska badawczego

1.3. Opis środowiska badawczego

Środowisko badawcze składało się z trzech uczestników i jednego organizatora sesji w nowo założonym zespole. W zależności od konkretnego badania, role członków zespołu ulegały zmianie. Komputery znajdowały się w tym samym budynku, ale w oddzielnych pomieszczeniach. Trzy komputery korzystały z połączenia internetowego dostarczanego przez NASK, natomiast jeden komputer korzystał z Internetu mobilnego, którego dostawcą była firma Polkomtel. Każda stacja robocza uczestnicząca w badaniu miała zainstalowany systemem Windows 10 Pro, desktopową aplikację Microsoft Teams w wersji 1.3.00.13565 oraz studencką subskrypcję pakietu Office 365. Konfiguracja aplikacji MS Teams była identyczna na każdym z komputerów. Zastosowane ustawienia były następujące:

- aplikacja nie uruchamia się automatycznie z systemem;
- język jest ustawiony na polski;
- przyśpieszenie sprzętowe procesora GPU jest włączone;
- żadne kontakty nie są zablokowane;
- aplikacja posiada uprawnienia do kamery, mikrofonu, głośników, wyświetlania powiadomień, linków zewnętrznych i urządzeń MIDI.

1.4. Ewidencja zasobów użytych w badaniu

Tab. 1. Arkusze opisu zasobów użytych w badaniu

Arkusz opisu komputera nr 1	
Identyfikator zasobu: K1	
Rodzaj komputera	Laptop
Model komputera	MSI CX61
Umiejscowienie komputera	Akademik Wojskowy
Model procesora	Intel Core I5-3210M
Ilość pamięci RAM	8 GB
Model karty graficznej	NVIDIA GeForce GT 640M
Nazwa dostawcy Internetu	Polkomtel
Prędkość pobierania[1]	3.26 Mbps
Prędkość wysyłania[1]	1.78 Mbps

Arkusz opisu komputera nr 2	
Identyfikator zasobu: K2	
Rodzaj komputera	Laptop
Model komputera	MSI GE60
Umiejscowienie komputera	Akademik Wojskowy
Model procesora	Intel Core i7-4720HQ
Ilość pamięci RAM	16 GB
Model karty graficznej	NVIDIA GeForce GTX 850M
Nazwa dostawcy Internetu	Naukowa i Akademicka Sieć Komputerowa
Prędkość pobierania[2]	5.53 Mbps
Prędkość wysyłania[2]	489.87 Mbps

Arkusz opisu komputera nr 3	
Identyfikator zasobu: K3	
Rodzaj komputera	Stacjonarny
Model komputera	-
Umiejscowienie komputera	Akademik Wojskowy
Model procesora	AMD Ryzen 5 2600
Ilość pamięci RAM	16 GB
Model karty graficznej	NVIDIA GeForce RTX 2070
Nazwa dostawcy Internetu	Naukowa i Akademicka Sieć Komputerowa
Prędkość pobierania[2]	5.34 Mbps
Prędkość wysyłania[2]	482.12 Mbps

[2] Sprawdzenie prędkości łącza odbywało się kilkukrotnie, bezpośrednio przed każdym z badań, a przedstawione wyniki to wartości średnie tych pomiarów.

Arkusz opisu komputera nr 4	
Identyfikator zasobu: K4	
Rodzaj komputera	Stacjonarny
Model komputera	-
Umiejscowienie komputera	Akademik Wojskowy
Model procesora	Intel Core i7-6700k
Ilość pamięci RAM	32 GB
Model karty graficznej	NVIDIA GeForce GTX 1060
Nazwa dostawcy Internetu	Naukowa i Akademicka Sieć Komputerowa
Prędkość pobierania[2]	5.21 Mbps
Prędkość wysyłania[2]	469.96 Mbps

2. Badanie użyteczności narzędzia komunikacyjnego Microsoft Teams do nauczania zdalnego na uczelni wyższej

2.1. Ewidencja hipotez badawczych poddanych weryfikacji

Tab. 2. Hipotezy badawcze poddane weryfikacji

Identyfikator badania	Hipoteza badawcza	Czy istnieje możliwość realizacji ?	Sposób realizacji
FH.1.1	Czy osoba spoza organizacji (WAT) może dołączyć do zespołu MS Teams?	Da się zrealizować	FR.1.1
FH.2.1	Czy istnieje możliwość pobrania listy obecności uczestników biorących udział w spotkaniu?	Da się zrealizować	FR.2.1
Identyfikator badania	**Hipoteza badawcza**	**Czy istnieje możliwość realizacji?**	**Sposób realizacji**
FH.3.1	Czy istnieje możliwość importowania listy członków zespołu/kanału?	Da się zrealizować	FR.3.1
FH.4.1	Czy istnieje możliwość udostępniania plików tylko wybranej grupie osób?	Da się zrealizować	FR.4.1
FH.5.1	Czy istnieje możliwość zmiany typu kanału z prywatnego na ogólny i na odwrót?	Nie da się zrealizować	-------
FH.6.1	Czy istnieje możliwość nagrywania i edycji materiałów nagranych podczas spotkania na kanale prywatnym?	Nie da się zrealizować	-------

BH.1.1	Czy organizator spotkania może zablokować rolę prezentera uczestnikom spotkania (dla spotkań organizowanych dla kanałów)?	Da się zrealizować	BR.1.1

2.2. Protokoły z przeprowadzonych badań

Tab. 3. Protokół badania FH.1.1

Identyfikator badania: FH.1.1	
Kategoria badawcza:	użyteczność funkcjonalna
Hipoteza badawcza:	Czy osoba spoza organizacji (WAT) może dołączyć do zespołu MS Teams?
Scenariusz badania:	Członek zespołu („Zadanie badawcze ZBI"), który posiada uprawnienia do dodawania nowych użytkowników do zespołu, spróbuje dodać nową osobę spoza organizacji WAT. W tym celu przy użyciu usługi, jaką oferuje strona *www.temp-mail.org* zostanie utworzony tymczasowy adres e-mail dla osoby spoza organizacji WAT. Członek zespołu spróbuje dodać nową osobę przy użyciu wygenerowanego wcześniej tymczasowego adresu e-mail.
Data badania:	27.06.2020, 19:30 – 20:00
Zasoby uczestniczące w badaniu:	K3 / Krzysztof Kabacki
Wynik badania:	Da się zrealizować
Sposób realizacji:	FR.1.1

Tab. 4. Protokół badania FH.2.1

Identyfikator badania: FH.2.1	
Kategoria badawcza:	użyteczność funkcjonalna
Hipoteza badawcza:	Czy istnieje możliwość pobrania listy obecności uczestników biorących udział w spotkaniu?
Scenariusz badania:	Organizator spotkania spróbuje pobrać listę obecności uczestników spotkania. W tym celu organizator zaplanuje spotkanie dla kanału ogólnego zespołu „Zadanie badawcze ZBI". Następnie pięć minut po rozpoczęciu spotkania spróbuje pobrać listę obecności osób aktualnie uczestniczących w spotkaniu.
Data badania:	17.06.2020, 13.50-14.10
Zasoby uczestniczące w badaniu:	K1 / Adam Abacki K2 / Borys Babacki K3 / Krzysztof Kabacki K4 / Natalia Nowacka
Wynik badania:	Da się zrealizować
Sposób realizacji:	FR.2.1

Tab. 5. Protokół badania FH.3.1

Identyfikator badania: FH.3.1	
Kategoria badawcza:	użyteczność funkcjonalna
Hipoteza badawcza:	Czy istnieje możliwość importowania listy członków zespołu/kanału?
Scenariusz badania:	Członek zespołu („Zadanie badawcze ZBI"), który posiada uprawnienia do dodawania nowych użytkowników, spróbuje w pierwszej kolejności wykonać import listy członków zespołu (potok szkoleniowy). Następnie, spróbuje dokonać importu listy członków dla kanału (grupa szkoleniowa – ćwiczenia).
Data badania:	25.06.2020, 13.00-14.00
Zasoby uczestniczące w badaniu:	K3 / Krzysztof Kabacki
Wynik badania:	Da się zrealizować
Sposób realizacji:	FR.3.1

Tab. 6. Protokół badania FH.4.1

Identyfikator badania: FH.4.1	
Kategoria badawcza:	użyteczność funkcjonalna
Hipoteza badawcza:	Czy istnieje możliwość udostępniania plików tylko wybranej grupie osób?
Scenariusz badania:	Członek zespołu udostępniający materiały szkoleniowe chce ograniczyć możliwość dostępu do zasobów tylko dla wybranej grupy osób. W tym celu członek zespołu opublikuje na kanale ogólnym zespołu („Zadanie badawcze ZBI") plik, a następnie spróbuje ograniczyć dostęp do tego pliku. Prawo do odczytu pliku będzie miało konto osoby spoza organizacji WAT.
Data badania:	28.06.2020, 13.00-14.00
Zasoby uczestniczące w badaniu:	K3 / Krzysztof Kabacki K4 / Natalia Nowacka
Wynik badania:	Da się zrealizować
Sposób realizacji:	FR.4.1

Tab. 7. Protokół badania FH.5.1

Identyfikator badania: FH.5.1	
Kategoria badawcza:	użyteczność funkcjonalna
Hipoteza badawcza:	Czy istnieje możliwość zmiany typu kanału z prywatnego na ogólny i na odwrót?
Scenariusz badania:	Administrator zespołu utworzy nowy kanał prywatny, a następnie spróbuje zmienić jego typ na kanał ogólny.
Data badania:	19.06.2020, 13.30-14.00
Zasoby uczestniczące w badaniu:	K3 / Krzysztof Kabacki
Wynik badania:	Nie da się zrealizować
Sposób realizacji:	**Brak takiej funkcji w aplikacji MS Teams. Brak takiej możliwości przy użyciu interpretera poleceń PowerShell i modułu „MircosoftTeams". Funkcja nie została jeszcze zaimplementowana.**

Tab. 8. Protokół badania FH.6.1

Identyfikator badania: FH.6.1	
Kategoria badawcza:	użyteczność funkcjonalna
Hipoteza badawcza:	Czy istnieje możliwość nagrywania i edycji materiałów nagranych podczas spotkania na kanale prywatnym?
Scenariusz badania:	Osoba prowadząca spotkanie nagra je, a następnie spróbuje dokonać edycji nagranego materiału.
Data badania:	22.06.2020, 17.00-17.30
Zasoby uczestniczące w badaniu:	K1 / Adam Abacki K2 / Borys Babacki K3 / Krzysztof Kabacki K4 / Natalia Nowacka
Wynik badania:	Nie da się zrealizować
Sposób realizacji:	**Brak takiej funkcji w aplikacji MS Teams. Tylko kanały ogólne dopuszczają możliwość nagrywania spotkania. Aplikacja Microsoft Stream umożliwia edycję nagranych materiałów.**

Tab. 9. Protokół badania BH.1.1

Identyfikator badania: BH.1.1	
Kategoria badawcza:	użyteczność funkcjonalna
Hipoteza badawcza:	Czy organizator spotkania może zablokować rolę prezentera uczestnikom spotkania (w przypadku spotkań organizowanych dla kanałów)?
Scenariusz badania:	Członek zespołu („Zadanie badawcze ZBI”) planuje spotkanie dla kanału, a następnie próbuje modyfikować role zaproszonych – nadać każdemu zaproszonemu domyślną rolę uczestnika.
Data badania:	19.06.2020, 22.00-22.30
Zasoby uczestniczące w badaniu:	K4 / Natalia Nowacka
Wynik badania:	Da się zrealizować
Sposób realizacji:	BR.1.1

3. Instrukcje sposobu realizacji wybranych czynności w aplikacji MS Teams

Zamieszczone w tabelach 10-14 instrukcje wykonania wybranych czynności weryfikowanych w badaniach, są oznaczone jako FR.x.x odpowiednio do badanych hipotez FH.x.x oraz BH.1.1 jako BR.1.1.

Tab. 10. Instrukcja realizacji czynności FR.1.1 w aplikacji MS Teams

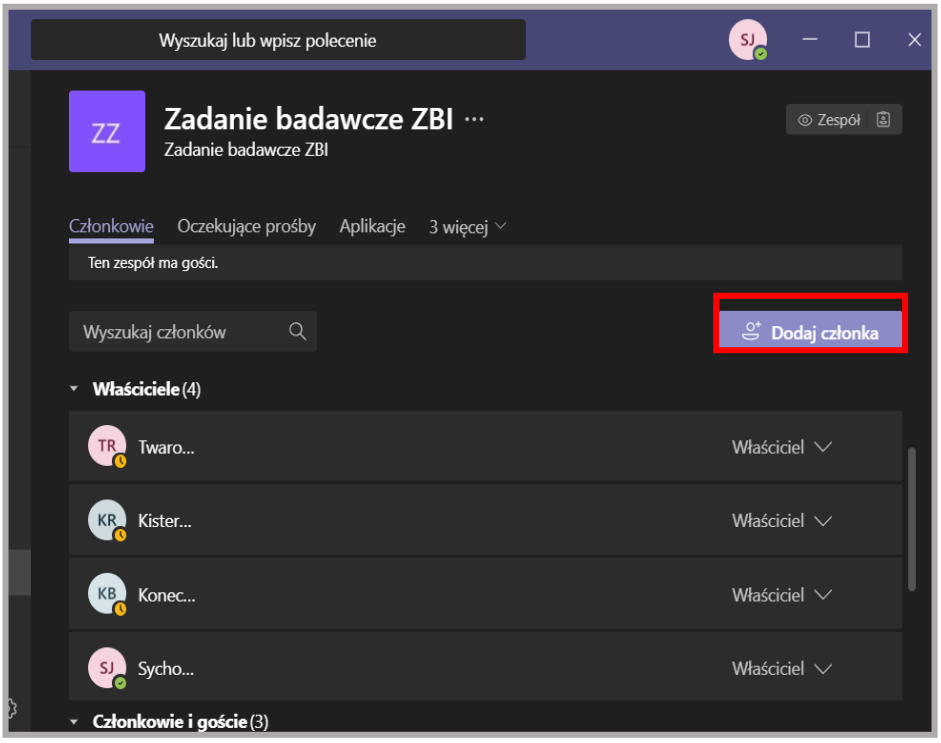
Arkusz sposobu realizacji nr 1	
Identyfikator sposobu realizacji: FR.1.1	
Identyfikator badania: FH.1.1	
Hipoteza badawcza:	Czy osoba spoza organizacji (WAT) może dołączyć do zespołu MS Teams?

Scenariusz realizacji:

Uczestniczące strony:

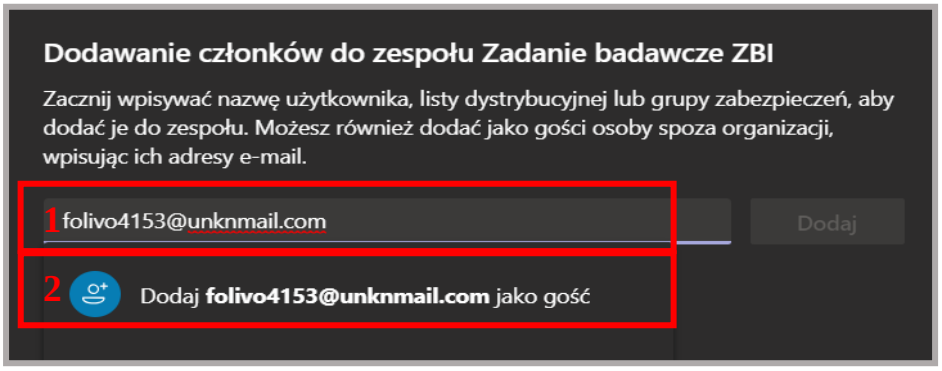
- administrator zespołu – członek zespołu (posiadający uprawnienia do dodawania nowych członków zespołu;
- nowy członek – osoba spoza organizacji.

1. Administrator zespołu, poprzez przycisk „Dodaj członka” ma możliwość dodania nowego członka do zespołu MS Teams.

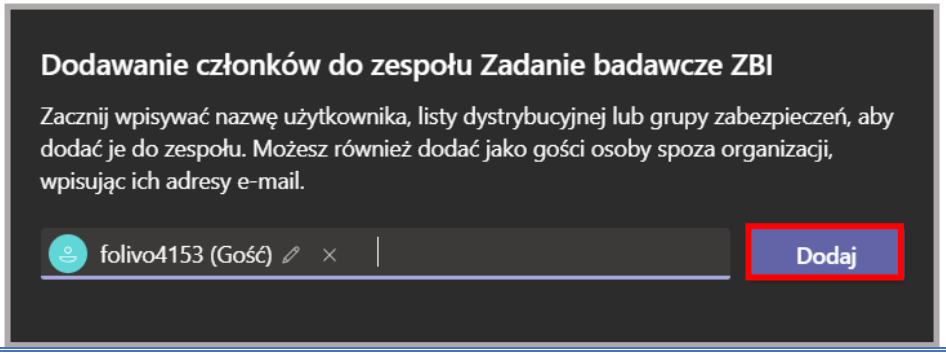


2. Na przykład, nowy członek ma adres skrzynki pocztowej.

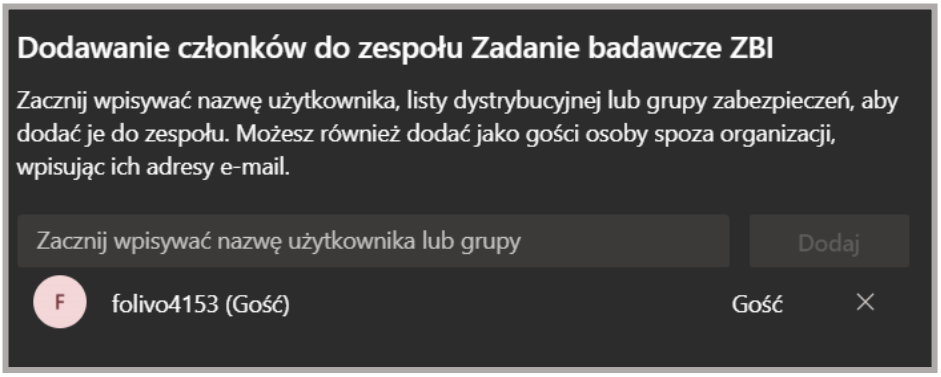
3. Naciśnięcie przycisku opisanego w punkcie pierwszym spowoduje wywołanie pola dodawania nowych członków do wybranego zespołu. Administrator zespołu w polu tekstowym oznaczonym na poniższym rysunku numerem 1 musi podać adres e-mail osoby spoza organizacji, w tym przypadku jest to adres *folivo4153@unknmail.com*. Następnie, poniżej pola tekstowego z adresem e-mail, ukaże się pole, które daje możliwość dodania nowego członka jako gościa (pole o numerze 2) − należy nacisnąć to pole.



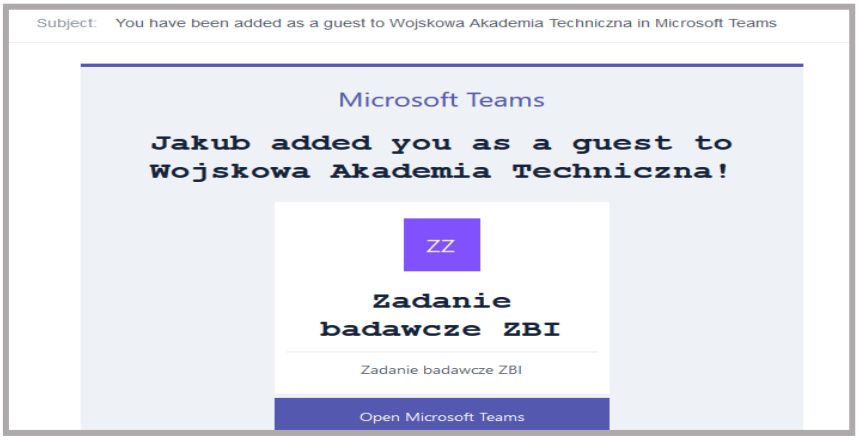
4. Następnie należy nacisnąć przycisk „Dodaj”.



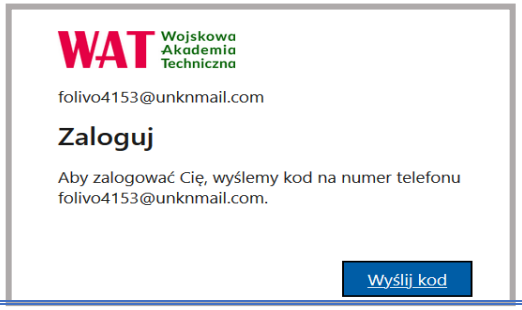
Na tym kończą się czynności, jakie musi wykonać administrator zespołu w celu dodania nowego członka spoza organizacji.



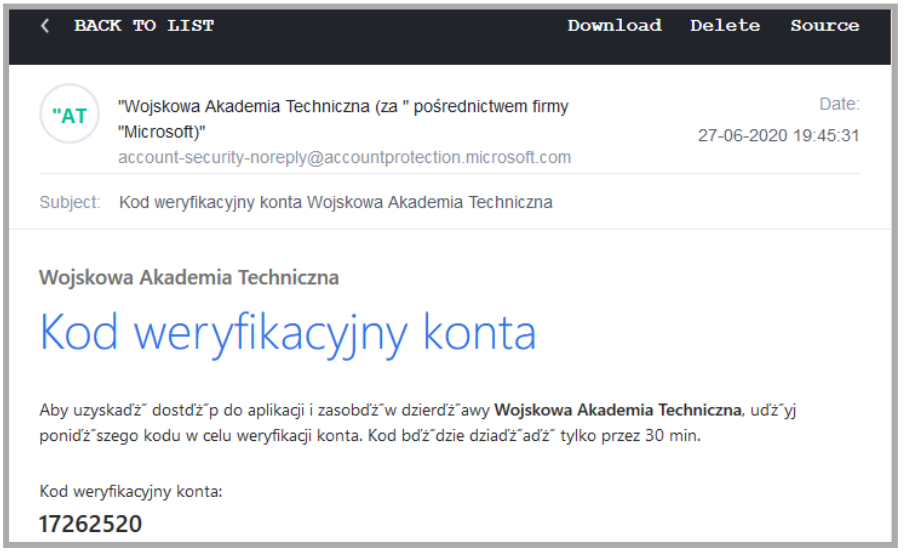
5. Po dodaniu nowego członka do zespołu, na jego skrzynkę pocztową jest przesłana poniższa wiadomość.



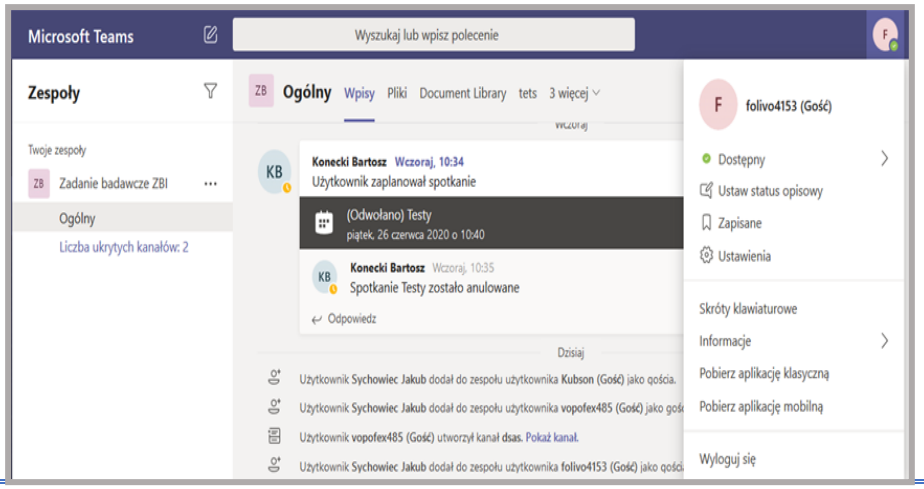
Naciśnięcie przycisku „Open Microsoft Teams” przekieruje nowego członka do panelu logowania organizacji WAT.



6. Uwierzytelnienie nowego członka w organizacji WAT jest realizowane przy użyciu jednorazowego, 8-cyfrowego kodu, aktywnego przez 30 minut.
7. Wiadomość z jednorazowym kodem jest przesyłana na skrzynkę pocztową osoby spoza organizacji.



8. Po wprowadzeniu jednorazowego kodu, nowy członek ma dostęp do zespołu MS Teams.



Tab. 11. Instrukcja realizacji czynności FR.2.1 w aplikacji MS Teams

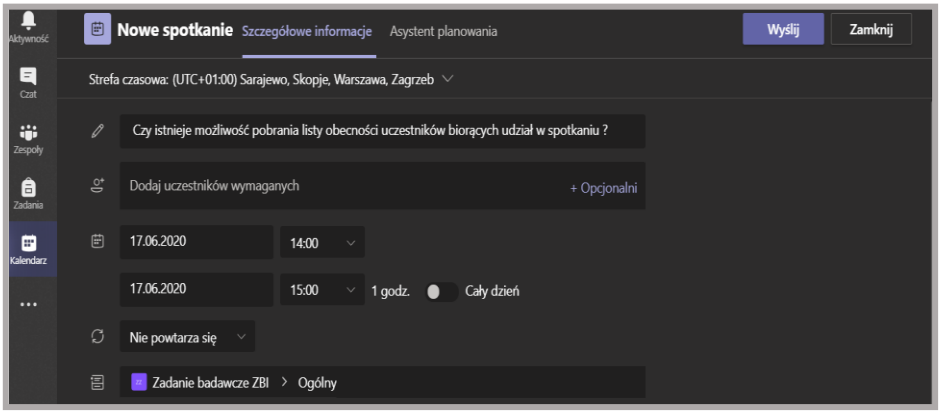
Arkusz sposobu realizacji nr 2	
Identyfikator sposobu realizacji: FR.2.1	
Identyfikator badania: FH.2.1	
Hipoteza badawcza:	Czy istnieje możliwość pobrania listy obecności uczestników biorących udział w spotkaniu?

Scenariusz realizacji:

Uczestniczące strony:

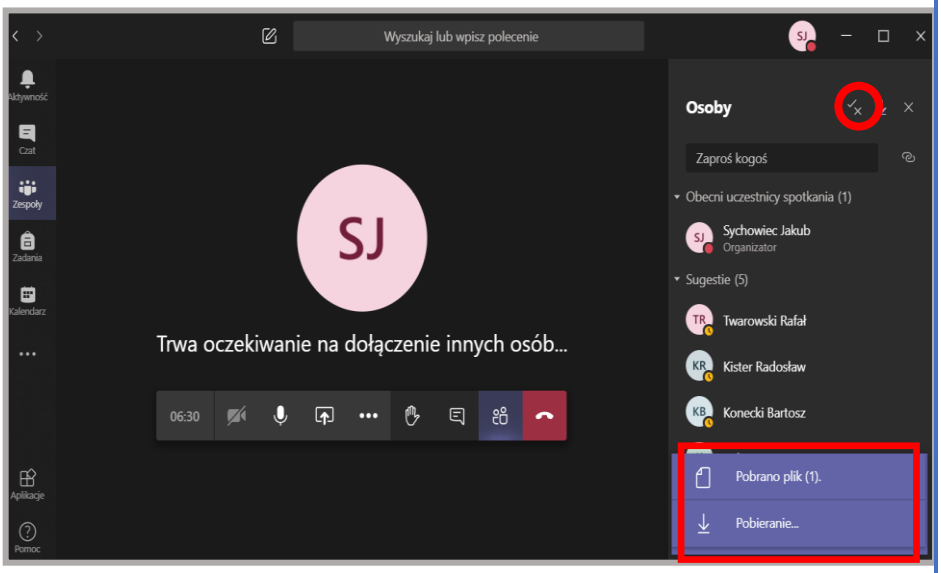
- organizator spotkania – członek zespołu, który zaplanował spotkanie;
- uczestnicy spotkania – członkowie wybranego kanału.

1. Organizator spotkania zaplanował nowe spotkanie na dzień 17.06.2020, które rozpocznie się o godzinie 14.00. Jako uczestników spotkania wskazał wszystkie osoby należące do zespołu „Zadanie badawcze ZBI”.

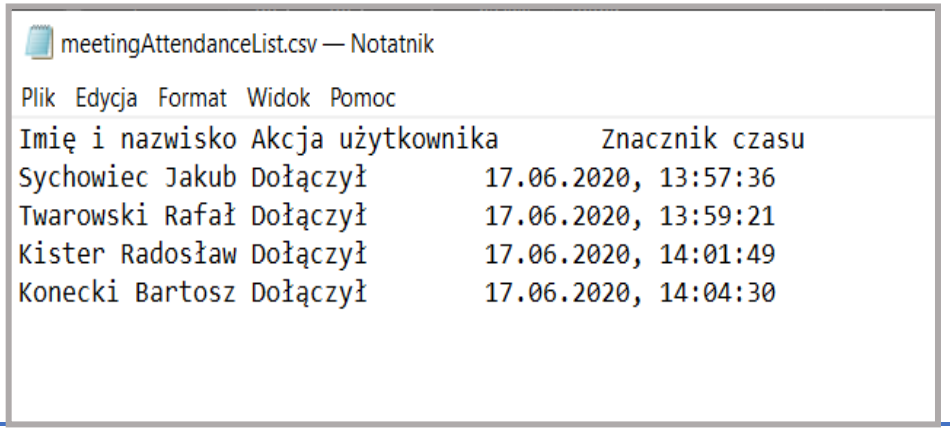


2. Organizator spotkania rozpoczął zaplanowane spotkanie.

3. W celu pobrania listy obecności uczestników spotkania należy nacisnąć przycisk zaznaczony na poniższym rysunku czerwonym okręgiem.



4. Plik w formacie .CSV z listą obecności został zapisany w folderze „Pobrane”. Domyślna nazwa pliku: meetingAttendanceList.csv. Plik zawiera listę wszystkich osób uczestniczących w spotkaniu wraz z datą dołączenia do spotkania.



Tab. 12. Instrukcja realizacji czynności FR.3.1 w aplikacji MS Teams

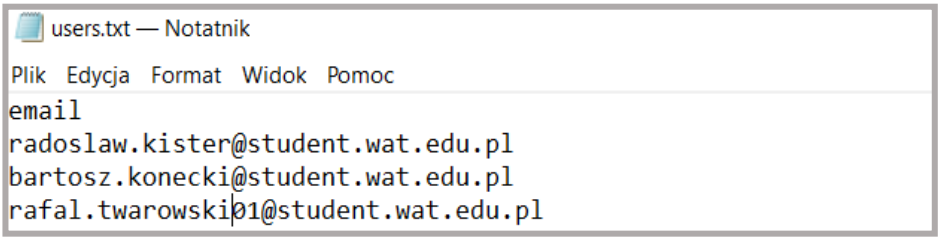
Arkusz sposobu realizacji nr 3	
Identyfikator sposobu realizacji: FR.3.1	
Identyfikator badania: FH.3.1	
Hipoteza badawcza:	Czy istnieje możliwość importowania listy członków zespołu/kanału?

Scenariusz realizacji (wymaga użycia interpretera poleceń PowerShell ISE oraz zainstalowania modułu *MicrosoftTeams*):

Uczestniczące strony:

- administrator zespołu − członek zespołu (posiadający uprawnienia do dodawania nowych członków zespołu.

1. Administrator zespołu musi przygotować listę adresów skrzynek pocztowych przyszłych członków zespołu/kanału, tak jak to przedstawiono poniżej:



2. Następnie z poziomu PowerShell ISE (uruchomić jako administrator) należy zainstalować moduł *MicrosoftTeams*. Służą do tego poniższe instrukcje:
   1) Register-PSRepository -Name PSGalleryInt -SourceLocation https://www.poshtestgallery.com/ -InstallationPolicy Trusted
   2) Install-Module -Name MicrosoftTeams -RequiredVersion 1.0.25 -Repository 'PSGalleryInt'
   3) Get-Module -ListAvailable -Name MicrosoftTeams
   4) Set-ExecutionPolicy -ExecutionPolicy RemoteSigned
   5) Import-Module MicrosoftTeams

Instrukcja 1): rejestruje repozytorium, na którym znajduje się moduł „MicrosofTeams";

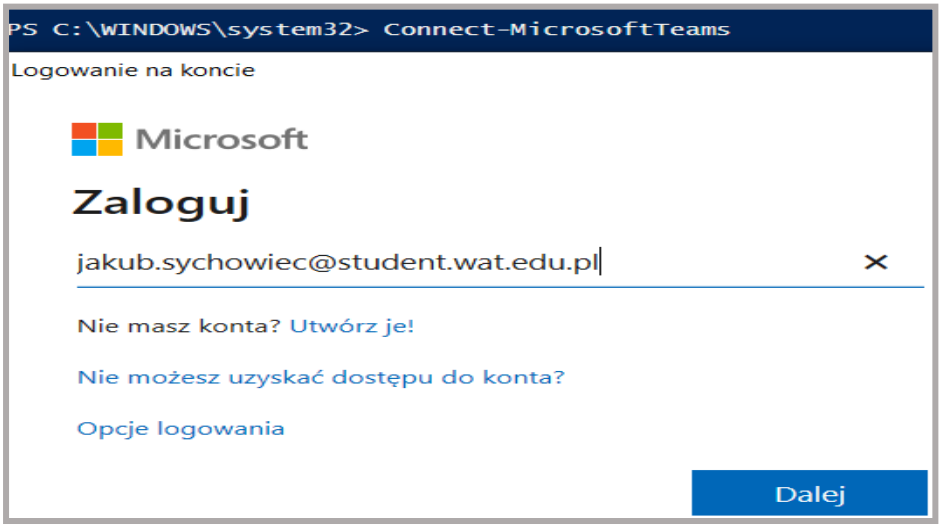
Instrukcja 2): instaluje moduł; w tym przypadku jest to wersja 1.0.25;

Instrukcja 3): sprawdza poprawność instalacji modułu;

Instrukcja 4): włącza możliwości wykonywania pobranych skryptów podpisanych przez zaufanych dostawców (po wykonaniu tej komendy należy ponownie uruchomić interpreter PowerShell ISE);

Instrukcja 5): ładuje moduł *MicrosoftTeams* do pamięci.

3. Po zainstalowaniu modułu *MicrosoftTeams* należy nawiązać połączenie z usługą Microsoft Teams za pomocą instrukcji: Connect-MicrosoftTeams



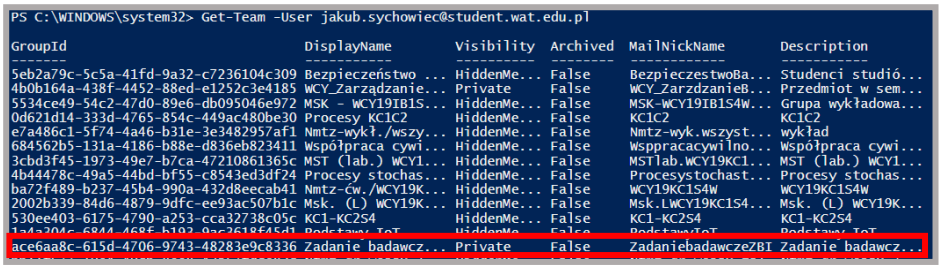

```
PS C:\WINDOWS\system32> Connect-MicrosoftTeams


Account      : jakub.sychowiec@student.wat.edu.pl
Environment  : AzureCloud
Tenant       : e66af1e9-d714-4a1f-8101-22a504f9622f
TenantId     : e66af1e9-d714-4a1f-8101-22a504f9622f
TenantDomain : student.wat.edu.pl
```

4. Następną czynnością jest pobranie identyfikatora zespołu. Służy do tego poniższa instrukcja: Get-Team -User Jakub.sychowiec@student.wat.edu.pl

   Należy zastosować parametr *-User*, a jako argument adres pocztowy użytkownika. Użycie komendy *Get-Team* bez parametru spowoduje próbę pobrania wszystkich zespołów utworzonych w organizacji użytkownika (może to trwać bardzo długo, a wynikiem końcowym będzie lista błędów, informujących o braku dostępu).

Poniższy rysunek przedstawia przykładowy wynik wykonania instrukcji. Czerwonym prostokątem zaznaczono identyfikator zespołu, który zostanie wykorzystany do realizacji następnych czynności.



5. Identyfikator wybranego zespołu należy skopiować lub przypisać do zmiennej środowiskowej, będzie on niezbędny podczas wykonywania kolejnych komend. Poniżej przedstawiono i opisano instrukcje, które umożliwiają zaimportowanie listy członków do całego zespołu lub wybranego kanału prywatnego:

    a) Import listy członków do zespołu:

        1) Import-Csv –Path “ścieżka_dostępu_do_pliku .CSV” | foreach{Add-TeamUser -GroupId ace6aa8c-615d-4706-9743-48283e9c8336 -User $_.email}
        2) Get-TeamUser -GroupId ace6aa8c-615d-4706-9743-48283e9c8336

    Instrukcja 1): importuje listę członków do zespołu;

    Instrukcja 2): weryfikuje, czy lista została zaimportowana poprawnie.

    b) Import listy członków do kanału ukrytego:

        1) Get-TeamChannel -GroupId ace6aa8c-615d-4706-9743-48283e9c8336
        2) Import-Csv -Path "ścieżka_dostępu_do_pliku .CSV " | foreach{Add-TeamChannelUser -GroupId ace6aa8c-615d-4706-9743-48283e9c8336 -DisplayName "Ćwiczenia - grupa szkoleniowa K9C1S4" -User $_.email}
        3) Get-TeamChannelUser -GroupId ace6aa8c-615d-4706-9743-48283e9c8336 -DisplayName "Ćwiczenia - grupa szkoleniowa K9C1S4"

    Instrukcja 1): wyświetlenie listy utworzonych kanałów publicznych i prywatnych w zespole.

    Instrukcja 2): import listy członków do ukrytego kanału; po parametrze – *DisplayName* należy przekazać nazwę ukrytego kanału.

    Instrukcja 3): weryfikacja, czy lista została zaimportowana poprawnie.

Tab. 13. Instrukcja realizacji czynności FR.4.1 w aplikacji MS Teams

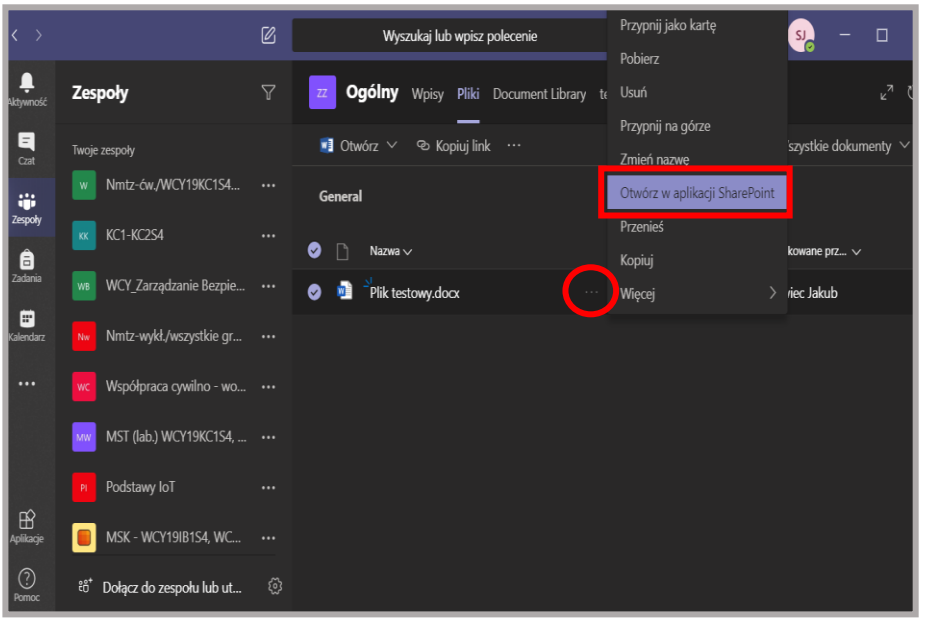
Arkusz sposobu realizacji nr 4	
Identyfikator sposobu realizacji: FR.4.1	
Identyfikator badania: FH.4.1	
Hipoteza badawcza:	Czy istnieje możliwość udostępniania plików tylko wybranej grupie osób?

Scenariusz realizacji:

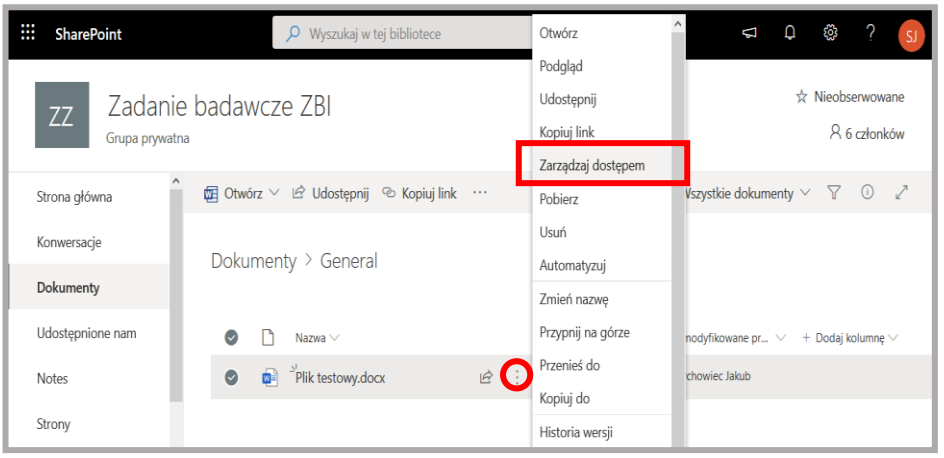
Uczestniczące strony:

- administrator zespołu – członek zespołu, posiadający uprawnienia do dodawania nowych członków zespołu;
- konto gościa – osoba spoza organizacji WAT, której został przydzielony dostęp tylko do odczytu opublikowanego pliku;
- konto członka zespołu – osoba z organizacji WAT, która nie posiada dostępu do opublikowanego pliku.

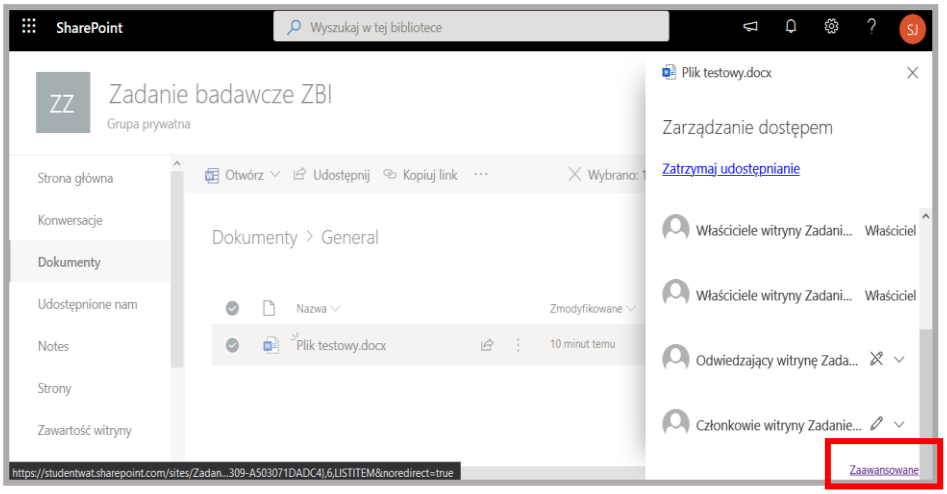
1. Warunek wstępny: Administrator zespołu opublikował plik na kanale ogólnym zespołu. Następnie należy rozwinąć listę dostępnych opcji dla nowo opublikowanego pliku. Z listy wybrać opcję *Otwórz w aplikacji SharePoint*. Opcja ta przekierowuje administratora zespołu na stronę internetową *Share Point*, z której administrator ma więcej możliwości w zarządzaniu udostępnionymi plikami niż z poziomu aplikacji MS Teams.



2. Z poziomu aplikacji internetowej *Share Point* należy rozwinąć listę dostępnych opcji dla nowo opublikowanego pliku, a następnie wybrać opcję „Zarządzaj dostępem”.

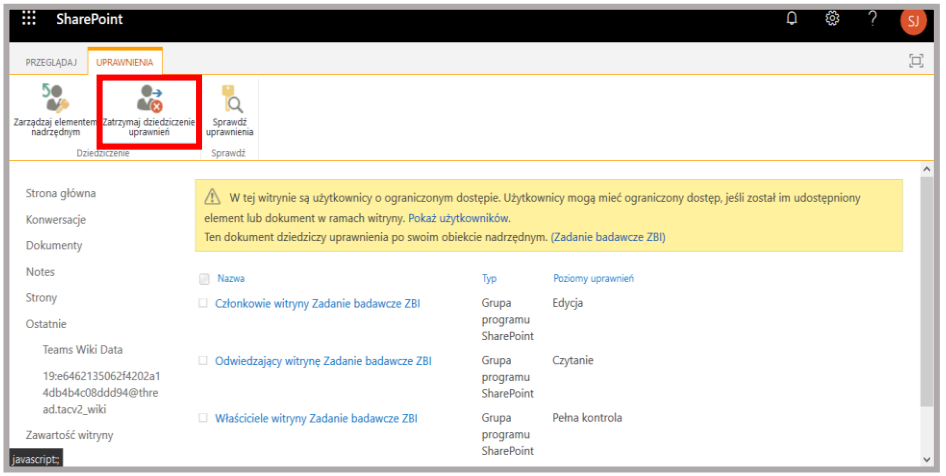


3. Z prawej strony zostanie wyświetlona lista kont, które posiadają aktualny dostęp do pliku wraz z przysługującymi im uprawnieniami. Z tego poziomu można edytować podstawowe uprawnienia kont do pliku, głównie zakres dostępu. W prawym dolnym rogu znajduje się opcja „Zaawansowane”, która przekierowuje użytkownika do rozbudowanego panelu zarządzania plikiem z dodatkowymi ustawieniami polityki dostępu.

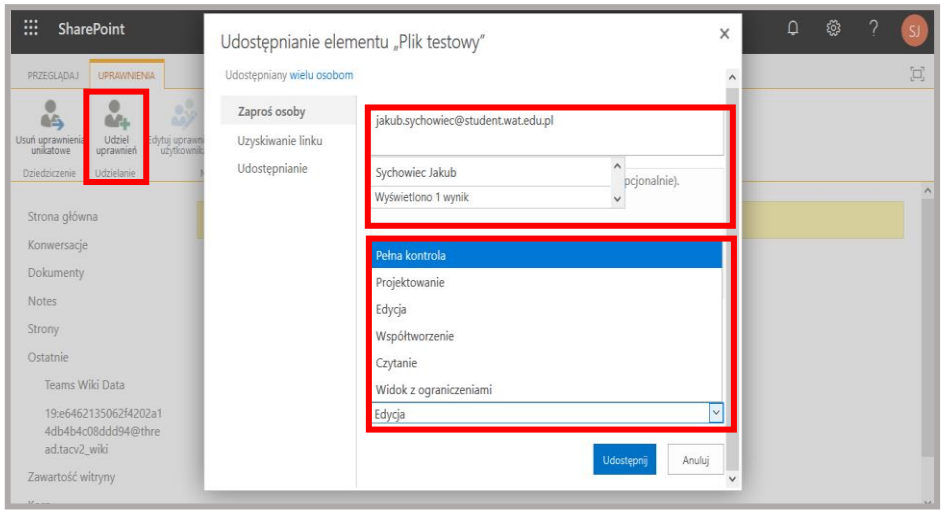


4. W celu zastosowania indywidualnych praw dostępu do pliku, należy w pierwszej kolejności „zatrzymać dziedziczenie uprawnień”. Dziedziczenie uprawnień ułatwia konfigurację polityki dostępu do zasobów w przypadku, gdy administrator zespołu chciałby utworzyć ukryte kanały dla wybranych grup

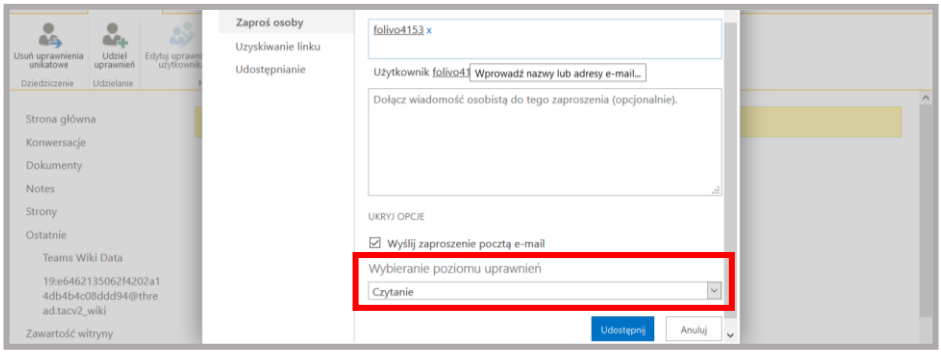
szkoleniowych. A następnie nadać uprawnienia dla folderu nadrzędnego wybranego kanału tak, aby tylko członkowie kanału mieli dostęp do umieszczonych w folderze kanału zasobów. Wszystkie zasoby umieszczone w takim folderze kanału odziedziczą jego uprawnienia. Z poniższego rysunku wynika, że dostęp do pliku mają: właściciele zespołu (pełna kontrola), członkowie zespołu (edycja), odwiedzający zespół (czytanie).



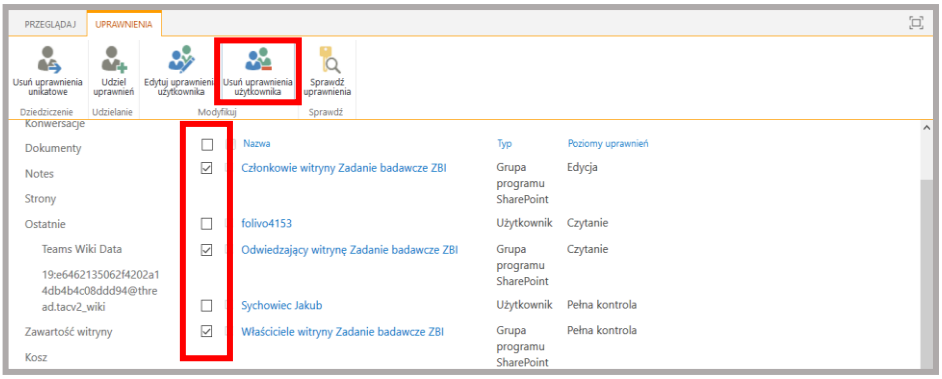
5. Po naciśnięciu przycisku *Zatrzymaj dziedziczenie uprawnień,* przycisk zostanie zastąpiony opcją *Udziel uprawnień*. Naciśnięcie tego przycisku otwiera pole, w którym administrator zespołu może przydzielić dostęp do zasobu wraz z zakresem uprawnień (pełna kontrola, projektowanie, edycja, współtworzenie, czytanie, widok z ograniczeniami). W pierwszej kolejności przyznano pełną kontrolę do pliku dla administratora zespołu.



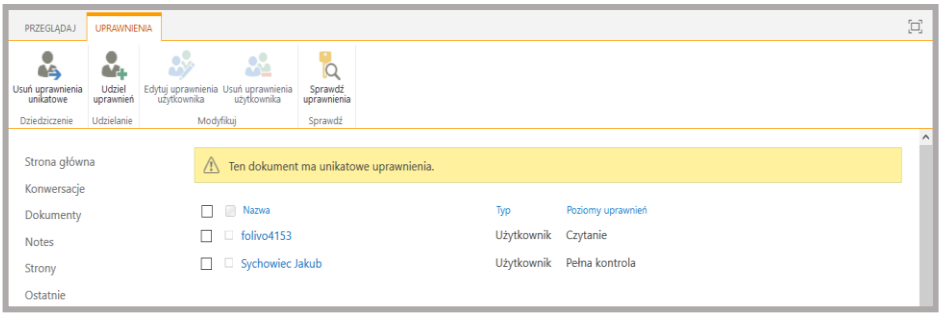
6. Następnie nadano uprawnienia do pliku dla konta gościa (*folivo453*), który ma prawo jedynie do odczytu opublikowanego pliku.



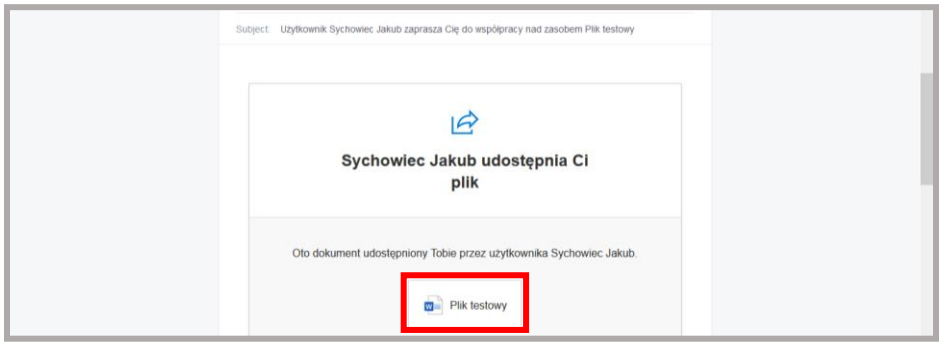
7. Po nadaniu odpowiednich uprawnień dla konta gościa, należy odebrać osobom uprawnienia, które zostały nadane w wyniku opcji dziedziczenia po folderze nadrzędnym. W tym celu należy zaznaczyć wybrane konta i użyć przycisku *Usuń uprawnienia użytkownika*.



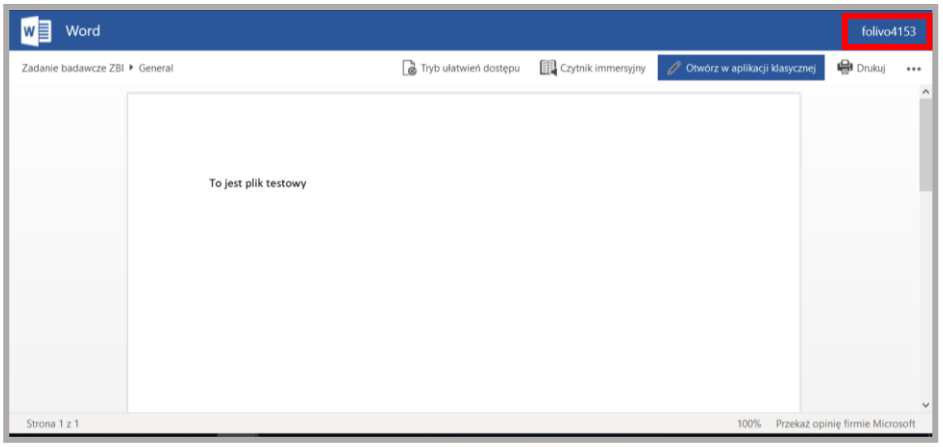
8. Po odebraniu uprawnień dla wybranych kont, dostęp do pliku ma konto: *Krzysztof Kabacki* i *folivo4153*.



9. Na skrzynkę pocztową konta gościa przesłana została wiadomość, poprzez którą konto gościa może uzyskać dostęp do opublikowanego pliku.



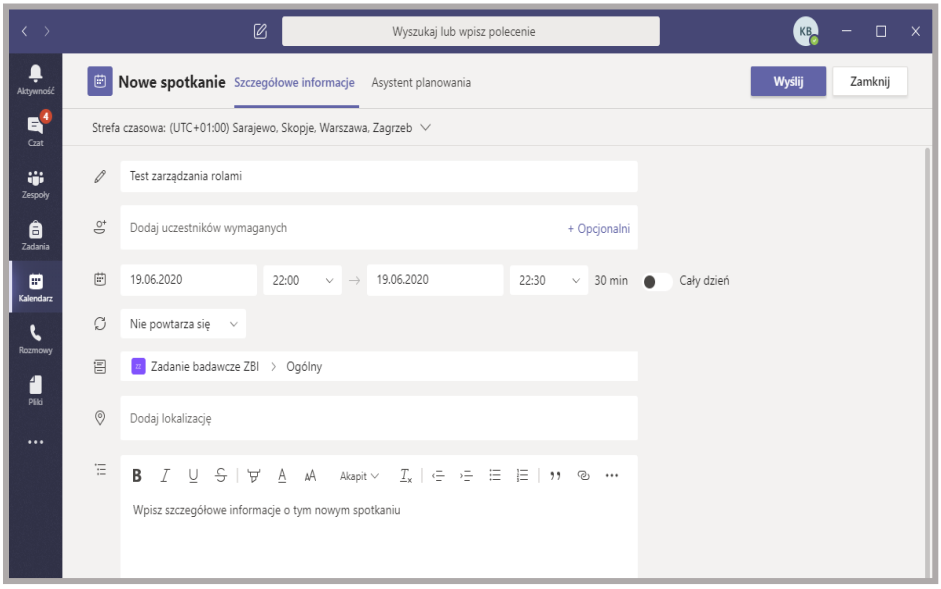
10. Po zalogowaniu się do konta gościa, przy użyciu jednorazowego, 8-cyfrowego kodu, gość może odczytać zawartość opublikowanego pliku.



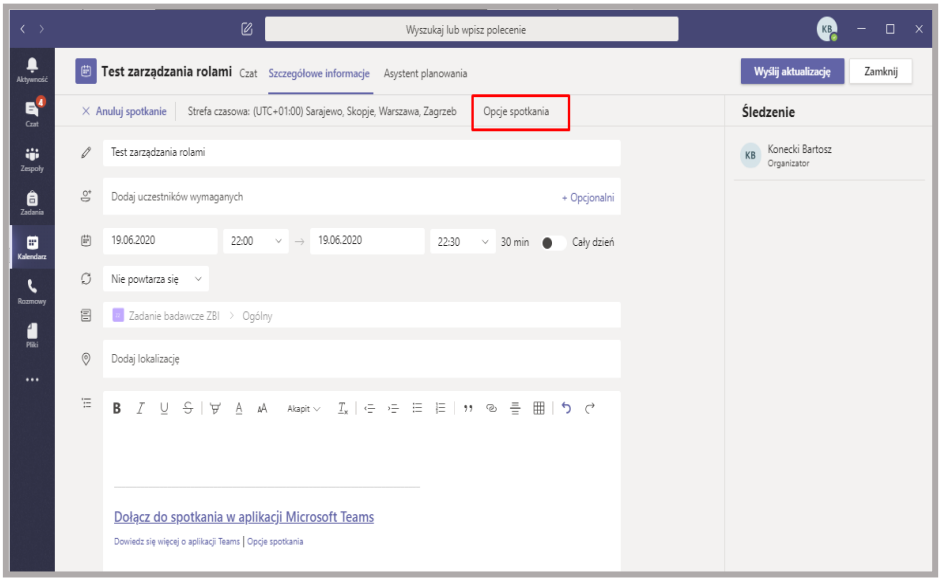
Tab. 14. Instrukcja realizacji czynności BR.1.1 w aplikacji MS Teams

Arkusz sposobu realizacji nr 5	
Identyfikator sposobu realizacji: BR.1.1	
Identyfikator badania: BH.1.1	
Hipoteza badawcza:	Czy organizator spotkania może zablokować rolę prezentera uczestnikom spotkania?
Scenariusz realizacji: Uczestniczące strony: • organizator spotkania – członek zespołu, który zaplanował spotkanie; • uczestnicy spotkania – członkowie wybranego kanału.	

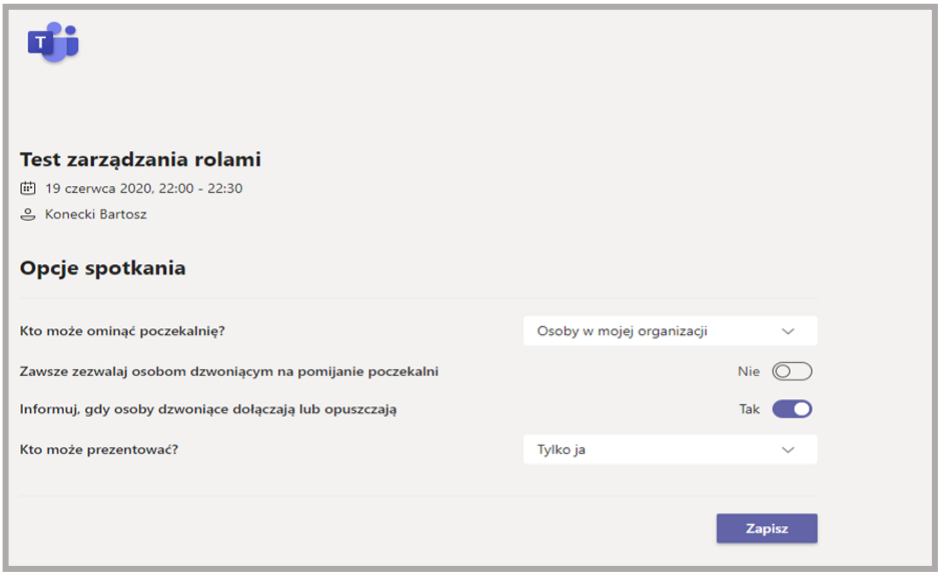
1. Organizator spotkania zaplanował nowe spotkanie na dzień 19.06.2020, które rozpocznie się o godzinie 22.00. Jako uczestników spotkania wskazał wszystkie osoby należące do zespołu *Zadanie badawcze ZBI*.

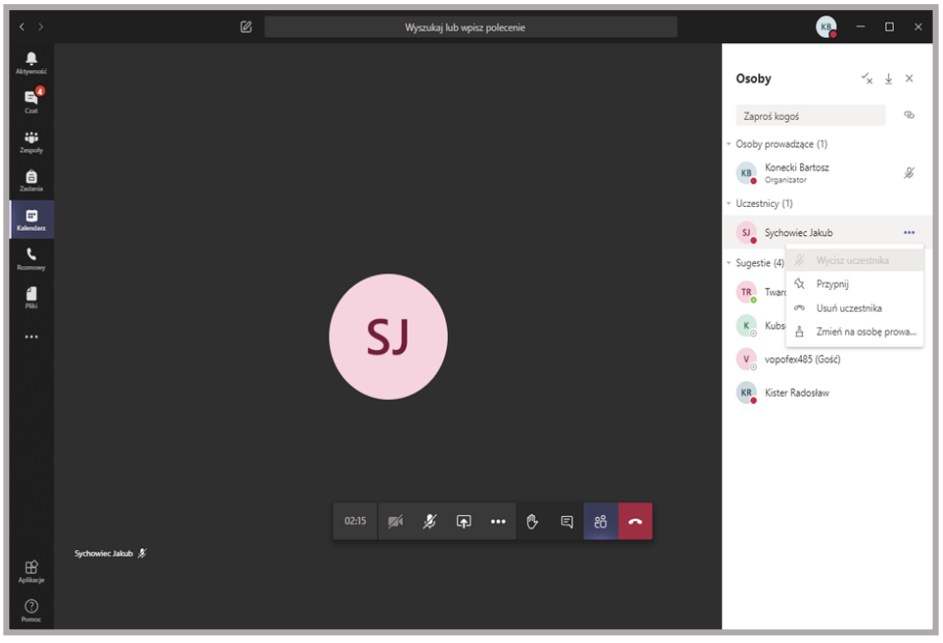


2. Organizator zmienia role zaproszonych osób na rolę uczestnika, poprzez zakładkę *Opcje spotkania*.



3. Dołączający do spotkania mają domyślnie nadaną nazwę uczestnika.





Wnioski

Na podstawie przeprowadzonych badań użyteczności narzędzia komunikacyjnego Microsoft Teams do nauczania zdalnego na uczelni wyższej stwierdzono, że narzędzie to nie jest wystarczająco przystosowane do prowadzenia zajęć zdalnych. Narzędzie nie ma funkcji ułatwiających pracę i zarządzanie grupami przez nauczycieli akademickich. Na przykład scenariusz, w którym nauczyciel chciałby utworzyć w szybki i skuteczny sposób zespół dla wybranego przedmiotu, składającego się z wielu potoków szkoleniowych (a w nim wielu członków), a następnie w ramach kanałów prywatnych utworzyć grupy ćwiczeniowe, jest trudny w realizacji i niemożliwy z poziomu aplikacji MS Teams − konieczne jest użycie interpretera PowerShell. Kolejną wadą jest brak możliwości nagrywania spotkania w kanałach prywatnych. Problem stanowi również brak przejrzystości i spójności instrukcji do narzędzia MS Teams oraz jej niepoprawne tłumaczenie na język polski (a raczej wygenerowanie tłumaczenia przez automat). Skutkuje to koniecznością dobrej znajomości języka angielskiego albo hiszpańskiego, aby móc skorzystać z rzetelnie wykonanej instrukcji obsługi narzędzia i usługi jako takiej.

Biorąc pod uwagę nie poddane badaniu bezpieczeństwo informacyjne (w tym RODO), należy zauważyć, że producent narzędzia poczuwa się i określa mianem administratora danych osobowych, spełnia wymogi RODO oraz dysponuje dużą ilością certyfikatów z rodziny ISO 27xxx i SOC [1], [2]. Tarcza Prywatności (Privacy Shield) US-UE oraz standardowe klauzule umowne (SCC) są podstawą prawną dla firmy Microsoft do transferu danych poza Europejski Obszar Gospodarczy (EOG) [5][3]. Firma Microsoft złożyła także deklarację, że jedynie dane techniczne oraz dane samych użytkowników są przesyłane poza EOG w celu optymalizacji i poprawy bezpieczeństwa, natomiast pozostałe dane (zapisy rozmów wideo, korespondencja) są przetwarzane w rejonowych centrach danych w pobliżu lokalizacji danego użytkownika (tj. centrach danych w Dublinie albo Amsterdamie). Zaletą MS Teams jest możliwość wykorzystania różnych typów uwierzytelniania, takich jak uwierzytelnianie wieloskładnikowe, czy uwierzytelnianie za pomocą single sign-on (SSO). Wadą − brak szyfrowania end-to-end podczas przesyłania danych jawnymi kanałami.

Konkludując, aplikacja MS Teams wraz z końcem kwietnia osiągnęła 75 milionów aktywnych, dziennych użytkowników na całym świecie [3]. Odnotowany wzrost był znaczący, ponieważ ze statystyk na dzień 11 marca wynika, że było to około 32 miliony użytkowników, a 18 marca już 44 miliony. Na tak znaczący wzrost zainteresowania aplikacją firmy Microsoft niewątpliwie

[3] W efekcie wyroku Trybunału Sprawiedliwości UE (TSUE) wydanego 16 lipca 2020 r. (sprawa Schrems II), czyli po złożeniu w Wydawnictwie niniejszego artykułu, ten zapis jest nieaktualny.

miała wpływ pandemia COVID-19, która zmusiła nie tylko uczelnie wyższe do przejścia z tradycyjnej formy prowadzenia zajęć na pracę zdalną. Tak duży wzrost użytkowników zaskoczył firmę Microsoft, ponieważ w połowie marca pojawiły się w Europie duże problemy z działaniem aplikacji. Sama platforma była dostosowywana i aktualizowana na bieżąco, tak aby była uniwersalna i mogła sprostać wymaganiom stawianym przez użytkowników zarówno biznesowych, jak i akademickich. Takie działanie (tj. częste aktualizowanie aplikacji i problemy ze stabilnością) świadczą o tym, że Microsoft nie był przygotowany na tak duże zainteresowanie aplikacją, a w szczególności wykorzystaniem jej w celu nauki zdalnej. Należy zaznaczyć, że MS Teams jest stale rozwijanym narzędziem. Powstała specjalna platforma [4] *https://microsoftteams.uservoice.com* dla użytkowników Teams, na której użytkownicy mogą zamieszczać swoje sugestie dotyczące kierunku rozwoju tego narzędzia. Na każdy pomysł można oddawać głos oraz obserwować postęp w jego implementacji. Obecnie liczba zgłoszeń w kategorii „Szkoły i uczelnie wyższe" liczy prawie 7 tysięcy. Przyszłe wersje tego narzędzia mogą okazać się zdecydowanie bardziej użyteczne dla wykładowców uczelni wyższych, prowadzących nauczanie zdalne.

Literatura

[1] WIELISIEJ M., *Księga bezpieczeństwa w komunikacji elektronicznej w pracy radcy prawnego – Analiza porównawcza ogólnej zgodności oraz niektórych elementów bezpieczeństwa aplikacji do telekonferencji: ZOOM, Microsoft Teams, CISCO Webex*. Krajowa Rada Radców Prawnych, Warszawa, 2020.

[2] ĆWIAKOWSKI M., GAWROŃSKI M., SZUMRAK P., *Księga bezpieczeństwa w komunikacji elektronicznej w pracy radcy prawnego – Ocena zgodności wykorzystania usług wideokonferencyjnych: Microsoft Teams będącej częścią pakietu Microsoft 365, Zoom 5.0, Cisco Webex do komunikacji przez radców z klientami w ramach wykonywania zawodu oraz w działalności organów samorządu radcowskiego.* Krajowa Rada Radców Prawnych, Warszawa, 2020.

Źródła elektroniczne

[3] WARREN T., *Microsoft Teams jumps 70 percent to 75 million daily active users*. https://www.theverge.com/2020/4/29/21241972/microsoft-teams-75-million-daily-active-users-stats (dostęp 19.07.2020).

[4] Microsoft Teams – *User Feedback Forum*. https://microsoftteams.uservoice.com (dostęp 19.07.2020).

[5] *Umowa dotycząca usług Microsoft (Microsoft Services Agreement, MSA)*. https://www.microsoft.com/pl-pl/servicesagreement/ (dostęp 19.07.2020).

[6] *Security and compliance in Microsoft Teams*, https://docs.microsoft.com/en-us/MicrosoftTeams/security-compliance-overview (dostęp 19.07.2020).

Usability analysis of Microsoft Teams videoconference platform for remote teaching at universities

ABSTRACT: The videoconference communication platform, which is Microsoft Teams, is a type of service implemented in the SaaS (Software as a Service) cloud computing model. Users of this platform can distribute signals from their cameras and microphones, text via chat, and files as attachments. The service provides various communication management functions available for the videoconference organizer. The paper presents results of usability study on selected functions of this paid service, due to its usefulness in remote learning.

KEYWORDS: Microsoft Teams, videoconference, remote teaching

Praca wpłynęła do redakcji: 29.06.2020 r.

PRZEGLĄD TELEINFORMATYCZNY
NR 1-4, 2020

Wybrane metody rozpoznawania osób na podstawie odcisków palców

Leszek GRAD

Instytut Teleinformatyki i Cyberbezpieczeństwa, Wydział Cybernetyki, WAT
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
leszek.grad@wat.edu.pl

STRESZCZENIE: W artykule przedstawiono zagadnienie rozpoznawania tożsamości osób na podstawie odcisków palców. Przedstawiono aktualny stan wiedzy, wybrane metody i techniki zarówno opisu obrazu linii papilarnych, jak i metody klasyfikacji.

SŁOWA KLUCZOWE: biometria, rozpoznawanie odcisków palców, identyfikacja, weryfikacja tożsamości

Wstęp

Obecnie obserwuje się gwałtowny rozwój elektronicznych systemów zabezpieczeń wykorzystujących techniki biometryczne w procesie uwierzytelniania. Ze wszystkich dotychczas stosowanych metod zabezpieczeń techniki biometryczne należą do najbezpieczniejszych oraz najwygodniejszych dla użytkowników. Bezpieczeństwo wynika z tego, że człowiek dysponuje wieloma unikatowymi cechami, które mogą być agregowane w celu osiągnięcia żądanego poziomu bezpieczeństwa. Systemy dostępu bazujące na biometrii są wykorzystywane powszechnie zarówno w dostępie do systemów o bardzo wysokim poziomie zabezpieczeń (systemy bankowe, bankomaty, laboratoria), jak i do zabezpieczeń personalnego sprzętu komputerowego (laptopy z czytnikami biometrycznymi, myszki, pamięci flash, smartfony). Jedną z ważniejszych charakterystyk biometrycznych są odciski palców. Oprócz zastosowań w systemach dostępu odciski palców od dawna były i są nadal wykorzystywane w kryminalistyce do identyfikacji przestępców (daktyloskopia). Systemy automatycznego rozpoznawania odcisków palców są z języka angielskiego określane skrótem AFIS (*Automated Fingerprint Identification System*).

Podstawowe pojęcia biometrii

Biometria (ang. *biometrics*) jest nauką zajmującą się identyfikacją lub weryfikacją tożsamości osoby na podstawie jej cech fizycznych lub behawioralnych. Owe cechy nazywane są cechami biometrycznymi (ang. *biometric traits*) [33] lub krótko biometrykami [5]. Dokonuje się systematyki biometryk. Są one dzielone na rejestrowane w sposób statyczny, nazywane fizycznymi lub fizjologicznymi (ang. *physiological traits*) oraz rejestrowane w pewnym przedziale czasu, zwane behawioralnymi (ang. *behavioral traits*), obejmujące cechy wykształcone lub wyuczone. Do pierwszej kategorii zaliczane są, będące przedmiotem rozważań niniejszego artykułu, odciski palców. Przykładem charakterystyki behawioralnej jest głos. Zestawienie podstawowych charakterystyk biometrycznych przedstawione zostało w tabeli 1, szczegółowy zaś opis poszczególnych biometryk można znaleźć w pracach [5], [18], [33].

Tab. 1. Podstawowe charakterystyki biometryczne

Cechy fizyczne	Cechy behawioralne
Odciski palców	Głos
Tęczówka oka	Składanie podpisu
Układ naczyń krwionośnych siatkówki oka	Ruch ust
Układ naczyń krwionośnych dłoni	Chód
Geometria dłoni	
Obraz twarzy	
Termogram	
Profil DNA	
Kształt ucha	

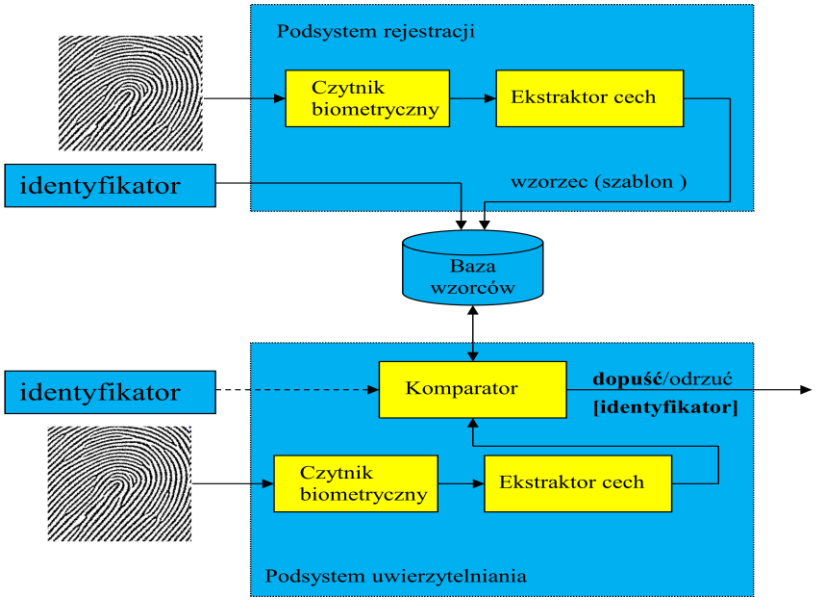
Przydatność danej biometryki jest oceniana na podstawie pięciu cech: unikatowości (ang. *unigueness*), uniwersalności (ang. *univesality*), trwałości (ang. *permanence*), mierzalności lub ściągalności (ang. *collectability*), akceptowalności (ang. *acceptance*). W tym świetle idealną cechą jest taka, która pozwala na jednoznaczną identyfikację osobnika w ramach określonej populacji, każdy osobnik ją posiada, łatwo ją zmierzyć oraz jej zdejmowanie nie budzi kontrowersji ani nie jest inwazyjne. Z wymienionych w tabeli 1 największe znaczenie praktyczne obecnie posiadają: odciski palców wraz z układem naczyń krwionośnych dłoni, tęczówka oka oraz głos (z biometryk behawioralnych).

Systemy biometryczne

Systemem biometrycznym nazywany jest system rozpoznawania (identyfikacji lub weryfikacji), w którym klasyfikacja odbywa się na podstawie

charakterystyk biometrycznych (zapisanych w postaci wektorów cech). Architekturę typowego biometrycznego systemu rozpoznawania przedstawiono na rysunku 1. Składa się on z dwóch podsystemów: rejestracji oraz identyfikacji/weryfikacji. Zadaniem pierwszego jest dokonanie rejestracji użytkownika. W trakcie jednorazowej rejestracji w bazie danych (lub ogólniej w systemie) zapisywany jest identyfikator oraz wzorzec (szablon) biometryczny. Zadaniem podsystemu identyfikacji/weryfikacji jest dokonanie identyfikacji poprzez porównanie pobranej próbki biometrycznej ze wzorcami zapisanymi w bazie lub zweryfikowanie tożsamości poprzez porównanie pobranej próbki ze wzorcem osoby, której tożsamość jest deklarowana.

Działanie biometrycznych systemów rozpoznawania oceniane jest na podstawie dwóch podstawowych wskaźników. Pierwszym z nich jest stopa fałszywej akceptacji (ang. *False Acceptance Rate* – FAR) wyznaczana jako procent zdarzeń polegających na pozytywnej weryfikacji fałszywej próbki. Drugim jest stopa fałszywego odrzucenia (ang. *False Rejection Rate* – FRR) wyznaczana jako procent zdarzeń polegających na stwierdzeniu niezgodności badanej próbki ze wzorcem w sytuacji, kiedy zgodność występuje. Do porównywania jakości działania systemów rozpoznawania wykorzystuje się wskaźnik EER (ang. *Equal Error Rate*) wyznaczany jako wartość wskaźnika FAR lub FRR dla takiego progu decyzyjnego, kiedy FAR = FRR.



Rys. 1. Architektura typowego biometrycznego systemu uwierzytelniania

System biometryczny jest systemem rozpoznawania wzorców. Wykorzystuje zatem znane metody klasyfikacji (klasyfikatory minimalno-odległościowe, sztuczne sieci neuronowe) [18], [23], [33], [47].

1. Odcisk palca jako charakterystyka biometryczna

Jak zaznaczono we wstępie, odciski palców należą do podstawowych charakterystyk biometrycznych. Są wykorzystywane do identyfikacji osób od dawna. Już w XVIII zostały wykorzystane przez Galtona do identyfikacji tożsamości [33]. Na początku XX wieku opracowany został system identyfikacji Sir Edwarda Henry'ego, udoskonalony przez FBI (stosowany w kryminalistyce do ręcznej identyfikacji tożsamości) [5]. Wykorzystuje on podział wszystkich odcisków na pięć podstawowych klas: pętla lewa (ang. *left loop*), pętla prawa (ang. *right loop*), wir (ang. *whorl*), łuk (ang. *arch*), łuk wyostrzony namiotowy, (ang. *tented arch*) (rys. 2). Wzorzec zawiera opis wszystkich dziesięciu palców wg schematu: [*łuk, pętla lewa, łuk namiotowy, wir...*]. Obecnie, w systemach automatycznego rozpoznawania klasyfikacja typów odcisków jest stosowana do wstępnego filtrowania bazy odcisków [9]. W obrazie linii papilarnych można wskazać dwa charakterystyczne miejsca (punkty, ang. *Singular points*). Pierwszym jest tzw. rdzeń (ang. *Core*) [12]. Jest to miejsce o największej zmienności kierunku przebiegu grzbietów[1] [4], [40]. Drugim jest miejsce, gdzie linie tworzą układ delty (ang. *Delta point*). Obydwa charakterystyczne punkty pokazane zostały na rysunku 3.

Rys. 2. Pięć podstawowych klas odcisków. Od lewej: pętla lewa (ang. *left loop*) (34%), pętla prawa (ang. *right loop*) (31%), wir (ang. *whorl*) (28%), łuk (ang. *arch*) (4%), łuk wyostrzony (namiotowy) (ang. *tented arch*) (3%). W nawiasach podano częstość występowania, obrazy z bazy FVC2002

[1] W obrazie linii papilarnych wyróżniamy grzbiety (ang. *ridge*), czyli miejsca w których palec przylegał do skanera oraz doliny albo bruzdy (ang. *valley*), czyli miejsca pomiędzy grzbietami.

Charakterystyka odcisku palca w świetle pożądanych cech

Unikatowość: bardzo niska powtarzalność – szacowane ok. 1 : 64 miliardów [5].

Uniwersalność: nieliczny odsetek nie posiada tej cechy (utrata kończyny, wady genetyczne).

Trwałość: wysoka – obraz linii papilarnych kształtuje się w okresie prenatalnym i nie zmienia się do końca życia, dość duża jednak podatność na uszkodzenia przy ranach prowadzących do blizn (można je jednak traktować jako zmianę charakterystyki).

Mierzalność: łatwa – skanowanie obrazu odcisku palca zabiera mało czasu i jest jedną z najmniej inwazyjnych metod biometrycznych.

Akceptowalność: w kryminalistyce cecha nieistotna, w systemach ochrony jest akceptowalna.

Poza powyższymi cechami systemy rozpoznawania bazujące na obrazach linii papilarnych charakteryzują się wysoką skutecznością rozpoznawania (FAR rzędu 0,01% przy FRR maksymalnie 10% [24], [33]).

Ważną cechą systemu biometrycznego jest odporność na oszustwa. W przypadku odcisków palców wysoką odporność gwarantują nowoczesne skanery odczytujące obraz trójwymiarowy oraz mierzące tętnienie krwi w naczyniach krwionośnych [48]. W zakresie polityki bezpieczeństwa systemów biometrycznych leży także ochrona baz wzorców przed kompromitacją [37][2].

Rys. 3. Punkty charakterystyczne obrazu odcisku palca: rdzeń oraz delta, obraz z bazy FVC2002 DB1_B

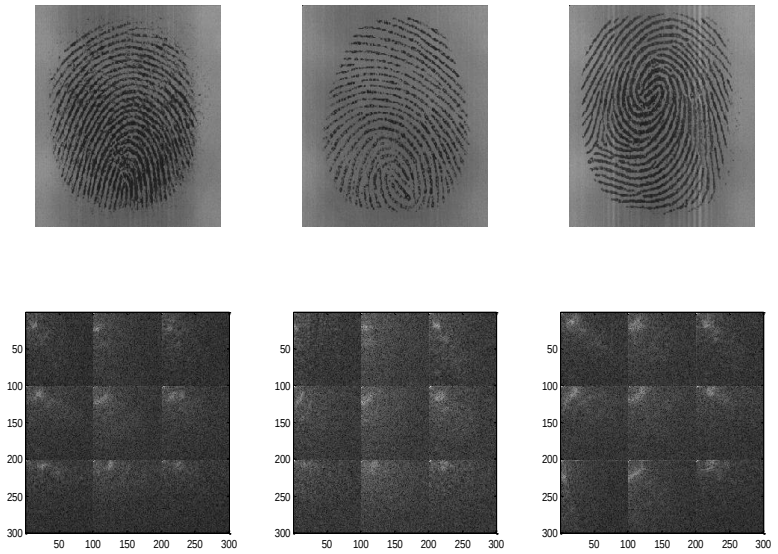
[2] W pracy przedstawiono wysoce bezpieczną technikę komparacji odcisków odporną na ataki DPA (ang. *Differential Power Analysis*), które mogą doprowadzić do kompromitacji wzorca.

Podstawowe metody ekstrakcji cech obrazu linii papilarnych

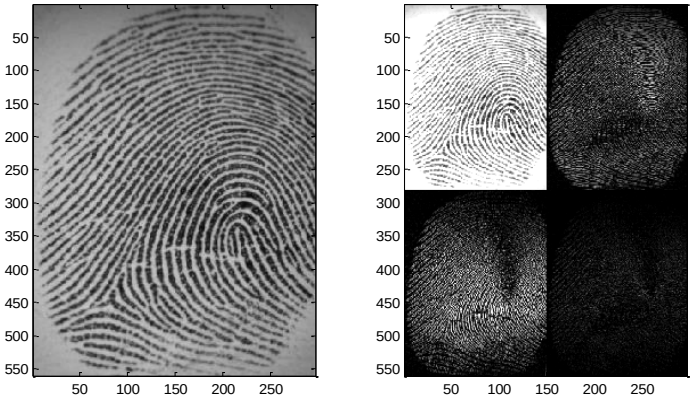
Obraz linii papilarnych poddawany jest analizie mającej na celu wydobycie cech istotnych dla procesu rozpoznawania (cech dystynktywnych) przy jednoczesnej redukcji danych, co pociąga za sobą szybsze działanie systemu rozpoznawania oraz zmniejszenie objętości bazy wzorców.

Obecnie w rozpoznawaniu odcisków palców wykrystalizowały się dwa podejścia. Pierwsze polega na rozpoznawaniu poprzez porównywanie obrazów odcisków (ang. *fingerprint matching*), najczęściej w dziedzinie transformat (przestrzenno-częstotliwościowej). Najczęściej wykorzystywane transformaty to: transformata Fouriera, transformata kosinusowa, transformata falkowa [2], [9], [36]. Na rysunku 4 przedstawione zostały obrazy trzech odcisków oraz transformaty kosinusowe tych obrazów wyznaczone w segmentach (lokalnie), każdy obraz został podzielony na 9 segmentów, wyraźnie widoczny jest zróżnicowany rozkład energii w odpowiadających sobie segmentach transformat związany z kierunkiem przebiegu linii. Z kolei rysunek 5 przedstawia wynik dekompozycji falkowej (pierwszego poziomu) obrazu odcisku. W wyniku dekompozycji uzyskuje się składową niskoczęstotliwościową oraz informację o szczegółach przebiegu linii (poziomych, pionowych oraz przebiegających ukośnie). Analiza kierunku przebiegu linii (rys. 6) stanowi jedną z podstawowych metod opisu obrazu odcisku i jest rozwijana od początku lat dziewięćdziesiątych ubiegłego stulecia [8], [9], [10], [20], [28], [30], [38], [43], [44], [45]. Rozpoznawanie odcisków w dziedzinie transformat cechuje duża odporność na niską jakość obrazu odcisku. Jest preferowane w identyfikacji kryminalistycznej, gdzie ważna jest minimalizacja FRR.

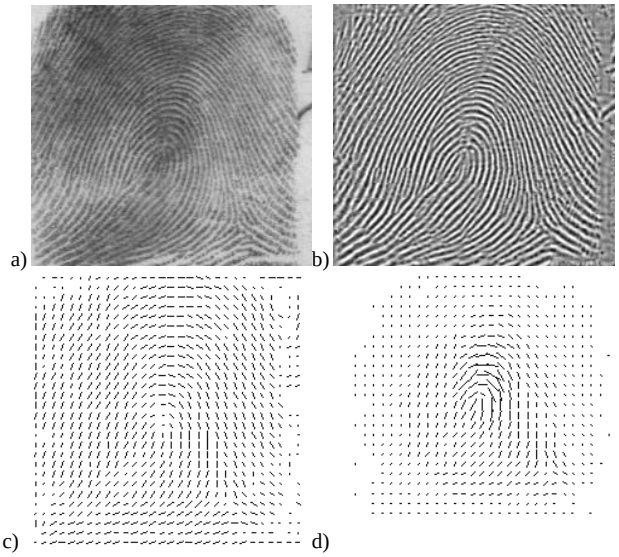
Drugie podejście do rozpoznawania odcisków polega na uwzględnieniu charakterystycznych cech budowy morfologicznej (szczególnych elementów geometrycznego wzoru tworzonego przez linie papilarne) tzw. minucji [18], [19], [29], [32], [33], [46]. Wyszczególniono kilkanaście różnych detali [49] (rys. 7), z których najczęściej wykorzystywane są dwa, tzn. początek/koniec linii oraz rozwidlenie pojedyncze (bifurkacja). W tym przypadku wzorzec odcisku obejmuje wektor minucji, z których każda opisana jest współrzędnymi położenia oraz kierunkiem przebiegu grzbietu. Początek układu współrzędnych umieszcza się w rdzeniu odcisku. Stosowanymi metodami znajdowania rdzenia są: metoda Poincare [17], [30], [31], [34] oraz R92 [31].



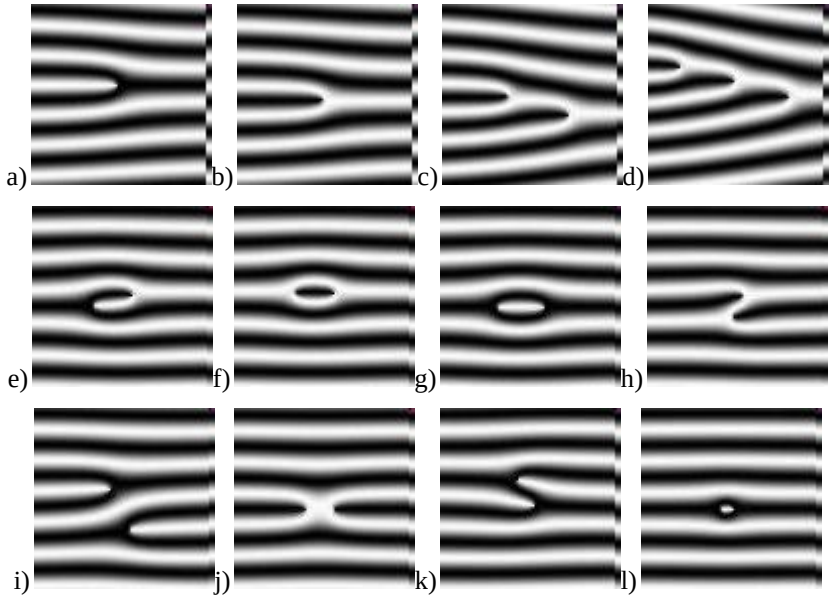
Rys. 4. Odciski trzech palców i odpowiadające im lokalne transformaty kosinusowe. Zastosowano podział obrazu na 9 segmentów, widoczny jest odmienny rozkład energii w odpowiadających sobie segmentach transformat. Obrazy z bazy FVC2002 DB3_B



Rys. 5. Transformata falkowa obrazu linii papilarnych (po prawej), pierwszy poziom dekompozycji. Prawy górny obraz opisuje detale poziome, lewy dolny – detale pionowe, prawy dolny – detale skośne. Obrazy z bazy FVC2002 DB1_B

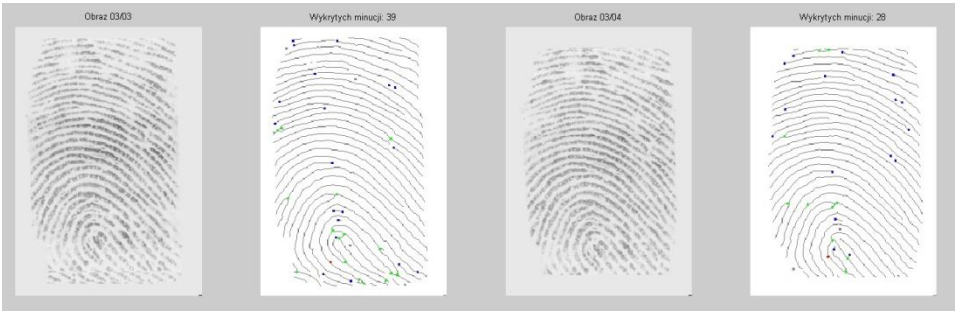


Rys. 6. Ekstrakcja cech w metodzie przedstawionej w pracy [8], a) obraz linii papilarnych, b) obraz o poprawionej jakości (ang. *enhancement*), c) kierunki przepływu bruzd (ang. *directional image*), d) directional image z wycentrowanym rdzeniem odcisku



Rys. 7. Minucje (linie przedstawione są kolorem białym): a) początek/koniec, b) rozwidlenie pojedyncze, c) rozwidlenie podwójne, d) rozwidlenie potrójne, e) haczyk, f) oczko, g) odcinek, h) mostek, i) linia przechodząca, j) skrzyżowanie, k) styk boczny, l) punkt Źródło: www.optel.com.pl

Z reguły w obrazach linii papilarnych wykrywa się 30-40 minucji. Do określenia zgodności odcisku ze wzorcem wystarczy zgodność na poziomie 10-20[3]. Rozpoznawanie na podstawie minucji preferowane jest w weryfikacji biometrycznej, gdzie ważna jest minimalizacja wskaźnika FAR. Detekcja minucji wymaga zastosowania wieloetapowego przetwarzania obrazu[4] [29]. Na rysunku 8 przedstawiono obrazy odcisków przetworzone do postaci szkieletowej z wykrytymi zakończeniami oraz rozwidleniami linii.



Rys. 8. Obrazy odcisków palców oraz obrazy szkieletowe z naniesionymi, wykrytymi minucjami (zakończenia oraz rozwidlenia)[5]

Poważnym problemem, który należy rozwiązać w systemach automatycznego rozpoznawania odcisków palców, jest problem rotacji i translacji. Co prawda skanery w przeważającej mierze są tak skonstruowane, że nie pozwalają na zbyt wielkie odchylenia osi palca od pionowej osi skanera oraz przesunięcie wzdłuż tej osi, ale nawet niewielkie wartości przesunięcia i obrotu mogą skutkować znaczącym pogorszeniem wyników rozpoznawania. Ustalenie osi palca, tym samym rotacji, jest dość łatwe, jeśli zarejestrowany obraz posiada pewien margines. W przeciwnym razie zadanie staje się trudne i stanowi element wielu prac badawczych (punkt 2). W przypadku korekcji błędu przesunięcia wykorzystuje się rdzeń odcisku jako punkt odniesienia.

[3] Na podstawie [48] oraz badań przeprowadzonych w ramach prac dyplomowych prowadzonych przez autora, ciekawe rezultaty badań przedstawiono także w pracy [21].

[4] Typowe fazy ekstrakcji minucji:

1. binaryzacja z progiem adaptacyjnym;
2. wyznaczenie kierunku przepływu linii w każdym pikselu – metody gradientowe;
3. wyznaczenie rdzenia odcisku;
4. szkieletyzacja – metody morfologiczne;
5. lokalizacja minucji;
6. eliminacja minucji fałszywych.

[5] Opracowanie wewnętrzne WAT, autor: Michał Kazimierczak.

W przypadku systemów opartych na minucjach, które są bardzo czułe na rotację i translację, stosuje się najczęściej lekko rozmyte dopasowywanie na etapie wykrywania poszczególnych minucji.

2. Wybrane przykłady metod i algorytmów rozpoznawania tożsamości na podstawie odcisków palców

W tym rozdziale dokonano opisu ciekawszych podejść do rozpoznawania tożsamości osób na podstawie obrazu linii papilarnych. Wybrano zarówno te, gdzie nacisk położono na metodę ekstrakcji cech (opis obrazu), jak i te, w których zaproponowano interesujące systemy klasyfikacji.

W pracy [13] przedstawiono wyniki zastosowania neuronowych sieci rezonansowych ART1 do wstępnej klasyfikacji odcisków. Dla każdej klasy, do ostatecznej identyfikacji jako klasyfikatora użyto również sieci neuronowej. Zbadano wpływ takiego podejścia na czas realizacji procesu rozpoznawania, porównując z działaniem systemu opartego na jednej sieci neuronowej. Otrzymano ponad dwudziestokrotne skrócenie czasu klasyfikacji. Poprawiła się także skuteczność rozpoznawania z 98% do 100% prawidłowych identyfikacji. Również w pracy [26] do weryfikacji zastosowano wielowarstwową sieć neuronową. W tym przypadku sieć neuronowa została wykorzystana jako jeden z trzech algorytmów wykrywania minucji (w metodzie uwzględniono zakończenia i rozwidlenia linii). Do komparacji ze wzorcem zaproponowano własny rozmyty operator, który pozwolił obejść problem różnej liczby wykrywanych minucji w obrazie. Testy wykazały skuteczność takiego podejścia na poziomie 95%.

Problem wstępnej klasyfikacji odcisków był rozważany także w pracach [9] oraz [45]. W pierwszej z nich przedstawiony został dwustopniowy system klasyfikacji wstępnej odcisków (tzn. zaliczania do jednej z podstawowych pięciu klas). W pierwszym stopniu zastosowano klasyfikację minimalnoodległościową opartą na transformacie KL (MKL – Multi-space KL). Wynikiem tego etapu było wytypowanie dwóch najbardziej prawdopodobnych klas. Ostateczne rozstrzygnięcie następowało w klasyfikatorze SPD, który został wytrenowany do rozpoznawania jednej z klas z każdej możliwej pary. Wyekstrahowany wektor cech dla pierwszego etapu liczył 1680 elementów i zawierał opis kierunku przepływu bruzd w 28×30 segmentach, w drugim etapie wektor cech został zredukowany do 80 elementów (poprzez dekorelację). Metodę przetestowano z wykorzystaniem bazy NIST DB4, uzyskano stopę błędnej identyfikacji równą 4,8%, co jest najlepszym wynikiem uzyskanym dla tej bazy [16]. Wcześniejsze prace autorów [6], [7] były również poświęcone zastosowaniu MKL w rozpoznawaniu odcisków. W pracy [45] przedstawiono metodę wstępnej klasyfikacji odcisków na podstawie występowania i położenia rdzenia oraz

delty. Opis parametryczny odcisku zawierał 3 elementy: liczbę rdzeni, liczbę delt, położenie delty (środek, strona lewa odcisku, strona prawa). Wzorce poszczególnych klas zostały opisane w następujący sposób:

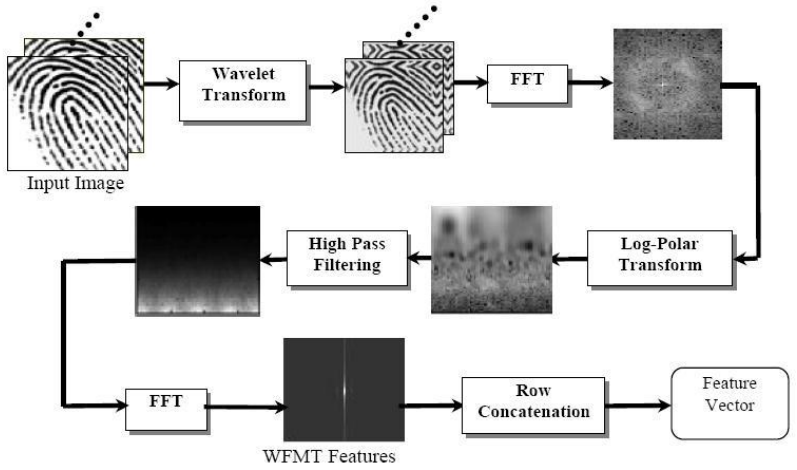
łuk – [0, 0, -], łuk namiotowy – [1, 1, środek], pętla lewa – [1, 1, prawo], pętla prawa – [1, 1, lewo], wir – [2, 2, -]. Do wyznaczenia zarówno rdzenia, jak i delty wykorzystano indeks Poincare. Tak nieskomplikowane określenie wzorców dało dość dobre rezultaty (stopa prawidłowych identyfikacji 84%).

W pracy [2] do parametrycznego opisu odcisku w zadaniu weryfikacji tożsamości zastosowano transformatę falkową oraz transformatę Fouriera–Mellina (WFMT – *Wavelet and the Fourier-Mellin Transform*). Wykorzystana tu została dekompozycja falkowa 2 poziomu w celu wygładzenia i utrwalenia przebiegu linii papilarnych[6]. Pozwala to na uniezależnienie się od zniekształceń kształtu[7] (ang. *shape distortion*). Otrzymano w ten sposób także obraz w mniejszej rozdzielczości, co wpływa na zmniejszenie nakładów obliczeniowych w dalszych etapach przetwarzania. Transformata Fouriera–Mellina zapewnia ekstrakcję cech oraz umożliwia uniezależnienie się od przesunięcia, obrotu i zmiany skali (ang. *invariants features*). Przebieg procesu ekstrakcji cech w proponowanej metodzie przedstawiony został na rysunku 9. W pierwszym kroku algorytmu realizowana jest transformata falkowa. Do dalszego przetwarzania zostaje wzięta jedynie niskoczęstotliwościowa składowa dekompozycji (redukcja przestrzeni, wygładzenie obrazu). W drugim kroku obraz odcisku poddawany jest transformacie Fouriera w celu uzyskania widma amplitudowego. Widmo amplitudowe jest nieczułe na translację.

Kolejny krok to przekształcenie widma do układu planarnego oraz jego zlogarytmowanie. Zabieg ten pozwala na uniezależnienie się od zmiany skali i zastosowanie kwantyzacji nieliniowej uwypuklającej harmoniczne o niższej częstotliwości. Zlogarytmowane widmo amplitudowe przedstawione w układzie biegunowym zostaje poddane filtracji górnoprzepustowej i ponownie transformacie Fouriera (cepstrum, uniezależnienie się od rotacji obrazu pierwotnego). Ostateczny wektor cech uzyskano, sumując wiersze macierzy wynikowej (wektor cech o długości wiersza obrazu odcisku palca po transformacie falkowej). Taka metoda ekstrakcji cech obrazu linii papilarnych została przetestowana na bazie FVC 2002. Dla różnych zbiorów odcisków tej bazy uzyskano ERR od 1,25 do 3,57, co należy uznać za wynik bardzo dobry.

[6] Wykorzystuje niskoczęstotliwościową składową dekompozycji.

[7] Takich jak przerwy w przebiegu linii papilarnych.



Rys. 9. Diagram algorytmu ekstrakcji cech odcisku palca zaproponowany w pracy [2]

Opis innych podejść stosowanych do rozpoznawania obrazów z inwariantnością cech (*integral transforms*, *moment invariants*) można znaleźć w pracy [36].

W pracy [17] opisano metodę opartą także na analizie obrazu odcisku w przestrzeni dwuwymiarowej dyskretnej transformaty Fouriera, z wykorzystaniem jedynie charakterystyki fazowej. Metoda pozwala na skuteczną ekstrakcję cech z obrazów niskiej jakości.

Podsumowanie

Przedstawiona w artykule cecha biometryczna, jaką jest układ linii papilarnych, jest stale wykorzystywana w systemach uwierzytelniana opartych na biometrii. Pomimo, jak się uznaje, lepszych cech, jak np. obraz tęczówki oka, układ żył palca czy śródręcza, odciski palców są stosowane w rozpoznawaniu. Dzieje się to za sprawą wysokiej dystynktywności, uwarunkowań historycznych (zastosowanie w kryminalistyce), rozpowszechnienia układów do akwizycji (niska cena), jak również istnienia ugruntowanych, zaawansowanych metod przetwarzania, analizy i rozpoznawania obrazów linii papilarnych, których przegląd został przedstawiony w niniejszym opracowaniu.

Literatura

[1] AHMED F., MOSKOWITZ I.S., *Composite signature based watermarking for fingerprint authentication*, MM&Sec ’05: Proceedings of the 7th workshop on Multimedia & Security, ACM, August 2005, pp. 137-142.

[2] ANDREW T.B.J., DAVID N.C.L., *Integrated Wavelet and Fourier-Mellin invariant feature in fingerprint verification system*. WBMA ’03: Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, ACM, November 2003, pp. 82-88.

[3] BEY K.B., GUESSOUM Z., MOKHTARI A., BENHAMMADI F., *Agent based approach for distribution of fingerprint matching in a metacomputing environment*. NOTERE ’08: Proceedings of the 8th International Conference on New Technologies in Distributed Systems, ACM, June 2008, pp. 1-7.

[4] BIAN W., XU D., LI O., CHENG Y., JIE B., DING X., *A Survey of the Methods on Fingerprint Orientation Field Estimation*. IEEE Access, 2019, Volume 7, pp. 32644-32663.

[5] BOLLE R.M., CONNELL J.H., PANKANTI S., RATHA N.K., SENIOR A.W., *Biometria*, WNT, Warszawa 2008.

[6] CAPPELLI M., MAIO D., MALTONI D., *Fingerprint Classification based on Multi-space KL*. In proceedings Workshop on Automatic Identification Advances Technologies (AutoID ’99), Summit (NJ), October 1999, pp. 117-120.

[7] CAPPELLI M., MAIO D., MALTONI D., *Multi-space KL for Pattern Representation and Classification*. IEEE Transactions on Pattern Analysis Machine Intelligence, Vol. 23, no. 9, September 2001, pp. 977-996.

[8] CAPPELLI R., LUMINI A., MAIO D., MALTONI D., *Fingerprint Classification by Directional Image Partitioning*. IEEE Transactions on Pattern Analysis and Machine Intelligence 21(5), 1999, pp. 402-421.

[9] CAPPELLI M., MAIO D., MALTONI D, NANNI L., *A two-stage fingerprint classification system.* WBMA ’03: Proceedings of the 2003 ACM SIGMM workshop on biometrics methods and applications, ACM, November 2003, pp. 95-99.

[10] CAO K., JAIN A.K., *Automated Latent Fingerprint Recognition*. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2019, Volume 41, Issue 4, pp. 788-800.

[11] CLANCY T.Ch., KIYAVASH N., LIN D.J., *Secure martcardbased fingerprint authentication*. WBMA ’03: Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, ACM, November 2003, pp. 45-52.

[12] DOROZ R., WROBEL K., PORWIK P., *An accurate fingerprint reference point determination method based on curvature estimation of separated ridges*, International Journal of Applied Mathematics and Computer Science, 2018, Vol. 28, no. 1, pp. 209-225.

[13] GOUR B., BANDOPADHYAYA T.K., PATEL R., *ART and Modular Neural Network Architecture for Multilevel Categorization and Recognition of Fingerprints.* IEEE Conference, Knowledge Discovery and Data Mining, 2010. WKDD '10, Third International Conference, pp. 536-539.

[14] GUPTA P., RAVI S., RAGHUNATHAN A., JHA N.K., *Efficient fingerprint-based user authentication for embedded systems*. DAC '05: Proceedings of the 42nd annual Design Automation Conference, ACM, June 2005.

[15] HOLZ Ch., BAUDISCH P., *The generalized perceived input point model and how to double touch accuracy by extracting fingerprints*. CHI '10: Proceedings of the 28th international conference on Human factors in computing systems, ACM, April 2010.

[16] HONG L., JAIN A.K., *Classification of Fingerprint Images*. http://www.cse.msu.edu/biometrics/Publications/Fingerprint/clas.pdf

[17] ITO K., MORITA A., AOKI T., HIGUCHI T., NAKAJIMA H., KOBAYASHI K., *A fingerprint recognition algorithm using phase-based image matching for low-quality fingerprints.* Image Processing, 2005, ICIP 2005, IEEE International Conference on, pp. II-33-6.

[18] JAIN A.K., HONG L., PANKANTI S., BOLLE R., *An Identity Autentication System Using Fingerprints*. Proc. of IEEE 85 (9), 1997, pp. 1365-1388, on line at: http://biometrics.cse.msu.edu/Publications/Fingerprint/JainEtAlIdentityAuthUsingFp_ProcIEEE97.pdf

[19] JAIN A.K., HONG L., BOLLE R., *On-Line Fingerprint Verification*. IEEE Transactions on Pattern Analysis and MAchine Intelligence, Vol. 19, no. 4, 1997, pp. 302-314.

[20] JAN H., ALI A., *Optimization of fingerprint size for registration*. Applied Computer Science, vol. 15, no. 2, 2019, pp. 19-30.

[21] KAPCZYŃSKI A., *Quantitative and qualitative characteristics of fingerprint biometric templates*. Zeszyty Naukowe. Organizacja i Zarządzanie / Politechnika Śląska, 2014, z. 74, s. 55-63.

[22] KAWAGOE M., TOJO A., *Fingerprint Pattern Classification*. Pattern Recognition, Vol. 17, no. 3, 1984, pp. 295-303.

[23] KWIATKOWSKI W., *Metody rozpoznawania wzorców*. Bel Studio, Warszawa, 2002.

[24] MALTONI D., MAIO D., PRABHAKAR S., *Handbook of Fingerprint Recognition, SprioSpringre Professional Computing Series*, 2003.

[25] MIL'SHTEIN S., PILLAI A., SHENDYE A., LIESSNER C., BAIER M., *Fingerprint Recognition Algorithms for Partial and Full Fingerprints*. 2008 IEEE Conference on Technologies for Homeland Security, pp. 449-452.

[26] MONTESANTO A., BALDASSARRI P., VALLESI G., TASCINI G., *Fingerprints recognition using Minutae extraction: a fuzzy approach*, Image analysis and processing, ICIAP 2007, 14th International Conference, pp. 229-234.

[27] PARK C.H., LEE J.J., SMITH M., PARK S., PARK K.H., *Directional filter bank-based fingerprint feature extraction and matching*. IEEE Trans. On Circuits and Systems for Video Tachnology, Vol. 14, 1, 2004, pp. 74-78.

[28] RAO A.R., *A Taxonomy for Texture Description and Identification*. Springer-Verlag, New York, 1990.

[29] RAPTA P., SAEED K., *A new algorithm for fingerprint feature extraction without the necessity to improve its image*. Bio-Algorithms and Med-Systems, 2010, Vol. 6, no. 12, pp. 25-29.

[30] SRINIVASAN V.S., MURTHY N.N., *Detection of Singular Points In Fingerprint Images.* Pattern Recognition 25(2), 1992, pp. 139-153.

[31] SURMACZ K., SAEED K., RAPTA P., *An improved algorithm for feature extraction from a fingerprint fuzzy image.* Optica Applicata, 2013, Vol. 43, no. 3, pp. 515-527.

[32] SZCZEPANIAK M., JÓŹWIAK I., *Data management for fingerprint recognition algorithm based on characteristic points group*. Foundations of Computing and Decision Sciences, 2013, Vol. 38, no. 2, pp. 123-130.

[33] ŚLOT K., *Wybrane zagadnienia biometrii*. WKŁ, Warszawa, 2008.

[34] TANG T.Y., MOON Y.S., CHAN K.C., *Efficient implementation of fingerprint verification for mobile embedded systems using fixed-point arithmetic*. SAC ’04: Proceedings of the 2004 ACM symposium on Applied Computing, ACM, March 2004, pp. 821-825.

[35] TARDOS G., *Optimal probabilistic fingerprint codes*. STOC '03: Proceedings of the thirty-fifth annual ACM symposium on Theory of computing, ACM, June, 2003, pp. 116-125.

[36] TICO M., IMMONEN E., RAMO P., KOUSMANEN P., SARINNEN J., *Fingerprint Recognition Using Wavelet Features*. Proc. of IEEE international Symposium on Circuits and Systems 2, 2001, pp. 21-24.

[37] YANG S., VERBAUWHEDE I.M., *A secure fingerprint matching technique*. WBMA ’03: Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, ACM, November, 2003, pp. 98-94.

[38] WANG S., ZHANG W.W., WANG Y.S., *Fingerprints Classification by Directional Fields.* ICMI'02: Proceedings of the 4th IEEE International Conference on Multimodal Interfaces, IEEE Computer Society, October, 2002, pp. 395-399.

[39] WEGSTEIN J.H., *An automated fingerprint identification system*. U.S. National Institute of Standards and Technology, NBS Special Publication 500-89, 1982.

[40] WIECLAW L., *Gradient based fingerprint orientation field estimation*. Journal of Medical Informatics & Technologies, Vol. 22, 2013, pp. 203-207.

[41] WOOD J., *Invariant Pattern Recognition: A Review*. Pattern Recognition, 29 (1), 1996, pp. 1-17.

[42] WÓJTOWICZ W., *A Fingerprint-Based Digital Images Watermarking for Identity Authentication.* Annales Universitatis Mariae Curie-Skłodowska. Sectio AI, Informatica, Vol. 14, no. 1, 2014, pp. 85-96.

[43] VALDES-RAMIREZ D., MEDINA-PÉREZ M.A.;MONROY R., LOYOLA-GONZÁLEZ O., RODRÍGUEZ J., MORALES A., HERRERA F., *A Review of Fingerprint Feature Representations and Their Applications for Latent Fingerprint Identification: Trends and Evaluation*. IEEE Access, Volume 7, 2019, pp. 48484-48499.

[44] VIZCAYA P.R., GERHARDT L.A., *A Nonlinear Orientation model for Global Description of Fingerprints.* Pattern Recognition 29 (7), 1996, pp. 1221-1231.

[45] ZHANG Q., HUANG K., YAN H., *Fingerprint classification based on extraction and analysis of singularities and pseudo ridges.* VIP '01: Proceedings of the Pan-Sydney area workshop on Visual information processing, Volume 11, Australian Computer Society Inc., May, 2001.

[46] ZHAO F., TANG X., *Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction*. Pattern Recognition 40, 2007, pp. 1270-1281, online at: www.sciencedirect.com

[47] ŻURADA J., BARSKI M., JĘDRUCH W., *Sztuczne sieci neuronowe*. Wydawnictwo Naukowe PWN, Warszawa, 1996.

[48] http://www.biometriclabs.pl/index.php?id=57&Itemid=112 (dostęp 17.09.2019).

[49] http://www.optel.com.pl/software/polska/metody.htm (dostęp 16.06.2019).

Fingerprint recognition – review of used methods

ABSTRACT: The paper considers the issue of the identity recognition of persons on the basis of fingerprints. The current state of knowledge, selected methods and techniques of fingerprint image description and classification methods are presented.

KEYWORDS: biometrics, fingerprint recognition, identification, verification

Praca wpłynęła do redakcji: 22.11.2019 r.

Badanie jakości działania użytkownika wykorzystującego urządzenie mobilne

Gesty pinch and stretch oraz wskazywanie w teście jednokierunkowym

Artur ARCIUCH, Antoni M. DONIGIEWICZ

Instytut Teleinformatyki i Cyberbezpieczeństwa, Wydział Cybernetyki WAT,
ul. gen. Sylwestra Kaliskiego 2, 00-908 Warszawa
{artur.arciuch}, antoni.donigiewicz@wat.edu.pl

STRESZCZENIE: W artykule przedstawiono wyniki badań jakości wykonywania gestów przez użytkownika wykorzystującego urządzenie mobilne. Jako urządzenie mobilne wykorzystano smartfon Nokia Lumia 800. Wyniki badań dotyczą podstawowego gestu pinch and stretch oraz jednokierunkowego testu wskazywania. Badania obejmują czas wykonania gestu i precyzję wykonania gestu. Wyniki uwzględniają podział użytkowników na grupy wiekowe oraz grupy używające i nie używające smartfona na co dzień. Przedstawiono porównanie wyznaczonych charakterystyk pomiędzy grupami.

SŁOWA KLUCZOWE: gesty pinch and stretch, jednokierunkowy test wskazywania, wprowadzanie gestów palcem, urządzenie mobilne, czas wykonania gestu, precyzja wykonania gestu

1. Wprowadzenie

W niniejszym artykule, który tematycznie jest kontynuacją prac [1] i [2], przedstawiono wyniki badań jakości wykonywania gestów jednym palcem przez użytkowników na ekranie urządzenia mobilnego. Jako urządzenie mobilne wykorzystano smartfon Nokia Lumia 800. Podstawowymi charakterystykami jakości wykonania gestów były czas wykonania gestu i precyzja wykonania gestu (odległość punktu dotyku ekranu palcem od środka dotykanego obiektu) oraz

prawdopodobieństwo błędu wykonania gestu. Gesty na ekranie wykonywano tylko palcem, a badaniami objętych było 60 osób w wieku 16-66 lat.

2. Działania podlegające badaniu

Wyniki badań jakości wykonywania gestów tap, double tap i flick przez użytkowników na ekranie urządzenia mobilnego przedstawiono w artykule [1], natomiast wyniki badań gestów pan i touch&hold przedstawiono w pracy [2]. W badaniach, których wyniki przedstawione są w niniejszym artykule, stosowano gesty *pinch&stretch* oraz działania wykonywane jako jednokierunkowy test wskazywania. Działania te również należą do typowych gestów wykonywanych przez użytkownika wykorzystującego smartfon.

Gest *pinch&stretch* polega na przeciąganiu (ściąganiu) ku sobie palców na ekranie (pinch – zmniejszanie, przycinanie) lub odsuwaniu od siebie dwóch palców na ekranie (stretch – rozciąganie, powiększanie). Gest ten stosowany jest do skalowania (powiększania lub zmniejszania) obrazu na ekranie przy korzystaniu z map, przy nawigowaniu, przy przeglądaniu stron internetowych lub treści multimedialnych (głównie zdjęć). Zakończenie gestu to podniesienie palców. W badaniach gest ten skonkretyzowano i polegał on na położeniu palców na obiekcie (kwadrat na ekranie) i przeskalowaniu obiektu do wielkości innego obiektu (kwadrat cel).

Działania wykonywane w ramach jednokierunkowego testu wskazywania to typowe działania użytkownika – wskazywanie i wybieranie obiektów na ekranie. Jednokierunkowy test wskazywania polegał na dotykaniu palcem prostokątów na ekranie. Prostokąty były ustalonej szerokości i ustawione były w określonej odległości od siebie.

3. Prace związane

Omówienie wybranych badań opisywanych w literaturze, dotyczących oceny jakości wykonywania gestów przez użytkowników na urządzeniach mobilnych, przedstawione zostało w artykule [1].

Tematyka badań jakości wykonywania gestów przez użytkowników urządzeń mobilnych ma swoje istotne miejsce w pracach dotyczących szeroko rozumianych zagadnień projektowania interakcji człowiek-komputer. Do stosunkowo nieodległych w czasie artykułów, w których wskazuje się na potrzebę uwzględniania wyników badań jakości działania użytkowników w projektowaniu interfejsów użytkownika urządzeń mobilnych, należą prace [3], [4] i [5]. Wyniki badań pozwalają projektantom wybrać najlepszy sposób

realizacji działań użytkowników nie tylko sprawnych percepcyjnie i ruchowo, ale również użytkowników z różnymi ograniczeniami [3] i użytkowników wykonujących zadania np. tylko jedną ręką [4].

Do grupy prac związanych z tematyką artykułu należy praca [6]. Praca dotyczy kinematyki palca wskazującego i kciuka oraz pomiarów wydajności dla typowych gestów na ekranie dotykowym. Badanie, poza analizą kinematyki stawów palcow, miało na celu m.in. ilościowe określenie różnic w 7 gestach na ekranie dotykowym.

Szczegółowe propozycje, wynikające z przeprowadzonych badań jakości realizacji działań użytkowników, a dotyczące użyteczności i projektowania czterech różnych rozmiarów paneli dotykowych dla osób starszych, młodych dorosłych i dzieci zostały zaproponowane w pracy [5].

4. Warunki prowadzenia badań

4.1. Urządzenia wykorzystywane w badaniach

W badaniach przedstawionych w tym artykule wykorzystywano, jak poprzednio, urządzenie mobilne – telefon Nokia Lumia 800 (dalej używana będzie nazwa smartfon). Podstawowe parametry smartfona – system operacyjny MS Windows Phone 7.5 Mango, jednordzeniowy procesor Qualcomm MSM8255T z zegarem 1,40 GHz. Typ ekranu – wyświetlacz pojemnościowy z wielodotykiem (funkcja multi-touch) o rozmiarze 3,7”. Technologia wykonania wyświetlacza AMOLED z wykorzystaniem ClearBlack, pozwalająca na pracę w rozdzielczości WVGA (480 × 800 px, 252 ppi ~54,7% screen-to-body ratio) [14], [15]. Użycie wyświetlacza pojemnościowego wykluczało wykorzystanie w działaniach rysika.

4.2. Aplikacja umożliwiająca przeprowadzenie badań

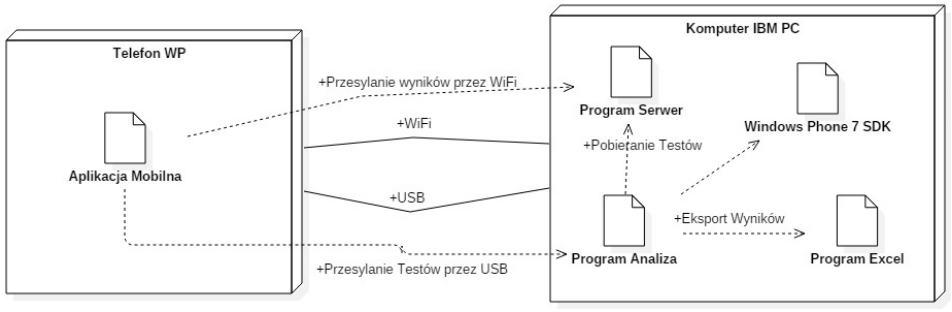
Do badań wykorzystano aplikację, której opis przedstawiony jest w artykułach [1] i [2]. Dla porządku przypominamy krótko ten opis.

Aplikacja umożliwiająca badanie miała budowę modułową (rys. 1) [7]:

– moduł *Aplikacja Mobilna* uruchamiany na telefonie działającym pod kontrolą systemu Windows Phone,

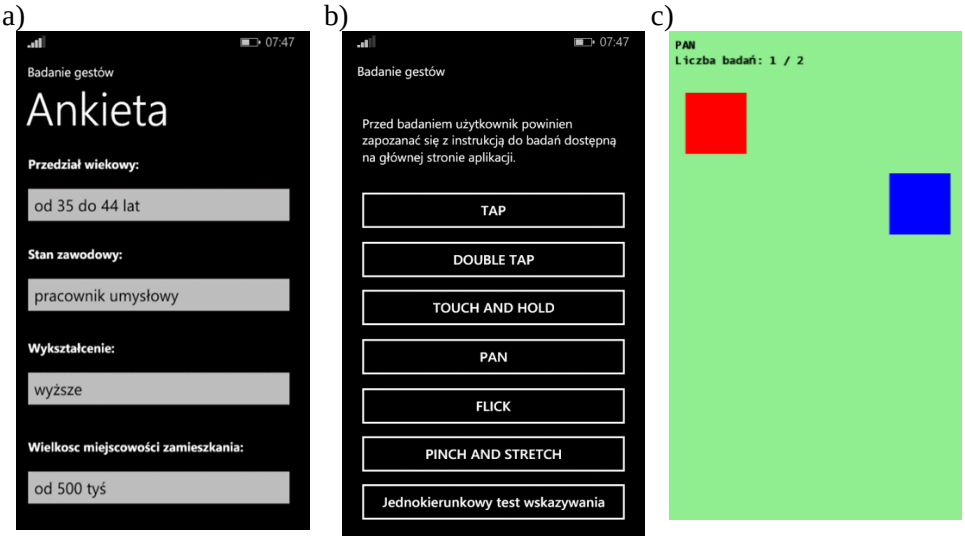
– moduł *Program Analiza* uruchamiany na komputerze klasy IBM PC z zainstalowanym systemem operacyjnym Windows 7,

– moduł *Program Serwer* – webservice uruchamiany na komputerze klasy IBM PC.



Rys. 1. Architektura aplikacji umożliwiającej przeprowadzenie badań [7]

Osoba wykonująca badanie, po uruchomieniu modułu *Aplikacja Mobilna*, wypełniała krótką ankietę (rys. 2a), po czym wykonywała określone gesty ustaloną liczbę powtórzeń (rys. 2b). Przykładowy ekran pokazujący stan po wyświetleniu obiektów i przed wykonaniem gestu pokazano na rysunku 2c.



Rys. 2. Aplikacja Mobilna a) ankieta, b) rodzaje pomiarów, c) widok w czasie wykonywania jednego gestu pan [7]

Wyniki badań były przesyłane z modułu *Aplikacja Mobilna* do modułu *Program Analiza* z wykorzystaniem webservice'u *Program Serwer* poprzez połączenie WiFi albo bezpośrednio z modułu *Aplikacja Mobilna* do modułu *Program Analiza* z wykorzystaniem połączenia przez interfejs USB. *Program*

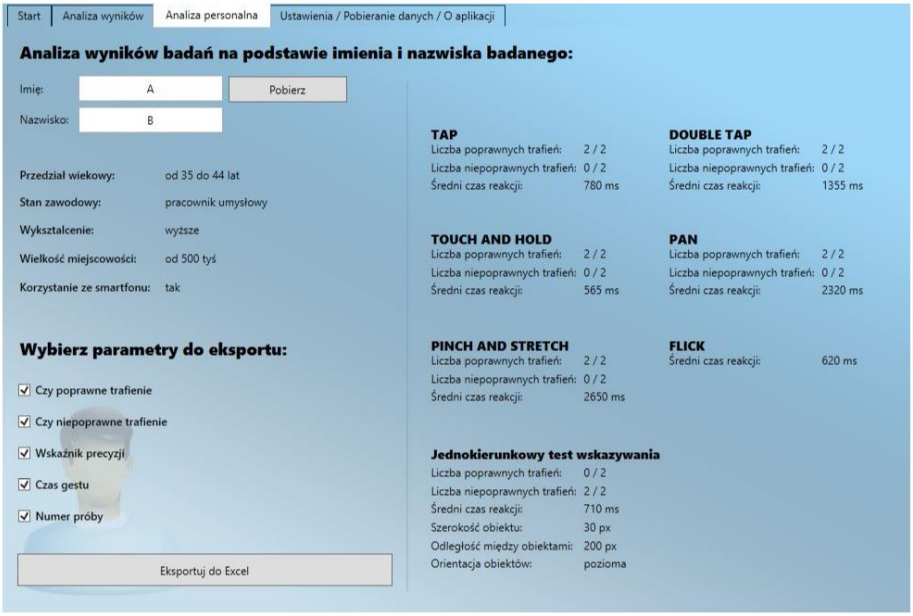
Analiza (rys. 3) miał możliwość prezentacji wyników całościowych (wszystkich badanych) i pojedynczego badania (gestu albo osoby).

Wybrane wyniki pomiarów można było wyeksportować z modułu *Program Analiza* do pliku w formacie Excel. W przedstawionych badaniach wykorzystano możliwość eksportu wyników do pliku w formacie Excel w celu dalszego przetwarzania. Podstawowymi danymi, do których możliwy był dostęp w ramach pliku w formacie Excel, były:

– informacja, czy trafiono w obiekt czy nie,

– odległość pomiędzy obiektem i palcem w chwili dotknięcia ekranu,

– czas wykonania gestu.



Rys. 3. Fragment zobrazowania w module *Program Analiza* [7]

4.3. Liczba osób badanych i warunki prowadzenia badań

Liczba osób badanych i warunki prowadzenia badań były takie same, jak podane w artykule [1].

Liczbę osób objętych badaniami podano w tabeli 1. Osobami badanymi było 60 osób w wieku 16-66 lat z przewagą osób młodych i w średnim wieku. Wyróżniono pięć grup wiekowych oznaczonych cyframi od 1 do 5. Wśród osób badanych były 2 kobiety.

Tab. 1. Liczba osób objętych badaniami

Przedział wiekowy [lat]	16-24	25-34	35-44	45-54	≥55	Razem
Numer grupy	1	2	3	4	5	
Liczba osób	14	5	23	13	5	60

Osobami badanymi byli głównie mężczyźni, pracownicy umysłowi z wykształceniem wyższym oraz kilku uczniów i studentów z wykształceniem średnim. Wśród badanych osób część osób używała smartfona codziennie, a część nie używała (tab. 2). Wszystkie osoby powtarzały gesty 30 razy.

Tab. 2. Liczba osób używających i nie używających smartfona codziennie

Cecha	Używa smartfon	Nie używa smartfon
Liczba osób	48	12

Badania wykonywano w pomieszczeniu w godzinach 8.00-16.00. Smartfon był trzymany w pozycji pionowej w lewej ręce (wśród osób badanych nie było osób leworęcznych). Osoby badane nie poruszały się, najczęściej siedziały (nie chodziły). Kolejny obiekt (cel) do wykonania akcji przez osobę badaną wyświetlany był bezpośrednio po zakończeniu poprzedniego gestu. Przed badaniami nie były przeprowadzane żadne próby zapoznawcze ani treningowe.

W badaniach, których wyniki są przedstawione w niniejszym artykule, stosowano gesty pinch and stretch oraz gesty wskazywania przy wykonywaniu jednokierunkowego testu wskazywania.

Podstawowymi parametrami wyznaczanymi na podstawie wykonywanych pomiarów były:

− średni czas wykonania gestu przez użytkownika,

− średnia precyzja wykonania gestu.

Do wykonania obliczeń w niniejszym artykule wykorzystano odpowiednie do warunków testy statystyczne [8], [9], [13]. Bezpośrednie obliczenia i wykresy wykonano, wykorzystując oprogramowanie do obliczeń naukowo-technicznych MATLAB [12].

5. Wyniki badań gestu pinch and stretch

Gest pinch and stretch w badaniach polegał na przeciąganiu (ściąganiu) ku sobie palców na ekranie (pinch – zmniejszanie, przycinanie) lub odsuwaniu od siebie dwóch palców na ekranie (stretch – rozciąganie, powiększanie). Gest

kończył się podniesieniem palców. Obiekt, który poddawany był manipulacjom w badaniach to czerwony kwadrat o wymiarach to 100 × 100 pikseli (rys. 4). Jego rozmiary zostały ustalone na 100 × 100 pix, jest to nieco większy rozmiar niż palec, który dotyka powierzchni ekranu.

Wielkości mierzone i rejestrowane dla osoby badanej (rys. 5):

x_{11}, y_{11} – współrzędne wierzchołka obiektu celu (kwadrat 1),

x_{12}, y_{12} – współrzędne wierzchołka obiektu zmienianego przez użytkownika (kwadrat 2),

t_a – chwila wyświetlenia obiektów (kwadratów) na ekranie,

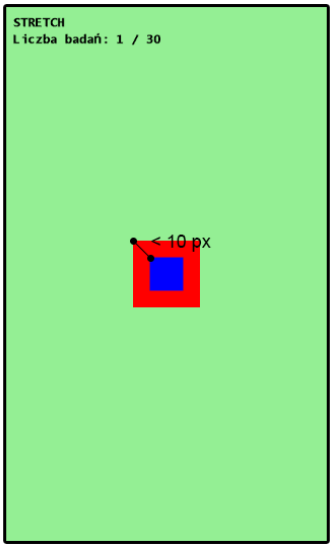
t_b – chwila oderwania pierwszego z palców od powierzchni ekranu.

Warunek poprawności wykonania gestu pinch and stretch:

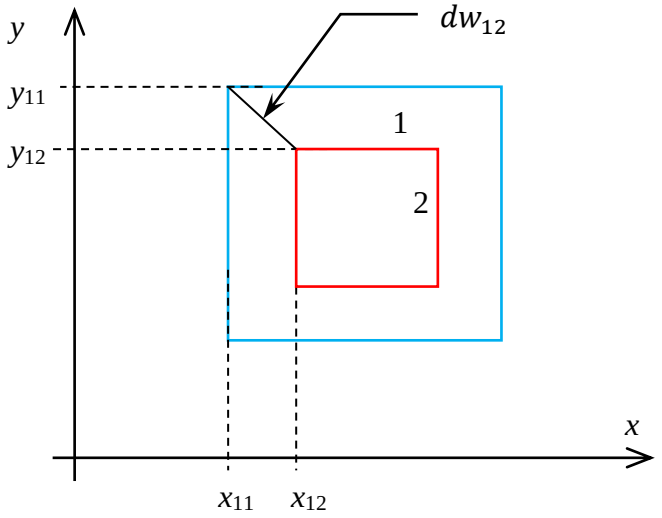
$$dw_{12} \leq 10 \tag{1}$$

gdzie: $dw_{12} = \sqrt{(x_{11} - x_{12})^2 + (y_{11} - y_{12})^2}$ – jak na rysunku 5.

Odległość dw_{12} pomiędzy kwadratami była wyznaczana na podstawie zarejestrowanych współrzędnych (w dalszej części artykułu odległość ta nazywana jest precyzją).



Rys. 4. Widok ekranu telefonu Nokia Lumia 800 przy wykonywaniu gestu pinch and stretch



Rys. 5. Ilustracja położenia obiektu – celu (kwadrat 1) i obiektu zmienianego przez użytkownika kwadratu (2) na cel na ekranie przy geście pinch and stretch, gdzie: $(x_{11}, y_{11}), (x_{12}, y_{12})$ – współrzędne wierzchołków kwadratów odpowiednio pierwszego i drugiego

Czas t_1 wykonania gestu pan przez użytkownika:

$$t_1 = t_b - t_a \ ,$$

gdzie: t_a – chwila wyświetlenia obiektów (kwadratów),

t_b – chwila oderwania pierwszego z palców przez użytkownika od powierzchni ekranu.

Po wykonaniu pomiarów wyznaczane były średnia precyzja gestu, średni czas wykonania gestu i prawdopodobieństwo błędu wykonania gestu pinch and stretch.

Średnia precyzja $\overline{dw}_{12}$ gestu:

$$\overline{dw}_{12} = \frac{1}{n}\sum_1^n dw_{12\,i}, \tag{2}$$

gdzie: $dw_{12\,i}$ – precyzja gestu w i-tym pomiarze,

n – liczba powtórzeń gestu ($n = 30$).

Średni czas $\bar{t}_1$ wykonania gestu:

$$\bar{t}_1 = \frac{1}{n}\sum_1^n t_{1\,i}\ , \tag{3}$$

gdzie: $t_{1\,i}$ – czas wykonania gestu w i-tym pomiarze,

n – liczba powtórzeń gestu ($n = 30$).

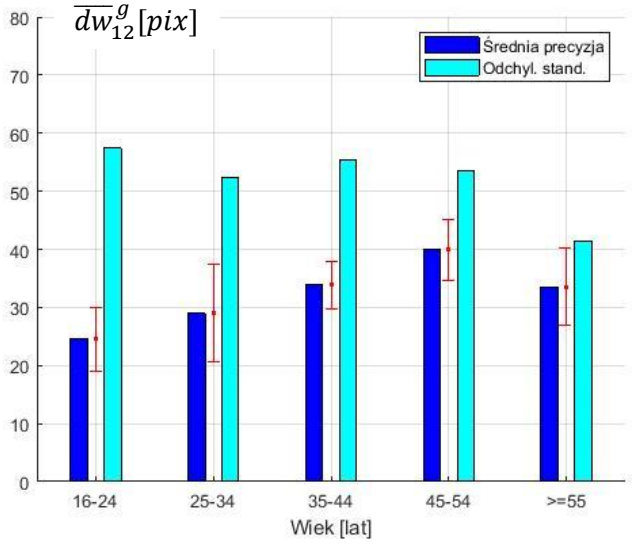
Prawdopodobieństwo błędu wykonania gestu pinch and stretch wyznaczono, wykorzystując warunek poprawności wykonania gestu (por. zależność (1)).

W celu wykonania odpowiednich porównań wyznaczono średnią precyzję $\overline{dw}_{12}^{g}$ wykonania gestu pinch and stretch w grupie wiekowej g, $g \in \{1, 2, 3, 4, 5\}$. Wyniki obliczeń podano w tabeli 3.

Tab. 3. Średnia precyzja $\overline{dw}_{12}^{g}$ wykonania gestu pinch and stretch w grupach wiekowych (wszystkie gesty)

Przedział wiekowy [lat]	16-24	25-34	35-44	45-54	≥55
Grupa g	1	2	3	4	5
Średnia precyzja $\overline{dw}_{12}^{g}$ wykonania gestu pan [pix]	24,6	29,0	33,9	39,9	33,5
Odchylenie standardowe precyzji [pix]	57,5	52,3	55,4	53,5	41,4

Analiza wartości średniej precyzji dla tego gestu wskazuje, że znaczna liczba gestów wykonanych przez osoby badane zakończyła się w większej odległości od celu. Potwierdzają to również znaczne wartości odchylenia standardowego precyzji (patrz tab. 3). Średnią precyzję, odchylenie standardowe precyzji i przedziały ufności precyzji wykonania gestu pinch and stretch przez osoby w grupach wiekowych dla wszystkich gestów pokazano na rysunku 6.



Rys. 6. Średnia precyzja $\overline{dw}_{12}^{g}$, odchylenie standardowe precyzji i przedziały ufności precyzji wykonania gestu pinch and stretch przez osoby w grupach wiekowych (wszystkie gesty)

Wykonano porównanie wyników badań pomiędzy grupami wiekowymi – w szczególności pomiędzy pierwszą grupą wiekową i pozostałymi grupami.

Sformułowano następujące hipotezy dla średniej precyzji wykonania gestu:

H0: średnie precyzje równe w grupach wiekowych 1 i j ($\overline{dw}_{12}^{i} = \overline{dw}_{12}^{j}$),

H1: średnie precyzje różne w grupach wiekowych 1 i j ($\overline{dw}_{12}^{i} \neq \overline{dw}_{12}^{j}$).

Biorąc pod uwagę fakt, że próby są liczne, wykorzystano typowy test do porównywania średnich [8], [9]. Testowanie hipotez wykonano na poziomie istotności $\alpha = 0{,}05$, natomiast wyniki porównania przedstawiono w tabeli 4.

Tab. 4. Wyniki porównania średniej precyzji wykonania gestu pinch and stretch przez użytkowników pomiędzy grupą pierwszą i pozostałymi grupami wiekowymi

Porównywane grupy	1-2	1-3	1-4	1-5
Decyzja o wyniku porównania średniej precyzji	Nie ma podstaw do odrzucenia H0	Odrzucić H0	Odrzucić H0	Odrzucić H0

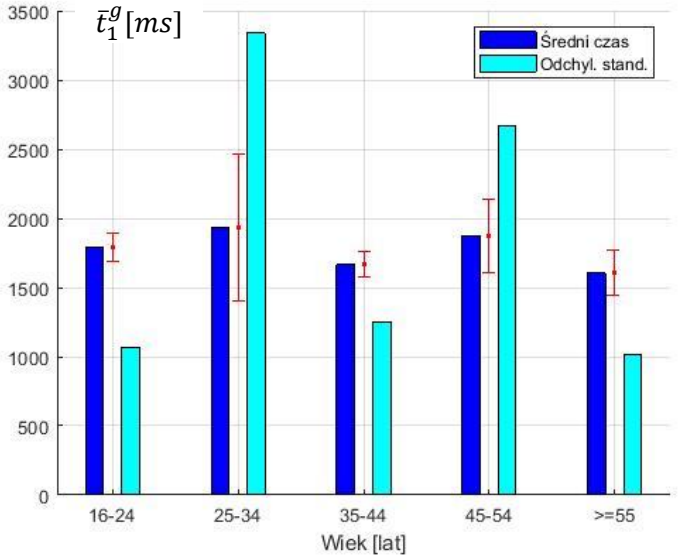
Dla przeprowadzonych badań wyznaczono średni czas $\bar{t}_1^g$ wykonania gestu pinch and stretch w grupie wiekowej g, $g \in \{1, 2, 3, 4, 5\}$. Poza średnim czasem wykonania gestu w grupie wiekowej, wyznaczono odchylenie standardowe czasu wykonania gestu i przedziały ufności dla czasu wykonania gestu w każdej grupie wiekowej.

Wyniki obliczeń średniego czasu wykonania gestu dla wszystkich gestów i dla gestów poprawnie wykonanych (warunek (1) spełniony) podano w tabeli 5.

Średni czas, odchylenie standardowe czasu i przedziały ufności czasu wykonania gestu pinch and stretch przez osoby w grupach wiekowych dla wszystkich gestów pokazano na rysunku 7, a dla gestów poprawnych (warunek (1) spełniony) na rysunku 8.

Tab. 5. Średni czas $\bar{t}_1^g$ wykonania gestu pinch and stretch w grupach wiekowych

Przedział wiekowy [lat]	16–24	25–34	35–44	45–54	≥55
Grupa g	1	2	3	4	5
Średni czas $\bar{t}_1^g$ wykonania gestu pinch and stretch (gesty wszystkie) [ms]	1791,9	1932,5	1666,1	1870,4	1603,9
Średni czas $\bar{t}_1^g$ wykonania gestu pinch and stretch (gesty, dla których spełniony jest warunek (1)) [ms]	2133,7	2105,3	2155,2	2354,6	1913,4



Rys. 7. Średni czas $\bar{t}_1^g$ wykonania gestu, odchylenie standardowe i przedziały ufności czasu wykonania gestu pinch and stretch przez osoby w grupach wiekowych (wszystkie gesty)

Gdy porówna się wartości średniego czasu wykonania gestu w grupach wiekowych (tab. 5), widoczny jest wyraźny wzrost tego czasu dla gestów poprawnych, dla których warunek poprawności (dokładności wykonania gestu) jest spełniony (warunek (1)). Wykonano porównanie wyników badań średniego czasu wykonania gestu pinch and stretch pomiędzy pierwszą grupą wiekową i pozostałymi grupami.

Sformułowano następujące hipotezy dla średniego czasu wykonania gestu:

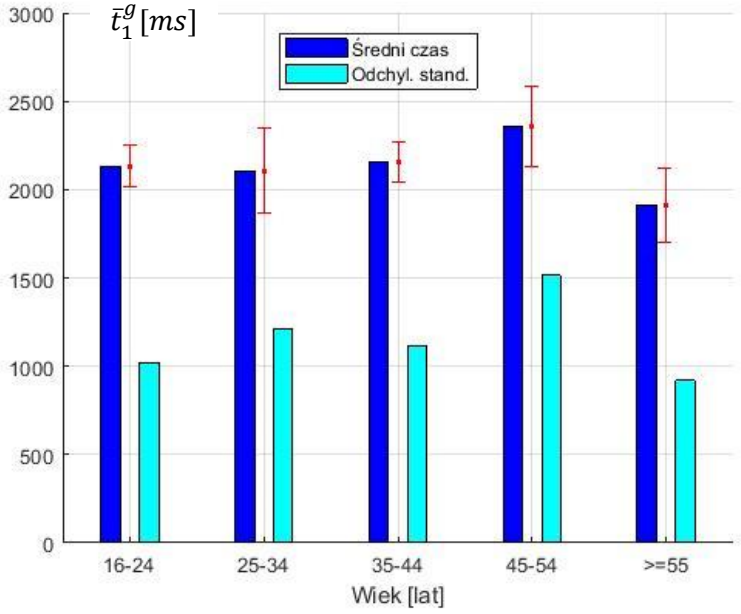
H0: średnie czasy równe w grupach wiekowych 1 i j ($\bar{t}_1^1 = \bar{t}_1^j$),

H1: średnie czasy różne w grupach wiekowych 1 i j ($\bar{t}_1^1 \neq \bar{t}_1^j$).

Biorąc pod uwagę fakt, że próby są liczne, wykorzystano typowy test do porównywania średnich [8], [9]. Testowanie hipotez wykonano na poziomie istotności $\alpha = 0{,}05$, natomiast wyniki weryfikacji hipotez podano w tabeli 6.

Tab. 6. Wyniki porównania średniego czasu wykonania gestu pinch and stretch przez użytkowników pomiędzy grupą pierwszą i pozostałymi grupami wiekowymi

Porównywane grupy	1-2	1-3	1-4	1-5
Decyzja o wyniku porównania średniego czasu	Nie ma podstaw do odrzucenia H0	Nie ma podstaw do odrzucenia H0	Nie ma podstaw do odrzucenia H0	Nie ma podstaw do odrzucenia H0



Rys. 8. Średni czas $\bar{t}_1^g$ wykonania gestu, odchylenie standardowe i przedziały ufności czasu wykonania gestu pinch and stretch przez osoby w grupach wiekowych (gesty poprawne – warunek (1))

Wyniki porównania wartości średniego czasu wykonania gestu w grupach wiekowych podane w tabeli 6 są takie same dla wszystkich gestów oraz dla gestów, dla których spełniony jest warunek (1).

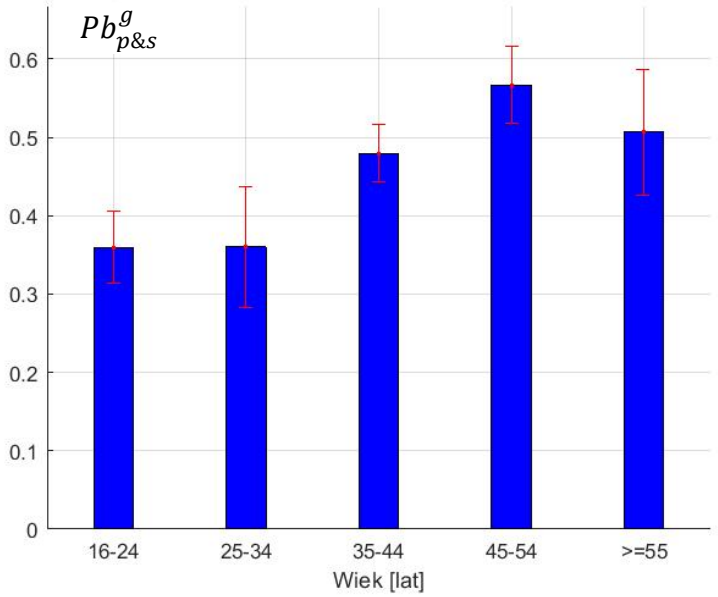
Biorąc pod uwagę warunek poprawności wykonania gestu pinch and stretch (warunek (1)), wyznaczono prawdopodobieństwo $Pb_{p\&s}^g$ błędu wykonania gestu pinch and stretch w grupach wiekowych. Wyniki przedstawiono na rysunku 9.

Sformułowano następujące hipotezy dla prawdopodobieństwo $Pb_{p\&s}^g$ błędu wykonania gestu pinch and stretch:

H0: prawdopodobieństwo błędu równe w grupach wiekowych 1 i j ($Pb_{p\&s}^1 = Pb_{p\&s}^j$),

H1: prawdopodobieństwo błędu różne w grupach wiekowych 1 i j ($Pb_{p\&s}^1 = Pb_{p\&s}^j$).

Biorąc pod uwagę fakt, że próby są liczne, wykorzystano typowy test do porównywania wskaźników struktury [7], [8]. Testowanie hipotez wykonano na poziomie istotności $\alpha = 0{,}05$, natomiast wyniki weryfikacji hipotez podano w tabeli 7.



Rys. 9. Prawdopodobieństwo błędu $Pb^{g}_{p\&s}$ i przedziały ufności dla gestu pinch and stretch w grupach wiekowych (warunek poprawności (1))

Tab. 7. Wyniki porównania prawdopodobieństwa błędu $Pb^{g}_{p\&s}$ gestu pinch and stretch dla osób pomiędzy grupą wiekową pierwszą i pozostałymi grupami wiekowymi

Porównywane grupy	1-2	1-3	1-4	1-5
Decyzja o wyniku porównania prawdopodobieństwa błędu	Nie ma podstaw do odrzucenia H0	Odrzucić H0	Odrzucić H0	Odrzucić H0

Przyjmijmy następujące oznaczenia.

$\overline{dw}^{u}_{12}$ – średnia precyzja wykonania gestu pinch and stretch przez użytkowników używających smartfona codziennie,

$\overline{dw}^{n}_{12}$ – średnia precyzja wykonania gestu pinch and stretch przez użytkowników nie używających smartfona codziennie,

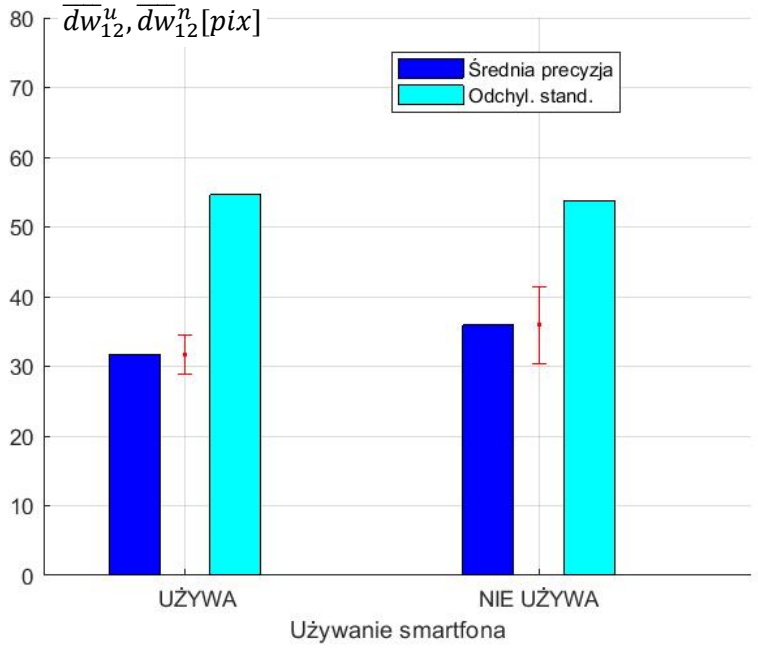
$\bar{t}^{u}_{1}$ – średni czas wykonania gestu pinch and stretch przez użytkowników używających smartfona codziennie,

$\bar{t}^{n}_{1}$ – średni czas wykonania gestu pinch and stretch przez użytkowników nie używających smartfona codziennie,

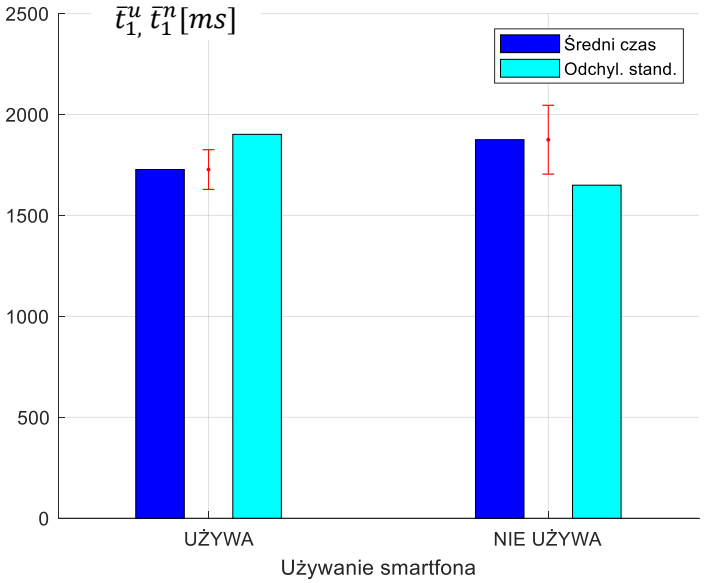
$Pb^{u}_{p\&s}$ – prawdopodobieństwo błędu w wykonaniu gestu pinch and stretch przez użytkowników używających smartfona codziennie,

$Pb^{n}_{p\&s}$ – prawdopodobieństwo błędu w wykonaniu gestu pinch and stretch przez użytkowników nie używających smartfona codziennie.

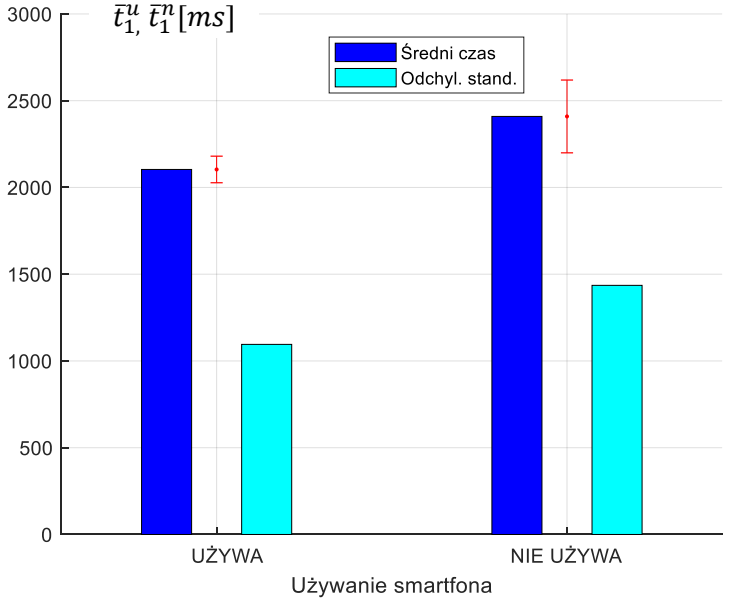
Na podstawie wyników badań wyznaczono średnią precyzję gestu, średni czas wykonania gestu i prawdopodobieństwo błędu wykonania gestu pinch and stretch w grupach osób używających smartfon codziennie i nie używających smartfona codziennie. Uzyskane wyniki dotyczące średniej precyzji gestu i średniego czasu wykonania gestu przedstawiono na rysunkach 10-12. Na rysunku 10 przedstawiono wyniki obliczeń dotyczące średniej precyzji gestu, natomiast na rysunku 11 – wyniki obliczeń średniego czasu gestu w obu grupach dla wszystkich gestów. Na rysunku 12 przedstawiono wyniki średniego czasu gestu w obu grupach dla gestów poprawnie wykonanych (warunek poprawności (1). Zauważyć można znaczne wartości odchylenia standardowego średniej precyzji wykonania gestu w grupach osób używających i nie używających smartfona codziennie. Podobnie widoczne są znaczne wartości odchylenia standardowego średniego czasu wykonania gestu, ale tylko w sytuacji, gdy uwzględniamy wszystkie gesty.



Rys. 10. Średnia precyzja, odchylenie standardowe precyzji i przedziały ufności precyzji wykonania gestu pinch and stretch przez osoby używające i nie używające smartfona codziennie

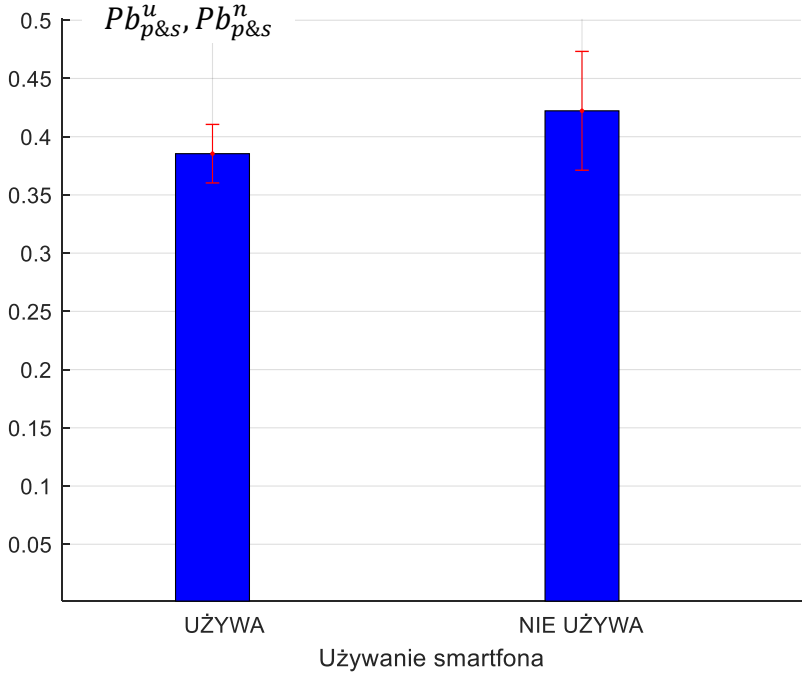


Rys. 11. Średni czas, odchylenie standardowe i przedziały ufności czasu wykonania gestu pinch and stretch przez osoby używające i nie używające smartfona codziennie (gesty wszystkie)



Rys. 12. Średni czas, odchylenie standardowe i przedziały ufności czasu wykonania gestu pinch and stretch przez osoby używające i nie używające smartfona codziennie (gesty poprawne – warunek (1))

Wyniki badań dotyczące prawdopodobieństwa błędu w wykonaniu gestu pinch and stretch w grupach osób używających i nie używających smartfona codziennie przedstawiono na rysunku 13. Poziom błędów w wykonaniu gestu pinch and stretch w obu grupach jest dość znaczny.



Rys. 13. Prawdopodobieństwo błędu i przedziały ufności prawdopodobieństwa błędu w wykonaniu gestu pinch and stretch przez osoby używające i nie używające smartfona codziennie

Sprawdzono również, czy fakt używania smartfona codziennie ma wpływ na jakość działania użytkowników (na jakość wykonania gestu pinch and stretch). Sformułowano następujące hipotezy:

H0: średnie precyzje równe (używający, nie używający smartfona) ($\overline{dw}^u_{12} = \overline{dw}^n_{12}$),

H1: średnie precyzje różne ($\overline{dw}^u_{12} \neq \overline{dw}^n_{12}$),

H0: średnie czasy wykonania gestu równe ($\bar{t}^u_1 = \bar{t}^n_1$),

H1: średnie czasy wykonania gestu różne ($\bar{t}^u_1 \neq \bar{t}^n_1$),

H0: prawdopodobieństwa błędu wykonania gestu równe ($Pb^u_{p\&s} = Pb^n_{p\&s}$),

H1: prawdopodobieństwa błędu wykonania gestu różne ($Pb^u_{p\&s} \neq Pb^n_{p\&s}$).

Do porównania wartości wykorzystano odpowiednie typowe testy [8], [9], [13]. Testowanie hipotez wykonano na poziomie istotności $\alpha = 0{,}05$, a wyniki weryfikacji podano w tabeli 8.

Tab. 8. Wyniki porównania średniego czasu i średniej precyzji w wykonaniu gestu pinch and stretch przez osoby używające i nie używające smartfona codziennie (gesty wszystkie)

Porównywany parametr	Średnia precyzja wykonania gestu	Średni czas wykonania gestu	Prawdopodobieństwo błędu w wykonaniu gestu
Decyzja o wyniku porównania	Nie ma podstaw do odrzucenia H0	Nie ma podstaw do odrzucenia H0	Nie ma podstaw do odrzucenia H0

Biorąc pod uwagę średni czas wykonania gestu pinch and stretch, ale tylko dla gestów poprawnych (warunek (1) spełniony), należy odrzucić hipotezę H0 o równości czasów na korzyść hipotezy alternatywnej.

Komentarze i wnioski z wyników badań

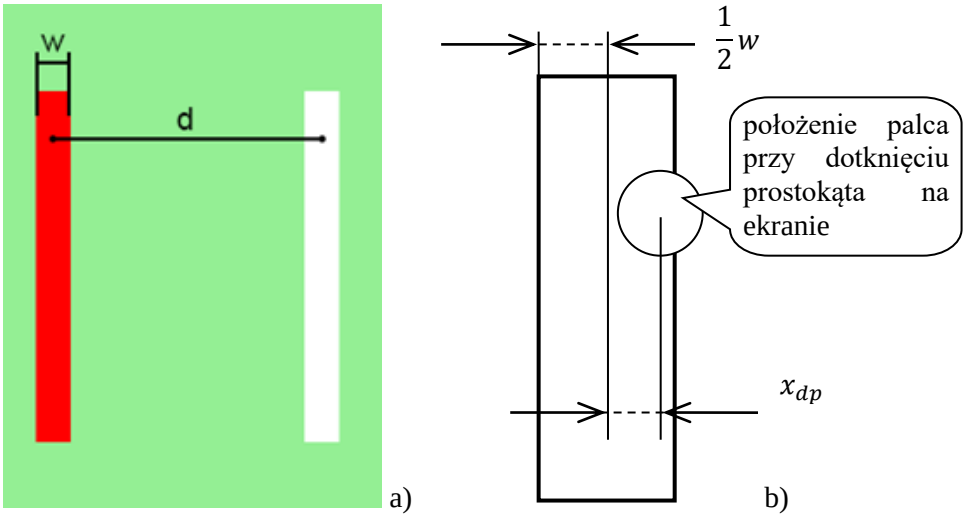
Na podstawie uzyskanych wyników badań można zaobserwować dość znaczne wartości odchylenia standardowego średniej precyzji wykonania gestu pinch and stretch we wszystkich grupach wiekowych podobnie jak dla gestu pan (por. artykuł [2]). Występują również różnice w średniej precyzji wykonania gestu pomiędzy pierwszą i trzecią, czwartą i piątą grupą wiekową (por. tab. 4). Wyniki porównania wartości średniego czasu wykonania gestu w grupach wiekowych nie wskazują na różnice (por. tab. (6)).

Wyniki badań wskazują również na znaczne wartości prawdopodobieństwa błędu wykonania gestu pinch and stretch w grupach wiekowych, podobnie jak dla gestu pan (por. artykuł [2]). Wyniki te wskazują na znaczne utrudnienie, jakim jest warunek poprawności (1). Dla czasu wykonania gestu (wszystkie gesty) tylko w dwóch grupach wiekowych (25-34 i 45-54) stwierdzono znaczne wartości odchylenia standardowego czasu wykonania gestu. Dla gestów poprawnych (spełniony warunek (1)) nie występuje taka sytuacja.

Biorąc pod uwagę osoby używające i nie używające smartfona codziennie, wyniki badań wykazały, że nie ma podstaw do odrzucenia hipotezy H0 o równości średniej precyzji wykonania gestu, średniego czasu wykonania gestu i prawdopodobieństwa błędu w wykonaniu gestu pinch and stretch pomiędzy tymi grupami osób.

6. Wyniki badań wskazań w jednokierunkowym teście wskazywania

Jednokierunkowy test wskazywania wykonywany jest następująco [10], [11]. Użytkownikowi przedstawiane są na ekranie dwa prostokąty o szerokości *w* i odległości *d* pomiędzy środkami prostokątów (rys. 14). Zadanie użytkownika polega na wskazywaniu prostokątów palcem na przemian (prawy, lewy). Każda seria testowa (30 dotknięć każdego prostokąta) rozpoczyna się wówczas, gdy zostaną wyświetlone prostokąty. Użytkownik dotyka czerwonego prostokąta, dotknięty prostokąt zmienia kolor na biały, a przeciwległy prostokąt staje się czerwony.



Rys. 14. Jednokierunkowy test wskazywania (a – widok ekranu telefonu, b – położenie palca przy dotknięciu prostokąta na ekranie i precyzja x_{dp} dotknięcia)

W badaniach zastosowano następujące warunki:

– szerokość obiektów (prostokątów) $w = 30\ [pix]$,

– odległość między prostokątami $d = 200\ [pix]$,

– orientacja pozioma.

Dane rejestrowane osoby badanej:

– przedział wiekowy (16-24, 25-34, 35-44, 45-54, ≥55) lat;

– używanie smartfona codziennie: tak, nie.

Wielkości mierzone dla osoby badanej:

x_{dp} – precyzja dotknięcia obiektu (prostokąta),

t_a – chwila podświetlenia obiektu (prostokąta),

t_b – chwila dotknięcia palcem do powierzchni ekranu.

Przyjęto następującą wartość warunku poprawności wykonania wskazania (dotknięcia):

$$x_{dp} \leq 15\ [pix], \tag{4}$$

gdzie: x_{dp} – jak na rysunku 14.

W czasie badania wyznaczany był czas wskazania:

$$t_1 = t_b - t_a\ ,$$

gdzie: t_a – chwila podświetlenia obiektu (prostokąta),

t_b – chwila dotknięcia palcem do powierzchni ekranu.

Po wykonaniu pomiarów wyznaczane były średnia precyzja wskazania, średni czas wskazania i prawdopodobieństwo błędu wskazania.

Prawdopodobieństwo błędu wykonania wskazania w teście jednokierunkowym wyznaczono, wykorzystując warunek poprawności wykonania gestu (por. zależność (4)).

W celu wykonania odpowiednich porównań wyznaczono średnią precyzję $\bar{x}_{dp}^{g}$ wskazania w teście jednokierunkowym w grupie wiekowej g, $g \in \{1, 2, 3, 4, 5\}$. Wyniki obliczeń podano w tabeli 9.

Tab. 9. Średnia precyzja $\bar{x}_{dp}^{g}$ wykonania wskazania w grupie wiekowej g

Przedział wiekowy [lat]	16-24	25-34	35-44	45-54	≥55
Grupa g	1	2	3	4	5
Średnia precyzja $\bar{x}_{dp}^{g}$ wskazania [pix]	14,8	16,4	14,7	14,1	18,2

Średnią precyzję, odchylenie standardowe precyzji i przedziały ufności precyzji wskazania w teście jednokierunkowym przez osoby w grupach wiekowych pokazano na rysunku 15.

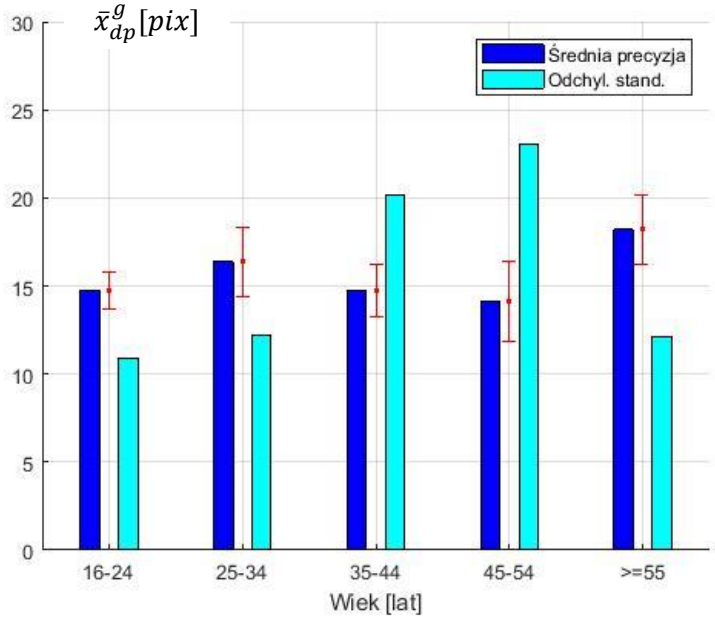
Wykonano porównanie wyników badań pomiędzy grupami wiekowymi – w szczególności pomiędzy pierwszą grupą wiekową i pozostałymi grupami.

Sformułowano następujące hipotezy dla średniej precyzji wykonania wskazania:

H0: średnie precyzje równe w grupach wiekowych 1 i j ($\bar{x}_{dp}^{i} = \bar{x}_{dp}^{j}$),

H1: średnie precyzje różne w grupach wiekowych 1 i j ($\bar{x}_{dp}^{i} \neq \bar{x}_{dp}^{j}$).

Biorąc pod uwagę fakt, że próby są liczne, wykorzystano typowy test do porównywania średnich [8], [9]. Testowanie hipotez wykonano na poziomie istotności $\alpha = 0{,}05$, natomiast wyniki porównania przedstawiono w tabeli 10.



Rys. 15. Średnia precyzja $\bar{x}_{dp}^{g}$, odchylenie standardowe precyzji i przedziały ufności precyzji wykonania wskazania w teście jednokierunkowym przez osoby w grupach wiekowych

Tab. 10. Wyniki porównania średniej precyzji wykonania wskazania przez użytkowników pomiędzy grupą pierwszą i pozostałymi grupami wiekowymi

Porównywane grupy	1-2	1-3	1-4	1-5
Decyzja o wyniku porównania średniej precyzji	Nie ma podstaw do odrzucenia H0	Nie ma podstaw do odrzucenia H0	Nie ma podstaw do odrzucenia H0	Odrzucić H0

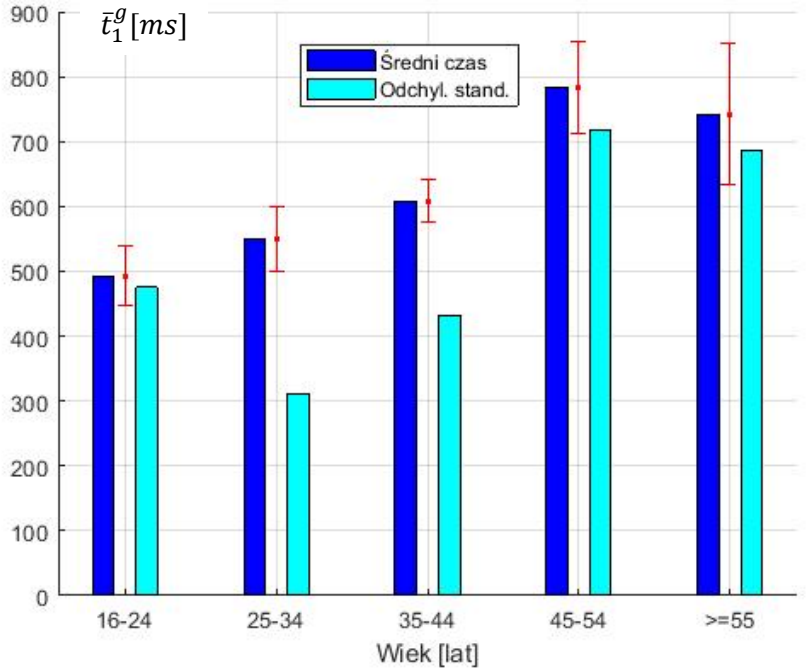
Dla przeprowadzonych badań wyznaczono średni czas $\bar{t}_1^g$ wykonania wskazania w teście jednokierunkowym w grupie wiekowej g, $g \in \{1, 2, 3, 4, 5\}$. Poza średnim czasem wykonania wskazania w grupie wiekowej, wyznaczono odchylenie standardowe czasu wykonania wskazania i przedziały ufności dla czasu wykonania wskazania w każdej grupie wiekowej.

Wyniki obliczeń średniego czasu wykonania wskazania dla wszystkich wykonanych wskazań i dla wskazań poprawnie wykonanych (warunek (4) spełniony) podano w tabeli 11.

Średni czas, odchylenie standardowe czasu i przedziały ufności czasu wykonania wskazania przez osoby w grupach wiekowych dla wszystkich wskazań pokazano na rysunku 16.

Tab. 11. Średni czas $\bar{t}_1^g$ wykonania wskazania w teście jednokierunkowym w grupie wiekowej g

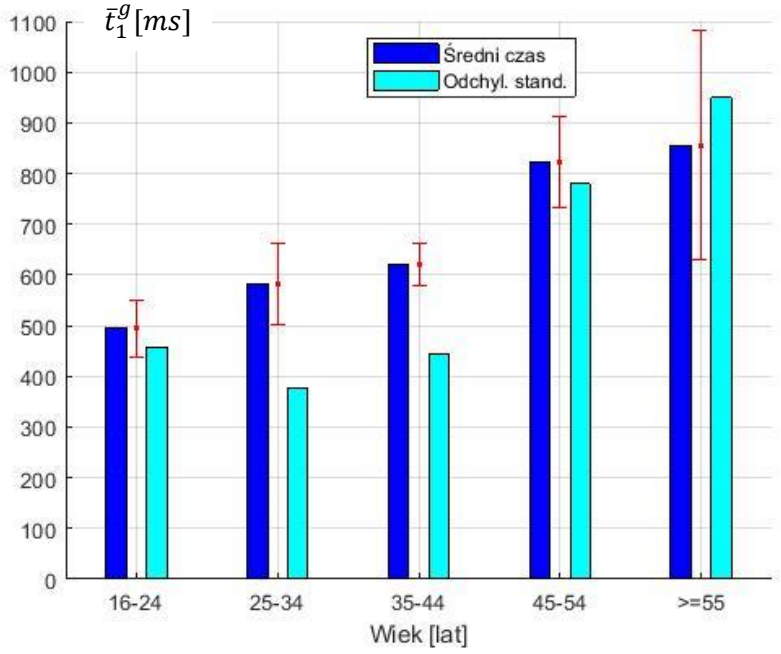
Przedział wiekowy [lat]	16-24	25-34	35-44	45-54	≥55
Grupa g	1	2	3	4	5
Średni czas $\bar{t}_1^g$ wykonania wskazania (wszystkie wskazania) [ms]	492,9	548,8	608,7	782,8	742,3
Średni czas $\bar{t}_1^g$ wykonania wskazania (wskazania poprawne) [ms]	494,8	582,6	620,2	822,6	855,1



Rys. 16. Średni czas $\bar{t}_1^g$ wykonania wskazania, odchylenie standardowe i przedziały ufności czasu wykonania wskazania przez osoby w grupach wiekowych (wszystkie wskazania)

Średni czas, odchylenie standardowe czasu i przedziały ufności czasu wykonania wskazania w teście jednokierunkowym przez osoby w grupach wiekowych dla wskazań poprawnie wykonanych (warunek (4) spełniony) pokazano na rysunku 17.

Wykonano porównanie średniego czasu wykonania wskazania w grupach wiekowych.



Rys. 17. Średni czas $\bar{t}_1^g$ wykonania wskazania, odchylenie standardowe i przedziały ufności czasu wykonania wskazania przez osoby w grupach wiekowych (wskazania poprawne)

Sformułowano następujące hipotezy dla średniego czasu wykonania wskazania w teście jednokierunkowym:

H0: średnie czasy równe w grupach wiekowych 1 i j ($\bar{t}_1^1 = \bar{t}_1^j$),

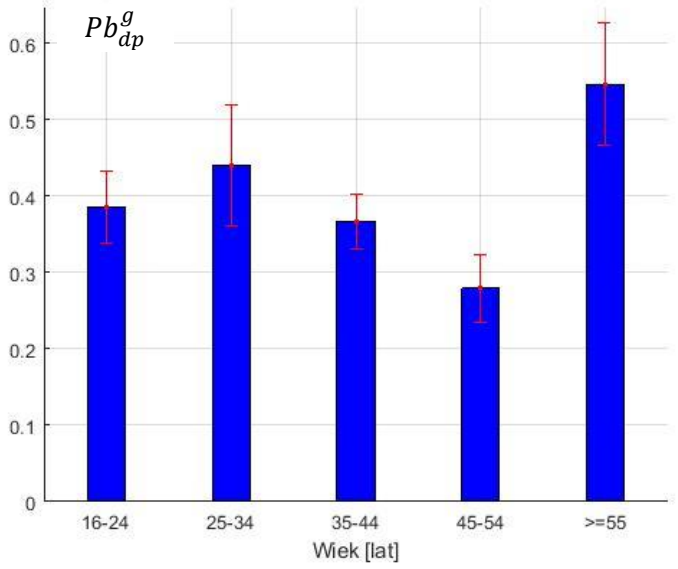
H1: średnie czasy różne w grupach wiekowych 1 i j ($\bar{t}_1^1 \neq \bar{t}_1^j$).

Biorąc pod uwagę fakt, że próby są liczne, wykorzystano typowy test do porównywania średnich [8], [9]. Testowanie hipotez wykonano na poziomie istotności $\alpha = 0{,}05$, natomiast wyniki weryfikacji hipotez podano w tabeli 12.

Tab. 12. Wyniki porównania średniego czasu wykonania wskazania przez użytkowników pomiędzy grupą pierwszą i pozostałymi grupami wiekowymi (wszystkie wskazania i wskazania poprawne)

Porównywane grupy	1-2	1-3	1-4	1-5
Decyzja o wyniku porównania średniego czasu wskazania	Nie ma podstaw do odrzucenia H0	Odrzucić H0	Odrzucić H0	Odrzucić H0

Biorąc pod uwagę warunek poprawności wskazania w teście jednokierunkowym (warunek (4)), wyznaczono prawdopodobieństwo Pb_{dp}^{g} błędu wykonania wskazania w teście jednokierunkowym w grupach wiekowych. Wyniki przedstawiono na rysunku 18.



Rys. 18. Prawdopodobieństwo błędu Pb_{dp}^{g} i przedziały ufności dla wskazań w teście jednokierunkowym przez osoby w grupach wiekowych

Sformułowano następujące hipotezy dla prawdopodobieństwa Pb_{dp}^{g} błędu wykonania wskazania w teście jednokierunkowym:

H0: prawdopodobieństwo błędu równe w grupach wiekowych 1 i j ($Pb_{dp}^{1} = Pb_{dp}^{j}$),

H1: prawdopodobieństwo błędu różne w grupach wiekowych 1 i j ($Pb_{dp}^{1} \neq Pb_{dp}^{j}$).

Biorąc pod uwagę fakt, że próby są liczne, wykorzystano typowy test do porównywania wskaźników struktury [8], [9], [13]. Testowanie hipotez wykonano na poziomie istotności $\alpha = 0{,}05$, natomiast wyniki weryfikacji hipotez podano w tabeli 13.

Przyjmijmy następujące oznaczenia:

$\bar{x}_{dp}^{u}$ – średnia precyzja wykonania wskazania przez użytkowników używających smartfona codziennie,

Tab. 13. Wyniki porównania prawdopodobieństwa Pb_{dp}^{g} błędu wskazania dla osób pomiędzy grupą wiekową pierwszą i pozostałymi grupami wiekowymi

Porównywane grupy	1-2	1-3	1-4	1-5
Decyzja o wyniku porównania prawdopodobieństwa błędu wskazania	Nie ma podstaw do odrzucenia H0	Nie ma podstaw do odrzucenia H0	Odrzucić H0	Odrzucić H0

$\bar{x}_{dp}^{n}$ – średnia precyzja wykonania wskazania użytkowników nie używających smartfona codziennie,

$\bar{t}_{1}^{u}$ – średni czas wykonania wskazania przez użytkowników używających smartfona codziennie,

$\bar{t}_{1}^{n}$ – średni czas wykonania wskazania przez użytkowników nie używających smartfona codziennie,

Pb_{dp}^{u} – prawdopodobieństwo błędu w wykonaniu wskazania przez użytkowników używających smartfona codziennie,

Pb_{dp}^{n} – prawdopodobieństwo błędu w wykonaniu wskazania przez użytkowników nie używających smartfona codziennie.

Na podstawie uzyskanych wyników badań wyznaczono średnią precyzję wykonania wskazania, średni czas wykonania wskazania i prawdopodobieństwo błędu wykonania wskazania w grupie osób używających smartfona codziennie i nie używających smartfona codziennie. Wyniki przedstawiono na rysunkach 19-21.

Sprawdzono również, czy fakt używania smartfona codziennie ma wpływ na jakość działania użytkowników wykonujących wskazania w teście jednokierunkowym. Sformułowano następujące hipotezy:

H0: średnie precyzje równe (używający, nie używający smartfona) ($\bar{x}_{dp}^{u} = \bar{x}_{dp}^{n}$),

H1: średnie precyzje różne ($\bar{x}_{dp}^{u} \neq \bar{x}_{dp}^{n}$),

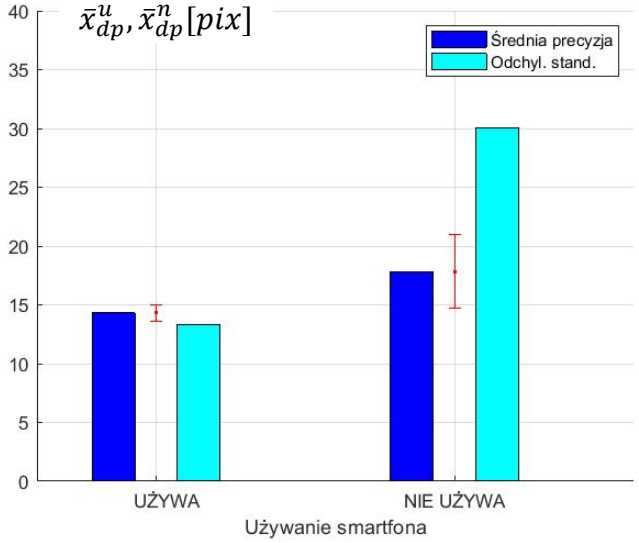
H0: średnie czasy równe ($\bar{t}_{1}^{u} = \bar{t}_{1}^{n}$),

H1: średnie czasy różne ($\bar{t}_{1}^{u} \neq \bar{t}_{1}^{n}$),

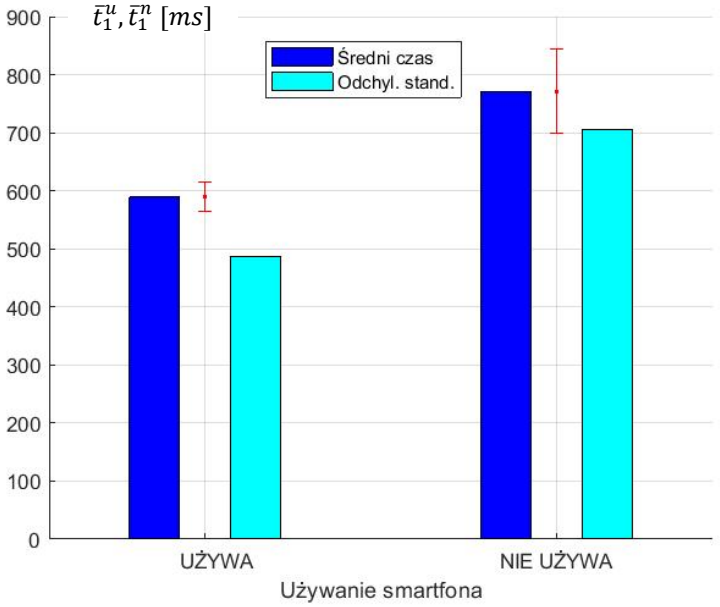
H0: prawdopodobieństwa błędu równe ($Pb_{dp}^{u} = Pb_{dp}^{n}$),

H1: prawdopodobieństwa błędu różne ($Pb_{dp}^{u} \neq Pb_{dp}^{n}$).

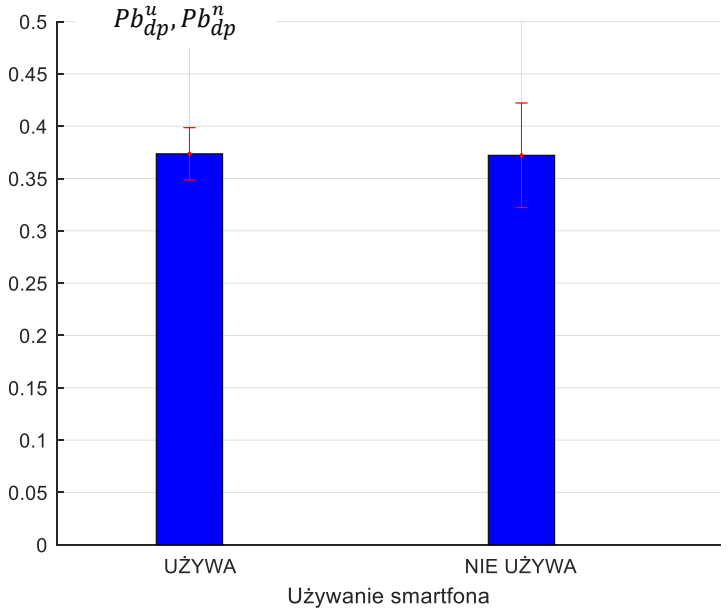
Testowanie hipotez wykonano na poziomie istotności $\alpha = 0{,}05$, wykorzystując typowe testy [8], [9], [13], a wyniki weryfikacji podano w tabeli 14.



Rys. 19. Średnia precyzja, odchylenie standardowe precyzji i przedziały ufności precyzji wykonania wskazania przez osoby używające i nie używające smartfona codziennie



Rys. 20. Średni czas, odchylenie standardowe czasu i przedziały ufności czasu wykonania wskazania przez osoby używające i nie używające smartfona codziennie



Rys. 21. Prawdopodobieństwo błędu i przedziały ufności prawdopodobieństwa błędu w wykonaniu wskazania przez osoby używające i nie używające smartfona

Tab. 14. Wyniki porównania średniego czasu, średniej precyzji i prawdopodobieństwa błędu w wykonaniu wskazania przez osoby używające i nie używające smartfon codziennie

Porównywany parametr	Średni czas	Średnia precyzja	Prawdopodobieństwo błędu
Decyzja o H0	Odrzucić H0	Odrzucić H0	Nie ma podstaw do odrzucenia H0

Komentarze i wnioski z wyników badań

Na podstawie uzyskanych wyników badań można zaobserwować stosunkowo umiarkowane wartości średniej precyzji wykonania wskazania, natomiast odchylenie standardowe średniej precyzji wykonania jest dość znaczne szczególnie w grupach wiekowych 35-44 i 45-54 lat. Wykonanie wskazania w teście jednokierunkowym jest dość podobne do gestu tap. Porównując wartości średniej precyzji i odchylenia standardowego precyzji z wartościami dla gestu tap (tab. 4 i rys. 6 w pracy [1]), można zauważyć, że wartości precyzji są trochę mniejsze, ale odchylenie standardowe precyzji większe, choć nierównomiernie wzrasta wraz z rosnącym wiekiem osób. Porównując średnią precyzję wykonania wskazania pomiędzy grupą wiekową

pierwszą a pozostałymi grupami, różnice występują tylko pomiędzy grupą pierwszą i ostatnią (najstarszą – wiek >=55 lat). W pozostałych przypadkach nie ma podstaw do odrzucenia hipotezy H0 o równości średniej precyzji wykonania wskazania.

Wartości średniego czasu wykonania wskazania w teście jednokierunkowym są mniejsze od wartości średniego czasu wykonania dla gestu tap i podobnie rosną wraz ze wzrostem wieku osób badanych. Wartości odchylenia standardowego czasu wskazania są nieco większe niż dla gestu tap i to zarówno dla wskazań wszystkich, jak i wskazań poprawnych (warunek (4) spełniony). Porównując średni czas wskazania pomiędzy grupami wiekowymi, stwierdzono brak różnic pomiędzy grupami 1 i 2, natomiast występują znaczne różnice pomiędzy średnim czasem wskazania pomiędzy grupą 1 i pozostałymi grupami wiekowymi. W tym zakresie jest pełna zgodność z wynikami porównania średniego czasu wykonania gestu tap (por. tab. 6 w pracy [1]).

Prawdopodobieństwo błędu wykonania wskazania w teście jednokierunkowym znacznie różni się od prawdopodobieństwa błędu dla gestu tap zarówno pod względem wartości prawdopodobieństwa, jak i zmiany wartości wraz ze wzrostem wieku osób badanych. Różnice wynikają z innego warunku poprawności wykonania wskazania. Dla grup wiekowych 1-2 i 1-3 nie ma podstaw do odrzucenia hipotezy H0 o równości prawdopodobieństwa błędu wskazania dla porównywanych grup. Dla pozostałych grup (1-4 i 1-5) należy odrzucić hipotezę H0 o równości prawdopodobieństwa błędu wskazania (por. tab. 13).

Biorąc pod uwagę osoby używające i nie używające smartfona codziennie, wyniki porównania średniej precyzji wykonania wskazania i prawdopodobieństwa błędu wykonania wskazania w teście jednokierunkowym są takie same jak gestu tap (por. praca [1]) – odrzucono hipotezę o równości średniego czasu wykonania wskazania i stwierdzono brak podstaw do odrzucenia hipotezy H0 o równości prawdopodobieństwa błędu wykonania wskazania dla osób używających i nie używających smartfona codziennie. Natomiast dla średniej precyzji wykonania wskazania brakuje zgodności wyników porównania dla wskazań w teście jednokierunkowym i dla gestu tap (por. praca [1]).

7. Podsumowanie

Niniejszy artykuł jest trzecią częścią szerszej pracy dotyczącej wyników badania jakości działania użytkowników wykorzystujących smartfon (i/lub tablet) i wskazujących obiekty za pomocą gestów na ekranie. W pierwszym artykule [1] przedstawiono wyniki badań gestów tap, double tap i flick,

natomiast w drugim (patrz praca [2]) przedstawiono wyniki badań gestów pan oraz touch and hold.

Przedstawione w tym artykule wyniki badań dotyczą gestów pinch and stretch i wskazywania obiektów w jednokierunkowym teście wskazywania (por. artykuły [10] i [11]).

Gesty wykonywane były za pomocą palca – nie używano rysika. Wyniki badań obejmują średnią precyzję wykonania i odchylenie standardowe precyzji wykonania gestu (wskazania) oraz średni czas wykonania i odchylenie standardowe czasu wykonania gestu (wskazania) przez osoby w grupach wiekowych. Na podstawie wyników badań wyznaczono średnią precyzję gestu, średni czas wykonania gestu i prawdopodobieństwo błędu wykonania gestu w grupach wiekowych osób i w grupach osób, które używają smartfona codziennie i nie używają smartfona codziennie.

Dla badanych rodzajów gestów przyjęto warunek poprawności wykonania gestu i na tej podstawie wyznaczono prawdopodobieństwo błędu wykonania gestu (wskazania) w grupach wiekowych.

Porównania parametrów (precyzja, czas wykonania gestu i prawdopodobieństwo błędu) wykonano pomiędzy grupą wiekową pierwszą i pozostałymi grupami, zakładając, że osoby z pierwszej grupy wiekowej są zwykle najsprawniejsze w wykonywaniu gestów (wskazań).

Analizując wartości średniej precyzji dla gestu pinch and stretch w grupach wiekowych, widać wyraźnie, że znaczna liczba gestów wykonanych przez osoby badane zakończyła się w odległości większej niż ustalony warunek poprawności – stąd wysokie prawdopodobieństwo błędu wykonania gestu. Porównując średnią precyzję gestów pomiędzy grupami wiekowymi dla wszystkich gestów, stwierdzono, że należy odrzucić hipotezę H0 o równości średnich precyzji przy porównaniu grupy wiekowej pierwszej z pozostałymi grupami wiekowymi poza porównaniem z drugą grupą wiekową. Porównano również średni czas wykonania gestów pan przez osoby badane w grupach wiekowych. Stwierdzono, że nie ma podstaw do odrzucenia hipotezy H0 o równości średnich czasów wykonania gestów w grupach wiekowych 1-2, 1-3, 1-4 i 1-5 dla wszystkich gestów. Taka sama sytuacja występuje dla gestów poprawnych.

Dla osób używających i nie używających smartfona codziennie stwierdzono, że nie ma podstaw do odrzucenia hipotezy o równości średniej precyzji wykonania gestu, średniego czasu wykonania gestu oraz prawdopodobieństwa błędu w wykonaniu gestu pinch and stretch pomiędzy tymi grupami osób dla wszystkich gestów.

Należy tutaj zauważyć, że wyniki badań gestu tap (praca [1]), dotyczące czasu wykonania gestu w najmłodszej grupie wiekowej, są w znacznym stopniu zbliżone do wartości uzyskanych w badaniach czasu realizacji gestu w pracy [6].

Wyniki badań wskazań wykonywanych w ramach jednokierunkowego testu wskazywania wykazały, że zmiany wartości średniego czasu wykonania wskazania wraz z wiekiem są dość podobne do zmian dotyczących gestu tap (patrz praca [1]). Odrzucono, podobnie jak to było dla gestu tap ([1]), hipotezy o równości średniego czasu wykonania wskazania pomiędzy grupą wiekową pierwszą i pozostałymi grupami wiekowymi, poza porównaniem z drugą grupą wiekową.

Znaczne wartości prawdopodobieństwa błędu wskazania w teście jednokierunkowym są związane ze znacznym ograniczeniem precyzji wykonania wskazania dla wskazań poprawnych (warunek poprawności (4)).

Dla osób używających i nie używających smartfona codziennie odrzucono hipotezę o równości średniego czasu wykonania wskazania i hipotezę o równości średniej precyzji wykonania wskazania. Natomiast dla prawdopodobieństwa błędu w wykonaniu wskazania w teście jednokierunkowym nie było podstaw do odrzucenia hipotezy o równości tego parametru.

Biorąc pod uwagę wartości parametrów charakteryzujących gesty uzyskane z badań przedstawionych w pracach [1] i [2] oraz w niniejszym artykule, można przykładowo podjąć próbę oszacowania czasu wykonywania czynności przez kierowcę samochodu przy nawiązywaniu połączenia telefonicznego. Wykonywanie takich czynności przez kierowców w czasie prowadzenia samochodu stanowi zagrożenie dla bezpieczeństwa ruchu drogowego. Będzie to przedmiotem dalszych analiz.

Literatura

[1] ARCIUCH A., DONIGIEWICZ A.M., *Quality study of user activity using mobile device. Tap, double tap, flick gestures.* Przegląd Teleinformatyczny, 3-4, 2018, s. 37-72. DOI: 10.5604/01.3001.0013.1662

[2] ARCIUCH A., DONIGIEWICZ A.M., *Quality study of user activity using mobile device. Pan, touch and hold gestures.* Przegląd Teleinformatyczny, 1-2, 2019, s. 35-66. DOI: 10.5604/01.3001.0013.5281

[3] NICOLAU H., GUERREIRO T., JORGE J., GONÇALVES D., *Mobile Touch Screen User Interfaces: Bridging the Gap between Motor-Impaired and Able-Bodied Users*. Universal Access in the Information Society, Vol. 13 Issue 3, 2014, pp. 303-313.

[4] LE H.V., MAYER S., BADER P., HENZE N., *Fingers' Range and Comfortable Area for One-Handed Smartphone Interaction Beyond the Touchscreen.* Proceedings of the 7th International Conference on Tangible, Embedded and Embodied Interaction, 2018, paper No. 31.

[5] CHANG H.T., TSAI T.H., CHANG Y.CH., CHANG Y.M., *Touch panel usability of elderly and children.* Computers in Human Behavior, Vol. 37, 2014, pp. 258-269.

[6] ASAKAWA D.S., DENNERLEIN J.T., JINDRICH D.L., *Index finger and thumb kinematics and performance measurements for common touchscreen gestures.* Applied Ergonomics, vol. 58, 2017, pp. 176-181.

[7] WAWRYNIUK R., *Metodyka oceny jakości działania użytkownika urządzenia mobilnego*. Praca dyplomowa, WAT, Warszawa, 2013.

[8] KOWALSKI L., *Statystyka*. Wyd. Wydział Cybernetyki WAT, BelStudio, Warszawa, 2005.

[9] CIECIURA M., ZACHARSKI J., *Metody probabilistyczne w ujęciu praktycznym*. Wizja Press&IT, Warszawa, 2007.

[10] ISO 9241-9:2000(E), Ergonomic requirements for Office work with visual display terminals (VDTs).Part 9: Requirements for non-keyboard input devices, ISO, 2000.

[11] DONIGIEWICZ A.M., *Wyniki badania jakości wskazywania obiektów w teście jednokierunkowym*. Biuletyn Instytutu Automatyki i Robotyki WAT, nr 31, 2011, s. 17-35.

Źródła elektroniczne

[12] http://www.mathworks.com/, http://www.ont.com.pl/

[13] http://statystyka.rezolwenta.eu.org/materialy.html (dostęp: 23.01.2017)

[14] http://gsmowo.pl/nokia-lumia-800/ (dostęp: 24.01.2016)

[15] https://tech.wp.pl/nokia-lumia-800-6039436541907585c (dostęp: 24.01.2016)

Quality study of user activity using a mobile device

Pinch and stretch gestures and tapping in the one-direction tapping test

ABSTRACT: The paper presents results of research on the quality of gestures performed by users using a mobile device. As an example mobile device smartphone Nokia Lumia 800 was used. The results of the research concern the basic pinch and stretch gesture and the one-direction tapping test. The time of the gesture and the precision of the gesture have been included. The results take into account the division of users into age groups as well as groups that are using or not a smartphone every day. A comparison of designated characteristics between groups is presented.

KEYWORDS: pinch and stretch gestures, one direction tapping test, gestures entering (input) by finger, mobile device, time of gesture execution, gesture precision

Praca wpłynęła do redakcji: 29.12.2020 r.

Recenzenci artykułów czasopisma naukowego PRZEGLĄD TELEINFORMATYCZNY

Lata 2019-2020

Aleksiejuk Mikołaj	Instytut Podstawowych Problemów Techniki PAN
Ambroziak Tomasz	Wydział Transportu, Politechnika Warszawska
Barczak Andrzej	Wydział Nauk Ścisłych, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Jakubowski Jacek	Wydział Elektroniki, Wojskowa Akademia Techniczna
Jasztal Michał	Wydział Mechatroniki i Lotnictwa, Wojskowa Akademia Techniczna
Jung Leszek	Instytut Sztuki i Nauk Technicznych, Społeczna Akademia Nauk
Kosiński Jerzy	Wydział Dowodzenia i Operacji Morskich, Akademia Marynarki Wojennej
Kawalec Adam	Wydział Elektroniki, Wojskowa Akademia Techniczna
Laskowski Dariusz	Wydział Elektroniki, Wojskowa Akademia Techniczna
Mąka Wojciech	Wydział Nauk Technicznych, Uniwersytet Warmińsko-Mazurski
Marć Paweł	Wydział Nowych Technologii i Chemii, Wojskowa Akademia Techniczna
Matuszewski Jan	Wydział Elektroniki, Wojskowa Akademia Techniczna
Olchowik Wiktor	Wydział Informatyki, Wyższa Szkoła Technologii Informatycznych
Różański Grzegorz	Wydział Elektroniki, Wojskowa Akademia Techniczna
Sondej Tadeusz	Wydział Elektroniki, Wojskowa Akademia Techniczna
Szmidt Janusz	Wojskowy Instytut Łączności
Sienkiewicz Piotr	Wydział Bezpieczeństwa, Logistyki i Zarządzania, Wojskowa Akademia Techniczna

Welker Elżbieta	Wydział Nawigacji i Uzbrojenia Okrętowego, Akademia Marynarki Wojennej
Weydman Romuald	MILSTAR
Wróbel Krzysztof	Wydział Nauk Ścisłych i Technicznych, Uniwersytet Śląski

Information for Authors – rules of papers preparation and reviewing for TELEINFORMATICS REVIEW

The *Teleinformatics Review* is devoted to the publication of original research results in fields of science including, but not limited to: computer science, telecommunication, signal processing, network systems, automation and robotics, etc., which have not been published elsewhere in their entirety or considerable part. If a submitted paper is a part of another published work, e.g. a doctoral dissertation, a postdoctoral thesis, etc., the source work should be included in the list of literature and the editorial office must be informed about it.

In order to publish a paper in the Teleinformatics Review it is necessary to submit it to the editorial office in an electronic form (and possibly its printed copy, one-sided, legible, on white A4 sheets) according to the given template. Only original works in English or Polish will be accepted. The text of the paper should be prepared in the format of Microsoft Word editor (versions 2003 or 2010 are suggested). Appropriate templates can be downloaded from website review.ita.wat.edu.pl (or przeglad.ita.wat.edu.pl). The electronic version submitted to the editorial office should contain a source file of the paper in DOC or DOCX format, with all figures and tables being inserted. The editorial office does not rewrite the text neither make drawings. In addition to the mentioned source file, all figures should be delivered in commonly used image formats (preferably as EPS, JPG, TIFF, or others).

Papers to be published in the Teleinformatics Review are subject to initial acceptance by the editorial office and then are subject to review by two external reviewers. Reviewers and authors do not know each other personal data. The content of the review will be available at the editorial office. If one review is negative (or imprecise) then a third reviewer may be appointed. If both reviews are negative the paper is rejected. If the review indicates a necessity of some corrections, the author must consider all of them and resubmit the improved paper by the determined deadline.

The volume of a submitted paper generally not exceed 20 pages of typescript A4. A deviation from this rule requires agreement of the editorial office. Except the last page, no more than 10% of any page within the paper can be left empty. Figures must be numbered and described below them as well as tables must be numbered and described at the top of them. The literature should hold the form given in the template.

The authors are obliged to submit a statement to the editorial office on the percentage contribution to the creation of the accepted paper, confirming the lack of prior publication of such a work, or a public speech on the subject at a conference or symposium.

The editorial board reserves rights to introduce minor editorial changes to the content of paper without consulting the author. The editorial office insists that no special formatting should be used, which would be inconsistent with the template.

Papers printed in the Teleinformatics Review and their abstracts are placed in the national database of Polish technical journals BazTech as well as on the INDEX COPERNICUS website. Additionally, the papers will be available in the electronic PDF form on website review.ita.wat.edu.pl.

Publication in the Teleinformatics Review does not involve any costs for authors. The editorial office does not charge for submitting, reviewing, preparing for publication and publishing the work. The publication of a paper in the Teleinformatics Review is tantamount to transfer of authors' property rights for publication to the publisher, i.e. the Military University of Technology. By submitting a paper for publication in the Teleinformatics Review, the author agrees, for publication purposes, to the processing by the editorial office the author's name, email address, affiliation, and other contact details.

The editorial office does not return received materials.

The editorial office does not pay fees for papers publishing.

The editor-in-chief may refuse to publish a paper in the following cases:

- if the content of the paper violates the law (principles of secrecy protection, press law, copyright law, etc.) or good manners;
- the author does not agree to introduce all necessary corrections proposed by the editorial board or reviewers;
- the text and illustrative material submitted by the author does not meet the technical requirements given in this document or the template.

Informacje dla autorów – zasady przygotowania tekstu i recenzowania artykułów do PRZEGLĄDU TELEINFORMATYCZNEGO

W Przeglądzie Teleinformatycznym zamieszczane są oryginalne artykuły z dziedzin: *informatyka, telekomunikacja, przetwarzanie sygnałów, systemy sieciowe, automatyka i robotyka* oraz pokrewnych, niepublikowane dotychczas w całości lub w znaczącej części. Jeśli nadesłana praca stanowi część innej opublikowanej pracy, np. pracy doktorskiej, habilitacji, etc., to źródło powinno być umieszczone w spisie literatury, a redakcja powinna być o tym poinformowana.

W celu opublikowania artykułu w *Przeglądzie* niezbędne jest dostarczenie do redakcji treści artykułu w postaci **elektronicznej** według podanego szablonu i ewentualnie jednego egzemplarza wydrukowanego (jednostronnie, czytelnie, na białym papierze formatu A4). Przyjmowane są tylko oryginalne prace w języku angielskim lub polskim. Tekst artykułu powinien być przygotowany w formacie edytora Microsoft Word (wersja 2003 lub 2010 jest zalecana). Szablony dla artykułów są dostępne w pliku na stronie przeglad.ita.wat.edu.pl (lub review.ita.wat.edu.pl). Przekazane do redakcji materiały powinny zawierać plik źródłowy w formacie DOC lub DOCX, ze wstawionymi rysunkami. Redakcja nie przepisuje tekstów i nie wykonuje rysunków. Dodatkowo należy dostarczyć pliki źródłowe rysunków (najlepiej w formacie EPS, JPG, TIFF lub innym powszechnie używanym).

Artykuły przeznaczone do opublikowania w *Przeglądzie* podlegają wstępnej ocenie przez redaktora działu, a następnie podlegają recenzji przez dwóch zewnętrznych recenzentów. Recenzenci i autorzy nie znają swoich danych personalnych. Z treścią recenzji można zapoznać się w redakcji. Jeśli jedna z recenzji jest negatywna (lub nieprecyzyjna), może być powołany trzeci recenzent. Jeśli dwie recenzje są negatywne, artykuł jest odrzucany. Jeśli z recenzji wynika konieczność dokonania poprawek w treści artykułu, to autor jest zobowiązany do ich rozpatrzenia i dostarczenia do redakcji poprawionej wersji artykułu, w terminie ustalonym przez redakcję.

Objętość artykułu zasadniczo nie powinna przekroczyć 20 stron maszynopisu A4. Odstąpienie od tej zasady wymaga uzgodnień z redakcją *Przeglądu*. Na stronach tekstu artykułu nie może być pozostawione więcej niż 10% pustego miejsca, za wyjątkiem ostatniej strony. Rysunki należy numerować i opatrzyć (pod spodem) wyczerpującym podpisem. Tabele również muszą być numerowane (tytuł nad tabelą). Literatura może być uszeregowana alfabetycznie oraz powinna mieć postać jak w szablonie.

Autorzy są zobligowani do złożenia w redakcji oświadczenia autorskiego o wkładzie procentowym w powstanie artykułu, braku wcześniejszej publikacji artykułu w przedstawionej formie lub wystąpieniu publicznym na ten temat na konferencji lub sympozjum.

Redakcja zastrzega sobie prawo wprowadzenia niewielkich redakcyjnych zmian w treści artykułu bez konsultacji z autorem. Redakcja nalega, aby **nie stosować** żadnego specjalnego formatowania i **trzymać się ściśle** ustaleń zawartych w szablonie.

Streszczenia i pełne teksty artykułów drukowanych w *Przeglądzie* zamieszczane są w krajowej bazie danych o zawartości polskich czasopism technicznych BazTech oraz na platformie INDEX COPERNICUS. Opublikowane w *Przeglądzie* artykuły będą także w całości udostępnione w internetowej wersji (format PDF) czasopisma, pod adresem przeglad.ita.wat.edu.pl (lub review.ita.wat.edu.pl).

Publikacja w *Przeglądzie* nie wiąże się z żadnymi kosztami dla autorów. Redakcja nie pobiera opłat za zgłoszenie, przygotowanie do druku, recenzję czy publikację pracy. Przekazanie artykułu do publikacji w *Przeglądzie* jest równoznaczne z przekazaniem autorskich praw majątkowych do publikacji na rzecz wydawcy, tj. Wojskowej Akademii Technicznej. Przekazując artykuł do publikacji w *Przeglądzie*, autor zgadza się na przechowywanie i przetwarzanie przez redakcję, w celach publikacyjnych, imienia, nazwiska, adresu e-mail i afiliacji.

Redakcja nie zwraca materiałów dostarczonych do redakcji.

Redakcja nie przewiduje honorariów za opublikowanie artykułu.

Redaktor naczelny może odmówić opublikowania artykułu w przypadku, gdy:

- treści zawarte w materiałach naruszają prawo (zasady ochrony tajemnicy, prawo prasowe, prawo autorskie itp.) lub dobre obyczaje;
- autor nie zgadza się na wprowadzenie wszystkich koniecznych poprawek zaproponowanych przez redakcję lub recenzentów;
- tekst i materiał ilustracyjny złożony przez autora nie spełnia wymagań technicznych podanych w niniejszym dokumencie i szablonie.