

Dr Piotr Świtalski

Uniwersytet w Siedlcach

Wydział Nauk Ścisłych i Przyrodniczych

III. PRACA Z SYSTEMEM OPERACYJNYM WINDOWS I ZAPEWNIENIE JEGO BEZPIECZEŃSTWA

WSTĘP

Dla osób korzystających z systemów komputerowych wygodnie, aby były one proste i intuicyjne. Jednak poziom złożoności systemu operacyjnego, który działa jak interfejs pomiędzy użytkownikiem a sprzętem rośnie. W konsekwencji takim zasobom, jak wydajność procesora, objętość pamięci operacyjnej czy pojemność dysku twardego stawia się coraz większe wymagania. Rozwój systemów komputerowych związany jest również z pojawiającymi się różnego rodzaju atakami na jego infrastrukturę. Dotyczy to zarówno rozwiązań sprzętowych jak i programowych.

W tym opracowaniu czytelnik pozna podstawy systemu Windows 10 i jego zabezpieczanie, a także: narzędzia systemowe, metody archiwizowania danych i ich ochrony, pracę w sieci oraz zagadnienia bezpieczeństwa komputerowego.

1. PODSTAWY PRACY



1.1. SYSTEM OPERACYJNY I ORGANIZACJA DANYCH

System operacyjny (ang. *Operating System, OS*) to zasadnicze oprogramowanie tworzące podstawową platformę dla działania innych zainstalowanych w nim aplikacji, zarządza on zasobami komputera i wspomaga użytkownika w korzystaniu z nich. Znajduje się na trwałym nośniku danych (dysku twardym) w postaci struktury katalogów oraz plików. Istnieje wiele systemów operacyjnych a najpopularniejsze to: Windows, Linux, MacOS.

System plików (ang. *file system*) jest podstawową częścią każdego systemu operacyjnego, zapewniając mechanizmy bezpośredniego przechowywania i dostępu do plików umieszczanych w pamięci masowej. Windows obsługuje następujące systemy plików: NTFS, FAT32, exFAT.

Każdy program lub dokument zapisuje się jako plik, którego podstawowymi atrybutami (il. 1) są:

1. Nazwa – prawie może być dowolna, nie powinna jednak zawierać razem ze ścieżką dostępu, więcej niż 255 znaków i tzw. specjalnych spośród nich, czyli: \ / : * ? „ , < > |. Jest konieczna, niedozwolone jest, aby powtarzała się w tym samym folderze.
2. Typ – określa rodzaj przechowywanych danych, np. tekst, obraz, dźwięk, natomiast sposób ich zapisu definiuje format. Identyfikuje go rozszerzenie pliku, z reguły trzyliterowe, które stanowi ostatni element nazwy oddzielony kropką i informuje system operacyjny, jakiego programu użyć do jego otwarcia.
3. Wielkość – zajmowany obszar na dysku wyrażany najczęściej wielokrotnością bajtów.
4. Atrybuty – np. ustawienie **tylko do odczytu** – spowoduje, że nie będzie można go modyfikować (również zawartych w nim informacji), a **ukryty** – to, że przestanie być widoczny w oknie Eksploratora lub innego programu służącego do zarządzania plikami i folderami.

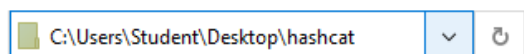
 example400.hash	21.11.2021 16:43	Plik HASH	1 KB
 example400.sh	21.11.2021 16:43	Plik SH	1 KB

1. Przykłady plików wraz z ich atrybutami: datą utworzenia (modyfikacji), typu pliku i jego wielkości

Położenie pliku określa **ścieżka dostępu**. To łańcuch znaków, który w przypadku komputera lokalnego składa się z nazwy dysku i katalogów, a zdalnego z nazwy komputera i udziału, oddzielonych od siebie:

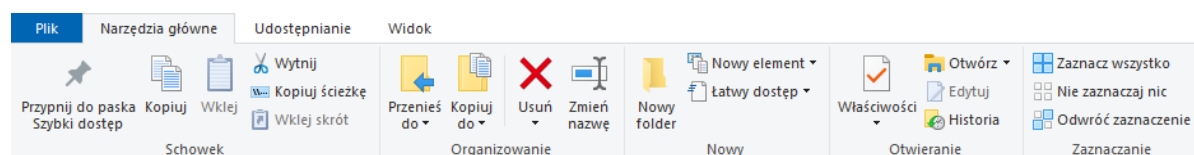
1. Dwukropkiem (:) w odniesieniu do dysku (il. 2),
2. Dwoma odwrotnymi ukośnikami (\\), gdy dotyczy to nazwy komputera,
3. Pojedynczym odwrotnym ukośnikiem (\) w wypadku folderów (il. 2).

Ścieżka pokazuje **drogę**, jaką należy przejść, aby odszukać plik, poczynając od najbardziej ogólnego położenia – dysku, poprzez kolejne foldery i kończąc na jego nazwie. Ogólna składnia ma następującą postać: dysk:\folder(y)\nazwa_pliku.



2. Przykład ścieżki dostępu w Eksploratorze plików systemu Windows 10

System Windows 10 posiada podręczną wstążkę (pasek narzędziowy) z przydatnymi opcjami do zarządzania strukturą plików i katalogów (il. 3).



3. Pasek narzędziowy okna Eksploratora plików

Użytkownik ma do dyspozycji szereg operacji:

1. Kopiowanie plików i katalogów:
 - 1.1. Zaznaczamy plik(i) lub/i katalog(i), które chcemy skopiować.
 - 1.2. Wybieramy z menu kontekstowego **Kopiuj** albo kombinację klawiszy **[Ctrl] + [C]** lub z paska narzędziowego ikonę **Kopiuj**.
 - 1.3. Przechodzimy do katalogu, w którym chcemy umieścić pliki.
 - 1.4. Wybieramy z menu kontekstowego **Wklej** albo kombinację klawiszy **[Ctrl] + [V]** lub z paska narzędziowego ikonę **Wklej**.
2. Przenoszenie plików i katalogów:
 - 2.1. Zaznaczamy plik(i) lub/i katalog(i), które chcemy przenieść.
 - 2.2. Wskazujemy z menu kontekstowego **Wytnij** albo kombinację klawiszy **[Ctrl] + [X]** lub z paska narzędziowego ikonę **Wytnij**.
 - 2.3. Przechodzimy do katalogu, w którym chcemy umieścić pliki.
 - 2.4. Wskazujemy z menu kontekstowego **Wklej** albo kombinację klawiszy **[Ctrl] + [V]** lub z paska narzędziowego ikonę **Wklej**.
3. Zmiana nazwy pliku lub katalogu:
 - 3.1. Zaznaczamy plik lub katalog.
 - 3.2. Wybieramy z menu kontekstowego **Zmień nazwę** albo klawisz **[F2]** lub z paska narzędziowego ikonę **Zmień nazwę**.
4. Usuwanie plików i katalogów:
 - 4.1. Zaznaczamy plik(i) lub/i katalog(i).
 - 4.2. Wskazujemy z menu kontekstowego **Usuń** albo klawisz **[Del]** lub z paska narzędziowego ikonę **Usuń**.

UWAGA! Plik lub katalog można usunąć trwale (bez przeniesienia do kosza) poprzez zaznaczenie go i użycie skrótu klawiaturowego **[Ctrl] + [Shift] + [Del]**.

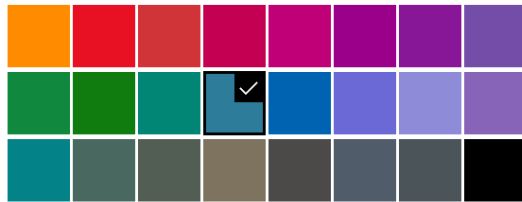
Przykład 1. Spersonalizuj pulpit i ustaw jednolity jasnoniebieski kolor tła.

1. Kliknij prawym przyciskiem myszy na pulpicie.
2. Wybierz:
 - 1.1. **Personalizuj**.
 - 1.2. Z lewej strony okna sekcję **Tło**.

Tło

Jednolity kolor ▾

Wybierz kolor tła

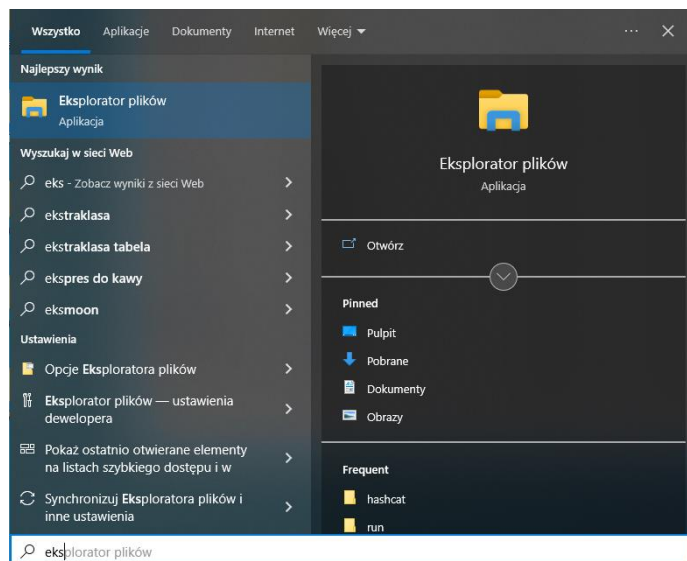


4. Ustawianie jednolitego koloru tła pulpitu

1.3. Po prawej z listy **Jednolity kolor**, a poniżej jasnoniebieski (il. 4).

Przykład 2. Znajdź szybko program Eksplorator plików.

1. Otwórz menu Start.
2. Zaczynj wpisywać początkowe litery nazwy aplikacji (il. 5).



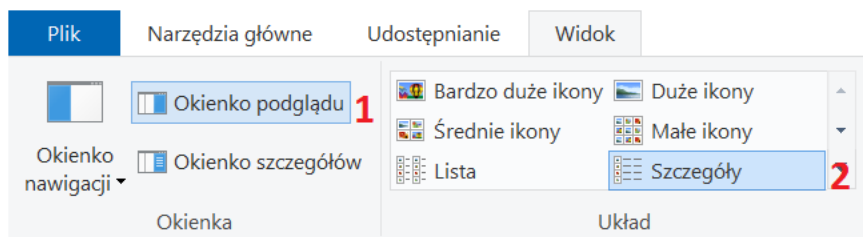
5. Wyszukiwanie programu w menu Start

Przykład 3. Włącz widoczność ukrytych folderów i plików w Eksploratorze plików.

1. Otwórz Eksploratora plików w jeden ze sposobów:
 - 1.1. Użyj skrótu klawiaturowego [Logo Windows] + [E].
 - 1.2. Kliknij najpierw prawym przyciskiem myszy na przycisku Start, a potem lewym na aplikacji.
2. Na pasku narzędzi kliknij zakładkę **Widok**.
3. W grupie **Pokazywanie/ukrywanie** zaznacz opcję **Ukryte elementy**.

Przykład 4. Skorzystaj z Eksploratora plików, aby wyświetlić podgląd dokumentu bez jego otwierania.

1. Uruchom aplikację Eksplorator plików.
2. Kliknij:
 - 2.1. Kartę **Widok** (il. 6).



6. Karta Widok z grupą Układ Eksploratora plików

2.2. **Okienko podglądu** (il. 6, 1).

2.3. Dokument, aby zobaczyć zawartość pliku.

Przykład 5. W Eksploratorze plików wybierz szczegółowy widok wyświetlania elementów.

1. Uruchom Eksplorator plików.
2. Wskaż:
 - 2.1. Na Wstążce kartę Widok (il. 6).
 - 2.2. W grupie **Układ** polecenie **Szczegóły** (il. 6, 2).

Przykład 6. Napisz w Notatniku swoje imię, nazwisko, kierunek studiów i numer grupy. Zapisz plik z nazwą **dane.txt** i ustaw dla niego atrybut **Tylko do odczytu**.

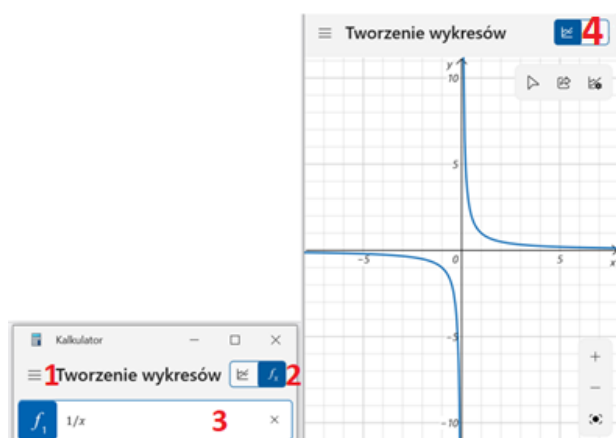
1. Otwórz Notatnik.
2. Wpisz swoje imię, nazwisko, kierunek studiów i numer grupy.
3. Zapisz plik z nazwą **dane.txt**.
4. Kliknij prawym przyciskiem myszy na pliku i wybierz **Właściwości**.
5. Na karcie **Ogólne** kliknij opcję **Tylko do odczytu** i zatwierdź wybór.

Przykład 7. Do programu Paint wklej zdjęcie miasta jakie chcesz zwiedzić, a poniżej dodaj adres strony, z której fotografia pochodzi. Zapisz pracę na dwa sposoby jako **cel.png** oraz **cel.jpg**. Który z plików zajmuje więcej miejsca?

1. Znajdź zdjęcie miasta i skopiuj do programu Paint.
2. Kliknij ikonę tekstu i pod obrazem wklej adres strony, z której pochodzi fotografia.
3. Zapisz pracę jako **cel.png** oraz **cel.jpg**.
4. Więcej miejsca zajmuje plik z formatem **jpg**.

Przykład 8. Za pomocą narzędzia Kalkulator utwórz wykres $1/x$.

1. Uruchom Kalkulator.
2. W lewym górnym rogu kliknij na ikonie **Otwórz nawigację** (il. 7, 1) i **Tworzenie wykresów**.



7. Kalkulator i tworzenie wykresów

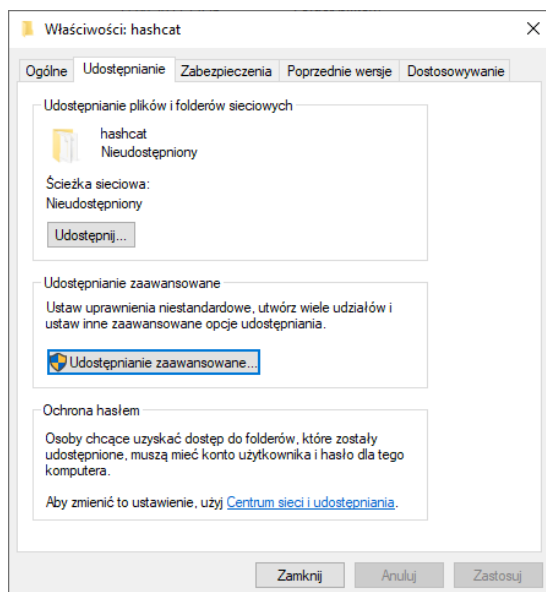
3. Z zaznaczeniem **Przełącz do trybu równania** (il. 7, 2) wpisz $1/x$ (il. 7, 3).
4. Wskaż **Przełącz do trybu wykresu** (il. 7, 4).

1.2. UDOSTĘPNIANIE ZASOBÓW

Użytkownik może korzystać z zasobów sieci lokalnej, w której się znajduje, jeśli są one udostępnione. Wówczas widać je w postaci ścieżki rozpoczynającej się dwoma odwrotnymi ukośnikami, np. \\localhost.

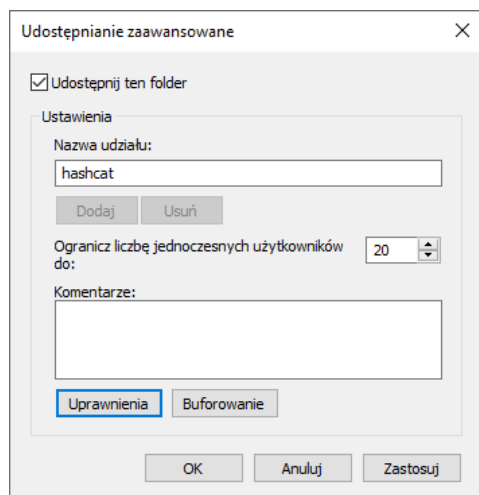
Przykład 9. Udostępnij folder hashcat do odczytu i zapisu.

1. Z menu kontekstowego wybierz **Właściwości**.
2. Przejdź do:
 - 2.1. Karty **Udostępnianie** (il. 8).
 - 2.2. Opcji **Udostępnianie zaawansowane**.



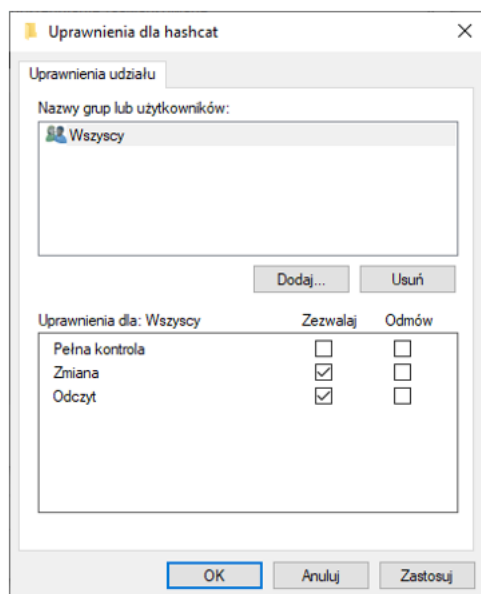
8. Okno z opcjami udostępniania zasobów w systemie Windows

3. Zaznacz **Udostępnij ten folder** i kliknij **Uprawnienia** (il. 9).



9. Okno udostępniania zaawansowanego

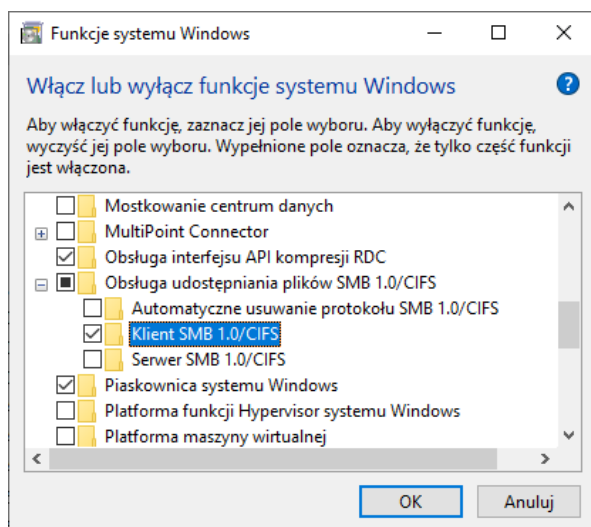
4. Udostępnij zasób do odczytu i zapisu (il. 10).



10. Uprawnienia dla zasobu

5. Pozamykaj okna przyciskiem OK.

UWAGA! Jeśli opcja udostępniania nie działa należy włączyć funkcję systemu Windows (narzędzie nazywa się **Włącz lub wyłącz funkcje systemu Windows**): Obsługa udostępniania plików SMB 1.0/CIFS > Klient SMB 1.0/CIFS (il. 11).



11. Okno funkcji systemu Windows

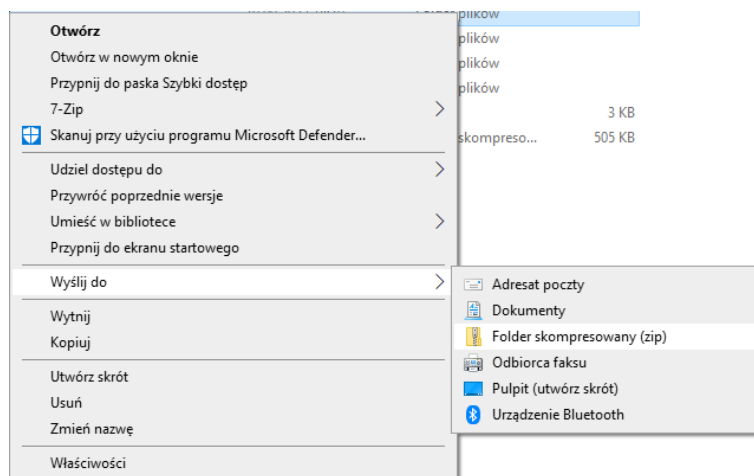
1.3. KOMPRESJA DANYCH

To zmiana sposobu zapisu informacji z wykorzystaniem algorytmów w celu zmniejszenia liczby zajmowanych bitów na dysku, co ułatwia przechowywanie i przesyłanie. Wyróżnia się **kompresję stratną**, gdzie w wyniku procesu odwrotnego zwanego dekompresją nie odzyskuje się pełni danych oraz **bezzstratną**, która pozwala wrócić do identycznej postaci pierwotnej. Pierwsza z nich wiąże się z utratą jakości i jest powszechnie stosowana do plików multimedialnych, np. zdjęć (jpeg) czy muzyki (mp3). Natomiast dla danych tekstowych i programów decydująca jest druga, bo idealnie odtwarza oryginał. System Windows posiada możliwość kompresji plików i folderów.

Przykład 10. Skompresuj wybrane pliki i katalogi.

1. Zaznacz potrzebne dane.

2. Z menu kontekstowego wskaż kolejno **Wyślij do > Folder skompresowany (zip)** (il. 12).

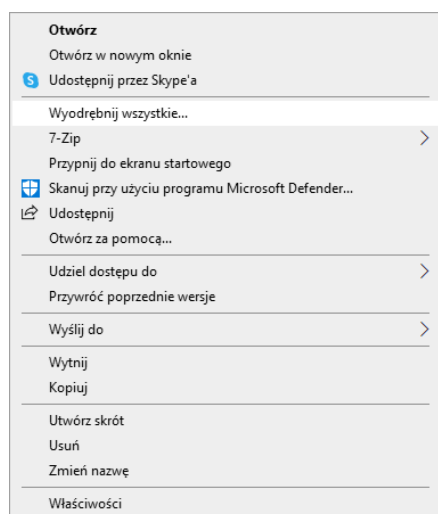


12. Opcja kompresji plików i katalogów

3. Nowy plik **zip** powstaje w tej samej lokalizacji, co kompresowane pliki i katalogi.

Przykład 11. Rozpakuj archiwum zip.

1. Kliknij prawym przyciskiem myszy na pliku zip.
2. Wybierz opcję **Wyodrębnij wszystkie** (il. 13).
3. Wskaż lokalizację docelową.
4. Kliknij **Wyodrębnij**.



13. Opcja dekompresji skompresowanego pliku

1.4. JEDNOSTKI INFORMACJI I SYSTEMY LICZBOWE

Bajt (ang. *byte*) – oznaczany dużą literą **B** jest najmniejszą adresowalną jednostką informacji pamięci komputerowej, składającą się z bitów (ang. bit pochodzi od *binary digit*), których symbolem jest mała litera **b**. W praktyce przyjmuje się, że $1\text{ B} = 8\text{ b}$, choć to nie wynika z powyższej definicji.

Praktycznie korzysta się z wielokrotności bajtu i stosuje przedrostki dziesiętne układu SI często w odniesieniu do zapisu dwójkowego:

- 1 kB = 1000 B (kB - kilobajt);
- 1 MB = 1000 kB (MB - megabajt);
- 1 GB = 1000 MB (GB - gigabajt);
- 1 TB = 1000 GB (TB - terabajt);
- 1 PB = 1000 TB (PB - petabajt).

Zwyczajowo jednak przyjmuje się te wielokrotności w następujący sposób: 1 kB = 1024 B, 1 MB = 1024 kB, itd¹. Toteż dla przedrostków dwójkowych stosuje się zapis zaproponowany przez jednostkę standaryzacyjną IEC²:

- 1 KiB = 1024 B (KiB - kibibajt);
- 1 MiB = 1024 KiB (MiB - mebibajt);
- 1 GiB = 1024 MiB (GiB - gibibajt);
- 1 TiB = 1024 GiB (TiB - tebibajt);
- 1 PiB = 1024 TiB (PiB - pebibajt).

Przykład 12. Łącze domowe oferuje przepustowość 100 Mb/s. Ile maksymalnie bajtów danych można przesłać w ciągu sekundy?

1. Przelicz:
 - 1.1. Megabity na megabajty: $100 \text{ Mb} / 8 = 12,5 \text{ MB}$.
 - 1.2. Megabajty na bajty: $12,5 * 1024 * 1024 = 13\,107\,200 \text{ B}$.
2. Przy przepustowości 100 Mb/s w ciągu sekundy można przesłać maksymalnie 13 107 200 bajtów danych.

Dwójkowy system liczbowy (inaczej binarny) to pozycyjny system, w którym podstawą są kolejne potęgi liczby 2. Jest powszechnie używany w informatyce. Liczby zapisuje się tu jako ciąg cyfr 0 i 1, z których każda jest mnożnikiem kolejnej potęgi liczby stanowiącej podstawę systemu.

Przykład 13. Zamień liczbę 1011 zapisaną w systemie dwójkowym na dziesiętny.

1. Każdą z cyfr (**1011**) pomnóż przez odpowiadającą potęgę liczby 2: $1x2^3 + 0x2^2 + 1x2^1 + 1x2^0$.
2. Dodaj wyniki: $8 + 0 + 2 + 1 = 11$.
3. Liczbie 1011 w systemie dwójkowym odpowiada liczba 11 w systemie dziesiętnym.

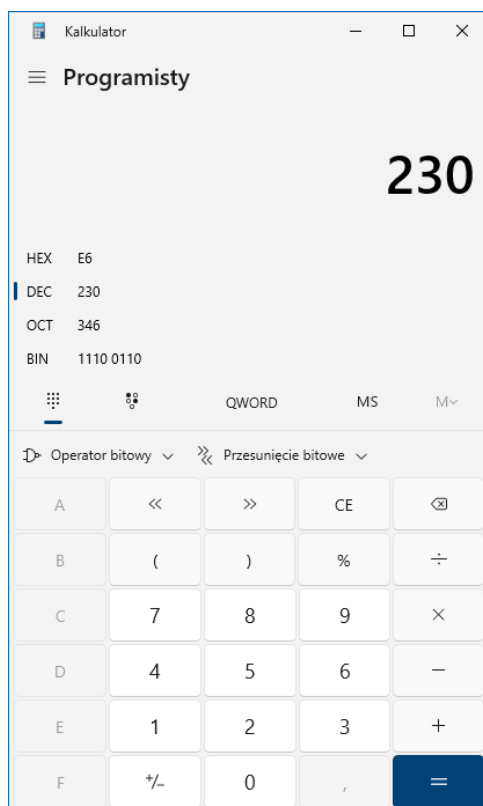
Łatwo jest konwertować liczby za pomocą kalkulatora systemu Windows po przełączeniu w tryb Programisty.

Przykład 14. Wykorzystaj Kalkulator do konwersji liczby 230 z systemu dziesiętnego na systemy: szesnastkowy (HEX), ósemkowy (OCT) i dwójkowy (BIN).

1. Otwórz aplikację Kalkulator.
2. W lewym górnym rogu kliknij na ikonę **Otwórz nawigację** (trzy poziome kreski) i wybierz opcję **Programisty** (il. 14).
3. W środkowej części okna wskaż system dziesiętny DEC (il. 14).
4. Wpisz liczbę 230.
5. Wyświetlą się odpowiadające jej wartości (il. 14) w systemach:
 - 5.1. HEX – E6;
 - 5.2. OCT – 346;
 - 5.3. BIN – 11 100 110.

¹ Producenci dysków twardych stosują wielokrotności SI dla wyrażania pojemności tj. 1 MB = 1 000 000 B.

² <https://iec.ch/homepage>, data dostępu: 10.09.2024.



14. Widok aplikacji Kalkulator (tryb Programisty) z wprowadzoną wartością w systemie dziesiętnym

Pliki przechowują dane jako ciągi zer i jedynek, ich odczytanie wymaga znajomości standardu określającego sposób organizacji i zapisu informacji - formatu. Rozpoznaje się go najczęściej po rozszerzeniu, które występuje w jego nazwie po kropce.

Generalnie pliki można podzielić na tekstowe i binarne. Pierwsze z nich mają formę znaków czytelnych dla odbiorcy, drugie zawierają dane w postaci bardziej złożonej i bez właściwego programu nie są bezpośrednio zrozumiałe. Zasadniczo pliki nazywane binarnymi to wszystkie te, które nie są tekstowe i zawierają między innymi: obrazy, dźwięki, filmy czy zapisane programy komputerowe. Poniżej przykładowe formaty plików:

1. Tekstowe – **txt**;
2. Programu Microsoft Word – **docx**; jego struktura jest bardziej rozbudowana w porównaniu z txt i obecnie bazuje na XML;
3. Wykonywalne systemu Windows – **exe**;
4. Bibliotek dynamicznie wiązanych systemu Windows – **dll**.

2. KODOWANIE PLIKÓW TEKSTOWYCH

Pliki mają określony sposób zapisu danych, które przechowują. W szczególności dotyczy to tekstu i siedmiobitowego kodu **ASCII** (ang. *American Standard Code for Information Interchange*), który przyjęty jest jako standard w systemach komputerowych. W nim każdy znak (np. litera, cyfra, symbol) ma przyporządkowaną liczbę od 0 do 127 (tabela 1) i tak jest reprezentowany. Ze względu na ograniczenia, np. brak znaków narodowych, kodowanie rozbudowano do ośmiu bitów (1 bajt) i dzięki temu powiększono do 256 znaków ($2^8=256$).

Obecnie używa się systemów kodowania kompatybilnych z ASCII, popularnym jest UTF (np. UTF-8, UTF-16, UTF-32), który do reprezentowania pojedynczego znaku wykorzystuje od 1 do 4 bajtów.

Tabela 1. Fragment tablicy ASCII

Znak	Nazwa znaku	Kod ASCII
!	Wykrzyknik	33

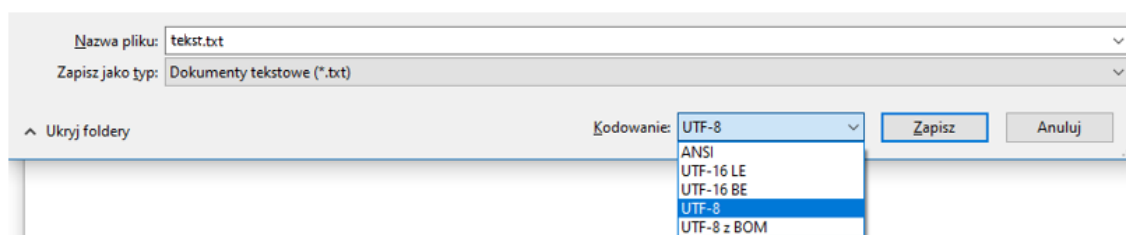
%	Procent	37
5	Pięć	53
a	Duża litera a	65
A	Mała litera a	97
{	Nawias klamrowy lewy	123

Systemy operacyjne zaczęły stosować również własne sposoby kodowania. Przykładem jest Windows-1250 przeznaczony do reprezentacji tekstów w językach środkowoeuropejskich, w tym polskiego; zbliżonym standardem jest ISO 8859-2.

Bardzo użytecznym programem do konwersji kodowania znaków jest Visual Studio Code, ale możliwe jest to też w Notatniku.

Przykład 15. Wklej do Notatnika zdanie: **Żółć to płyn produkowany przez wątrobę**, zapisz plik z nazwą **tekst.txt** i kodowaniem **UTF-8**.

1. Otwórz Notatnik i wprowadź zdanie.
2. Wybierz opcję Plik > Zapisz jako.
3. Na dole okna dialogowego wskaż docelowe kodowanie (il. 15).



15. Fragment okna dialogowego Notatnika

Przykład 16. Plik **tekst.txt** z poprzedniego przykładu otwórz w programie Visual Studio Code i zapisz z kodowaniem Windows-1252. Obejrzyj go w programie Notatnik. Czy kodowanie polskich znaków jest poprawne?

1. Uruchom aplikację Visual Studio Code.
2. Wybierz:
 - 2.1. Plik > Otwórz plik > tekst.txt.
 - 2.2. Na dole opcję UTF-8 (il. 16).



16. Obszar dolny belki programu Visual Studio Code

- 2.3. U góry polecenie **Zapisz z kodowaniem**.
- 2.4. Z listy **Windows-1252**.
3. Obejrzyj plik w programie Notatnik.
4. Polskie znaki diakrytyczne nie wyświetlają się poprawnie.

3. PODSTAWY BEZPIECZEŃSTWA KOMPUTEROWEGO

Według Simsona Garfinkela „system komputerowy jest bezpieczny, jeżeli jego użytkownik może na nim polegać, a zainstalowane oprogramowanie działa zgodnie ze swoją specyfikacją”³. Koncepcję bezpieczeństwa najczęściej przedstawia się jako triadę wymogów:

1. Poufności (ang. *confidentiality*):
 - 1.1. Poufność danych to pewność, że informacja nie zostanie przechwycona ani wydedukowana przez podmiot nieuprawniony do jej uzyskania.
 - 1.2. Prywatność, czyli możliwość szczegółowego kontrolowania, które elementy informacji mogą być odczytywane i (lub) modyfikowane przez określone podmioty.

³ Garfinkel S., Spafford G., Schwartz A., Practical UNIX and Internet Security. 3rd Edition, Wyd. O'Reilly Media, 2003, s. 5.

2. **Integralności** (ang. *integrity*) - możliwość modyfikowania danych i programów jedynie w ściśle określony sposób. W warunkach komunikujących się stron oznacza ochronę przesyłanych informacji przed powielaniem, wstawianiem, modyfikowaniem, zmianą kolejności i powtarzaniem treści oraz przed utratą danych.
3. **Dostępności** (ang. *availability*) - zdolność systemu do natychmiastowej reakcji na żądania/e uprawnionego podmiotu w zgodzie z projektem systemu, bez groźby sparaliżowania jego usług przez nieautoryzowany dostęp.

Podstawowymi pojęciami są:

1. **Zagrożenie** - potencjalne naruszenie bezpieczeństwa w postaci uwarunkowania, zdolności, akcji czy nawet samej możliwości przełamania zabezpieczeń, ze wszystkimi negatywnymi konsekwencjami.
2. **Atak** - zamach na bezpieczeństwo systemu z pogwałceniem jego polityki jako następstwo inteligentnego usiłowania ominięcia usług ochrony.
3. **Ryzyko** - prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu, aby spowodować straty w nim lub jego zniszczenie.
4. **Analiza ryzyka** - proces jego identyfikacji, określania wielkości i obszarów wymagających zabezpieczeń.
5. **Bezpieczeństwo informacji** - zaufanie, że są one gromadzone, chronione i udostępniane zgodnie z wolą i intencjami właściciela.

PAMIĘTAJ! Nie ma absolutnego bezpieczeństwa! Im bardziej złożony system, tym to zadanie jest trudniejsze i nie jest on bezpieczny, dopóki nie ma w tym względzie całkowitej pewności. Bardzo często wzrost jego ochrony odbywa się kosztem wygody użytkownika, ale można ją obejść - włamujący się do systemu ma tego świadomość i to WYKORZYSTA.

3.1. WSPÓŁCZESNE FORMY ATAKÓW

Do obecnie występujących typowych form ataków należą:

1. **Inżynieria społeczna** (ang. *social engineering*) – to socjotechnika mająca na celu uzyskanie niejawnych informacji poprzez wyrobienie u ofiary przekonania, że atakujący jest zaufaną osobą (podmiotem), bo często za taką się podaje, aby wyłudzić interesujące go dane (ang. *phishing*).
 - 1.1. Rodzajem ataku bazującym na inżynierii społecznej jest tzw. **nigeryjski szwindel**. Oszustwo, najczęściej zapoczątkowane kontaktem poprzez pocztę elektroniczną, polega na wciągnięciu ofiary w grę psychologiczną, która oparta jest na fikcyjnym transferze dużej kwoty z jednego z krajów afrykańskich, głównie Nigerii, choć obecnie często w grę wchodzi Wielka Brytania czy Hiszpania, w celu wyłudzenia pieniędzy.
 - 1.2. **Phishing** - w dzisiejszych czasach używany do celów zarobkowych. Zazwyczaj do dużej liczby użytkowników danej usługi rozsyła się niechcianą wiadomość (ang. *spam*), która zawiera prośbę o podanie określonych danych lub zalogowanie na podstawioną przez przestępcę fałszywą stronę internetową, np. banku (il. 17).

ING Bank info@ing.pl przez o2.pl
do Recipients ▾

⚠ Dlaczego ta wiadomość jest w Spamie? Bo jej zawartość jest typowa dla spamu. Dowiedz się więcej



Szanowny Kliencie cenione,

Masz płatność przychodząca trafi na Twoje konto. Ta transakcja nie może być ukończona z powodu błędów w informacji o koncie.

Jesteś zobowiązany do kliknij na logo poniżej wobec utrwalic ten problem natychmiast.

[Zaloguj się](#)

Prosimy nie odpowiadać na tę wiadomość. Jeśli masz pytania, zadzwoń obsługi klienta w numer na odwrocie karty. Są dostępne 24 godziny na dobę, 7 dni w tygodniu.

Mamy nadzieję, że znajdziesz nasze usługi Internet Banking, łatwe i wygodne w użyciu.

Pozdrawiam serdecznie

ING Bank Śląski S.A.
Cyfrowe dyrektork bankowości

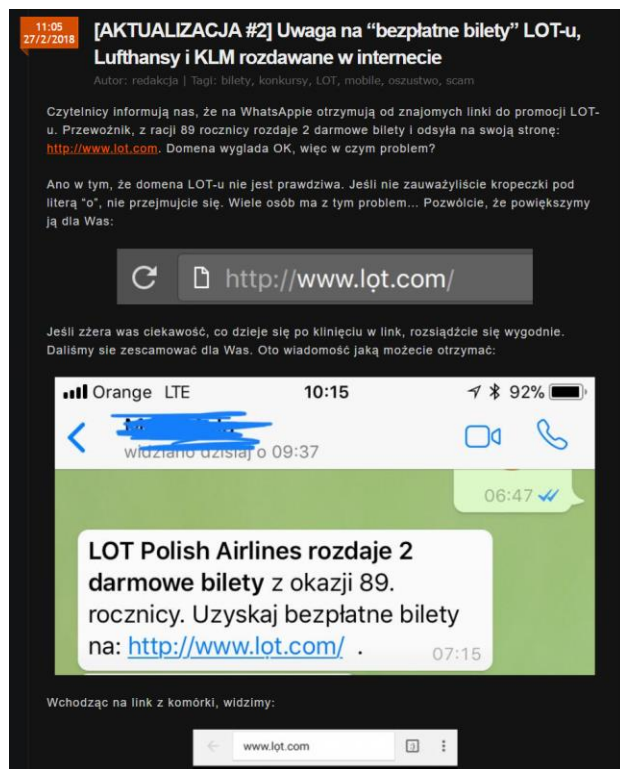
17. Przykład wiadomości phishingowej w postaci listu e-mail skłaniającego do kliknięcia odnośnika⁴

PAMIĘTAJ! Szczególnie niebezpieczne są ataki wykorzystujące zdalny pulpit. Osoba zwykle podszywająca się za pracownika banku nakłania ofiarę do pobrania oprogramowania typu Anydesk lub TeamViewer QuickSupport i dzięki temu uzyskuje bezpośredni dostęp do jej komputera. Atakowany często w ten sposób traci wszystkie pieniądze, które ma na koncie. Zobacz ten film⁵.

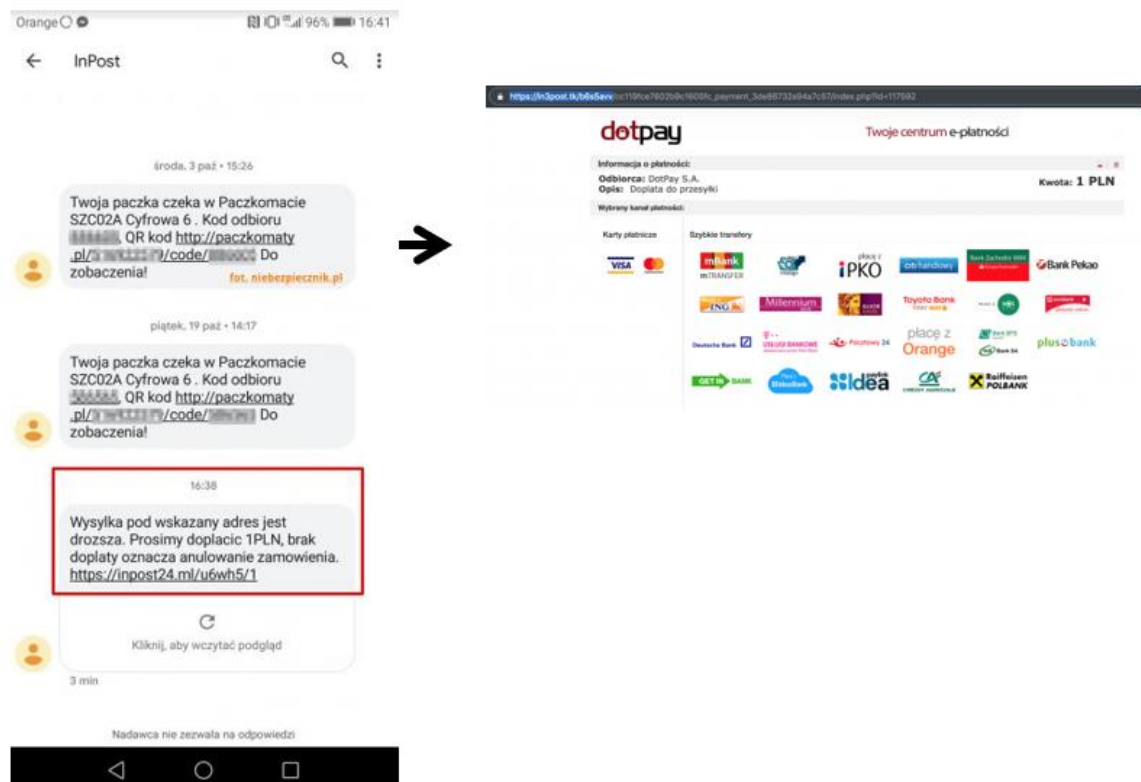
3. **Złośliwe oprogramowanie** (ang. malware) – może mieć również postać skryptu, działa szkodliwie i niebezpiecznie dla użytkownika. Przybiera różne formy (m.in. **wirusa** lub **exploita**) i rozmaite metody (np. przechwytywanie naciśniętych klawiszy na klawiaturze przez **keylogger**). Na ogół podszywa się pod znane firmy i rozsyła wiadomości spam, np. na temat zakupu na Allegro czy przesyłki z Poczty Polskiej. Takie ataki określa się jako **scam**, a ich wspólnym elementem jest załącznik ze złośliwym oprogramowaniem lub odnośnik do niego. Może on przyjmować różne postacie, także informacji wysyłanych przez bramki SMS. Prowadzą na ogół do nieprawidłowych adresów, które nieznacznie różnią się od prawdziwych (il. 18, 19), pod którymi kryje się złośliwe oprogramowanie.

⁴ Źródło: <https://niebezpiecznik.pl/post/kiepski-ale-smieszny-phishing-skierowany-w-klientow-ing-banku-slaskiego/>, data dostępu: 20.09.2024.

⁵ https://www.youtube.com/watch?v=SbCcmLqmQSS&ab_channel=Niebezpiecznik, data dostępu: 24.09.2024.



18. Przykład wiadomości phishingowej w postaci scamu - oferowanie darmowych biletów lotniczych⁶



19. Przykład wiadomości phishingowej w postaci scamu - dopłata do paczki⁷

⁶ Źródło: <https://niebezpiecznik.pl/post/uwaga-na-bezpłatne-bilety-lot-u-rozdawane-rzekomo-ze-względu-na-89-rocznicę-przewoźnika/>, data dostępu: 20.09.2024.

⁷ Źródło: <https://niebezpiecznik.pl/post/3-ataki-którymi-od-tygodni-cyberprzestępcy-okradają-polaków/>, data dostępu: 20.09.2024.

- 3.1. Przykładem programu służącego do przestępczości internetowej jest **ransomware**. Jego działanie polega na wnikięciu do atakowanego systemu i zaszyfrowaniu danych użytkownika, które zazwyczaj jest trudne albo niemożliwe do złamania. Po czym wyświetla się informacja dla odbiorcy, np. uruchamiana w oknie przeglądarki WWW, aby spełnić określone warunki i odzyskać dostęp. Najczęściej dotyczy to przelania na konto przestępcy określonej kwoty w zamian za klucz deszyfrujący (il. 20).



20. Przykład działania złośliwego oprogramowania typu ransomware⁸

- 3.2. Złośliwe oprogramowanie obecne jest również w serwisach społecznościowych takich jak Twitter lub Facebook. Atak przebiega przez umieszczenie linków na tablicach znajomych, które przed otwarciem wyglądają na zdjęcie, ale w rzeczywistości są wykonywalnym plikiem .exe. Po jego uruchomieniu komputer jest infekowany automatycznie (il. 21).

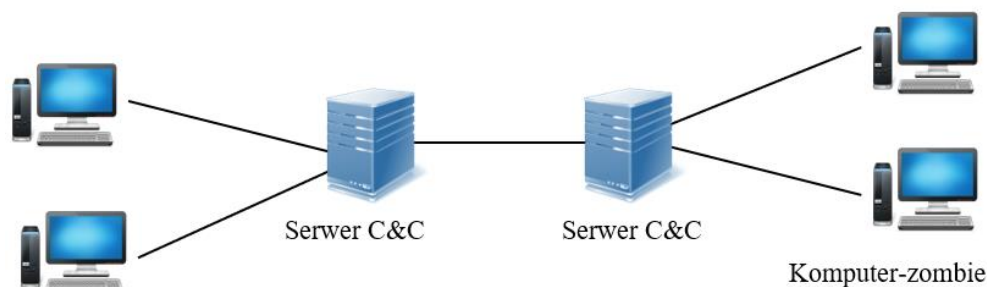


21. Przykład działania złośliwego oprogramowania w serwisie Facebook⁹

4. **Sieci botnetowe.** Botnet jest grupą komputerów zainfekowanych złośliwym oprogramowaniem (np. robakiem), które w ukryciu przed użytkownikiem wykonuje zdalne polecenia atakującego. W większości **komputer-zombie**, tj. należący do sieci botnet, realizuje przestępcze działania, np. ataki DDoS (ang. *Distributed Denial of Service*), kradzież poufnych danych lub rozsyłanie spamu, bez zgody i wiedzy właściciela. Znanym przypadkiem jest sieć ok. 4,5 mln komputerów zainfekowanych trojanem Zeus, co pozwoliło ukraść ok. 70 mln dolarów. Centralnym punktem każdego botnetu są **Serwery C&C** (ang. *Command and Control Servers*, nazywane także bot masterami) (il. 22). To one wydają rozkazy do komputerów-zombie i gromadzą wykradzione dane. W danym botnecie może istnieć więcej serwerów C&C. Bez ich zarządzającej roli sieć jest bezczynna, a zniszczenie jej polega na przejęciu nad nią kontroli.

⁸ Źródło: <https://niebezpiecznik.pl/post/zainfekowal-cie-cryptolocker-oto-jak-nie-placac-haracz-odzyskac-pliki/>, data dostępu: 20.09.2024.

⁹ Źródło: <https://niebezpiecznik.pl/post/nowa-fala-atakow-na-facebooku/>, data dostępu: 20.09.2024.



5. Komputer-zombie

22. Przykład działania sieci botnet

PAMIĘTAJ! Człowiek zazwyczaj jest najsłabszym ogniwem systemu bezpieczeństwa, którego nie da się kontrolować. Skłonny jest bezgranicznie ufać drugiej osobie, jeśli widzi dla siebie określone korzyści. Jeden z najbardziej znanych hakerów Kevin Mitnick często mówił, że łamał ludzi, nie hasła.

3.2. BEZPIECZEŃSTWO W SYSTEMIE WINDOWS

System Windows oferuje wiele możliwości zabezpieczeń. Jednym z jego ważnych elementów jest właściwe zarządzanie kontami oraz ich hasłami. Przyjmuje się, że każdy użytkownik powinien posiadać swój profil chroniony odpowiednio trudnym hasłem, bo łatwe do odgadnięcia są zazwyczaj pierwotnym i kluczowym problemem.

Bezpieczne hasła powinny podlegać trzem prostym zasadom¹⁰:

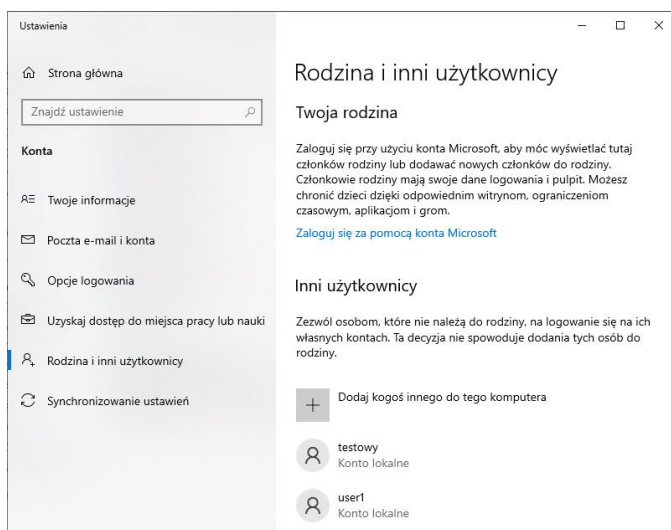
1. **Zawierać minimalnie 14 znaków:** dużych/małych liter, cyfr i znaków specjalnych, np. **ZpP.#B%!E("9<6e)=L38mv**. Można je wygenerować przy pomocy narzędzi takich jak Password Generator¹¹. Nie ma przeszkód, aby tworzyć silne hasła używając pełnych zdań, np. „zielonyParkingDla3małychSamolotow”. Trzeba jednak pamiętać, aby popularne cytaty znacząco modyfikować.
2. **Różne hasła do różnych usług.** Każde z nich powinno być unikatowe, w szczególności do kont: pocztowych, bankowych czy portali społecznościowych.
3. **Weryfikacja dwuetapowa.** To dwuskładnikowe uwierzytelnianie w czasie logowania, gdzie najpierw podaje się hasło bądź PIN, a potem jednorazowy kod, np. wysłany SMS-em, potwierdzenie w zainstalowanej aplikacji lub użycie dedykowanego klucza USB.

Zarządzanie kontami i grupami użytkowników w systemie Windows jest możliwe przy użyciu jednego z następujących narzędzi:

1. **Rodzina i inni użytkownicy** (Start > Ustawienia > Konta) - oferuje ograniczone możliwości (il. 23).

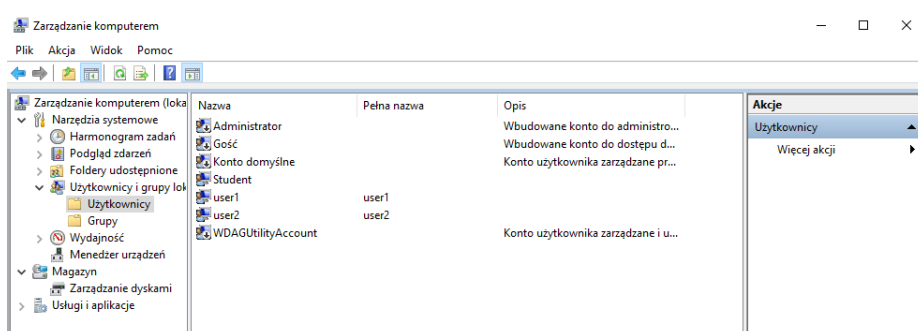
¹⁰ <https://cert.pl/bezpieczne-hasla/>, data dostępu: 21.09.2024.

¹¹ <https://www.passwordgenerator.com/>, data dostępu: 21.09.2024.



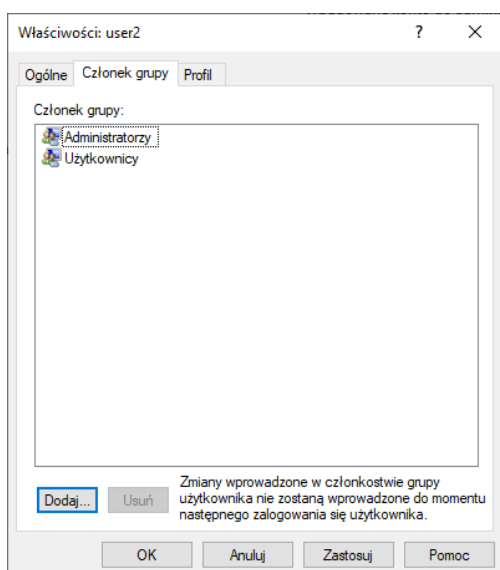
23. Narzędzie Rodzina i inni użytkownicy

2. **Użytkownicy i grupy lokalne** (Narzędzia administracyjne systemu Windows > Zarządzanie komputerem > Narzędzia systemowe > Użytkownicy i grupy lokalne). Aplet (il. 24) można też wywołać poleceniem **lusrmgr.msc**.



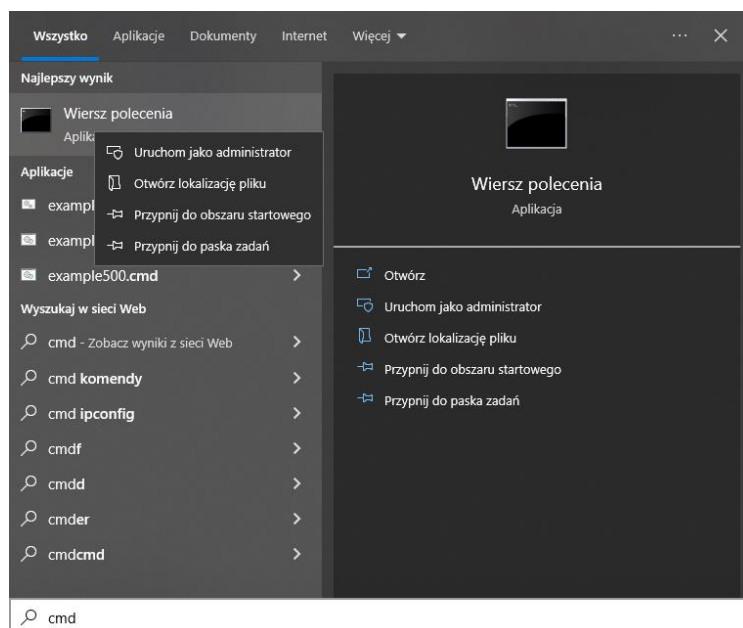
24. Okno zarządzania komputerem – widok zarządzania użytkownikami

Aby dodać użytkownika do grupy należy kliknąć na nim prawym przyciskiem myszy, wybrać opcję **Właściwości**, przejść do karty **Członek grupy** i kliknąć **Dodaj** (il. 25). Teraz można wskazać nazwę grupy, do której chcemy przydzielić użytkownika, np. Administratorzy.



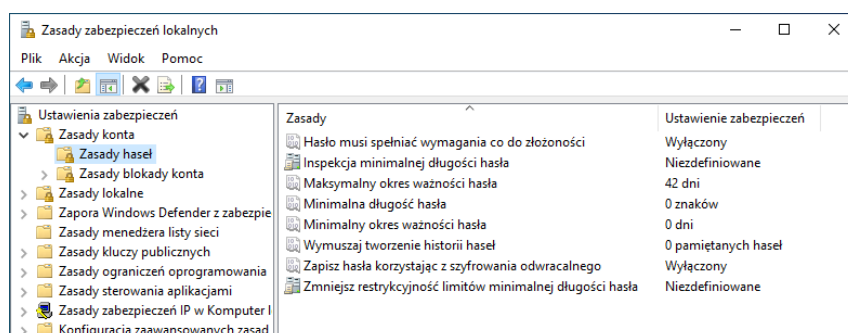
25. Okno właściwości użytkownika

3. Dyspozycja **net** w wierszu polecenia oferuje największe możliwości. Dodanie konta o nazwie **testowy** wymaga polecenia: **net user testowy * /ADD** (gwiazdka symbolizuje potrzebę podania hasła dla nowotworzonego konta). Usunięcie użytkownika odbywa się podobnie: **net user testowy /DELETE**. Do uruchomienia wiersza poleceń należy wpisać **cmd**. Warto zrobić to w trybie administratora, czyli kliknąć prawym przyciskiem myszy i wskazać opcję **Uruchom jako administrator** (il. 26).



26. Uruchomienie wiersza polecenia

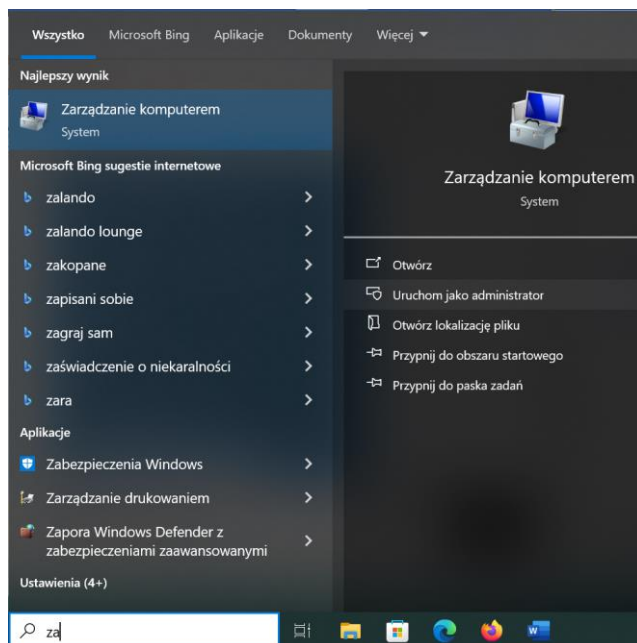
Konta użytkowników mogą posiadać zasady tworzenia, np. minimalną długość hasła czy okres jego ważności. Zmiana tych opcji wymaga przejścia do narzędzia **Zasady zabezpieczeń lokalnych** dostępnego w Narzędziach administracyjnych (il. 27).



27. Okno narzędzia Zasady zabezpieczeń lokalnych

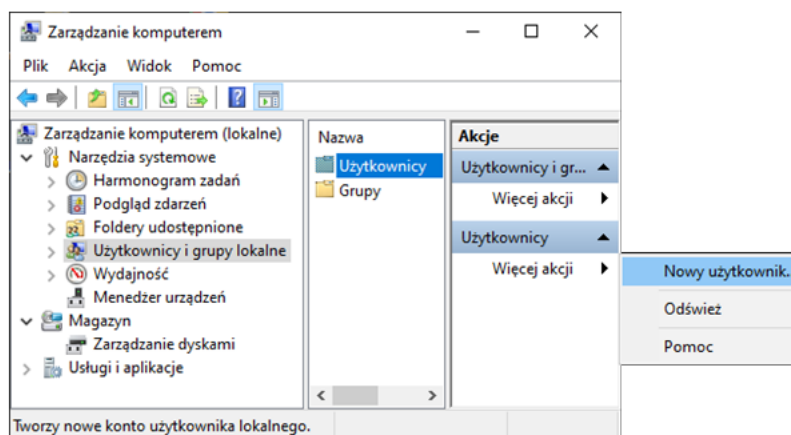
Przykład 17. Uruchom jako administrator narzędzie **Zarządzanie komputerem** i utwórz nowego użytkownika **Techno1**. Ustaw dla konta hasło i spraw, aby trzeba je było zmienić przy następnym logowaniu. Sprawdź działanie tego rozwiązania.

1. Kliknij:
 - 1.1. Menu **Start** i zacznij wpisywać pierwsze litery **Zarządzanie komputerem** (il. 29).
 - 1.2. Z prawej **Uruchom jako administrator** (il. 28).



28. Wyszukiwanie w menu Start

2. **Użytkownicy i grupy lokalne** (il. 29).
3. Po prawej stronie okna z menu kontekstowego dla **Użytkownicy** wybierz **Nowy użytkownik** (il. 29).



29. Okno Zarządzania komputerem – Użytkownicy i grupy lokalne

4. Wpisz nazwę **Techno1** i hasło (il. 30).

30. Okno nowego użytkownika

5. Zaznacz opcję **Użytkownik musi zmienić hasło przy następnym logowaniu** (il. 30).
6. Naciśnij **Utwórz i Zamknij** (il. 30).
7. Po zalogowaniu na konto Techno1 pojawia się komunikat o zmianie hasła.

Przykład 18. Wykorzystaj wiersz polecenia, aby utworzyć nowego użytkownika **Techno2**.

1. Uruchom wiersz polecenia **cmd** (il. 26).
2. Wpisz: **net user Techno2 * /ADD** (il. 31).
3. Wprowadź hasło i je powtórz je (il. 31).

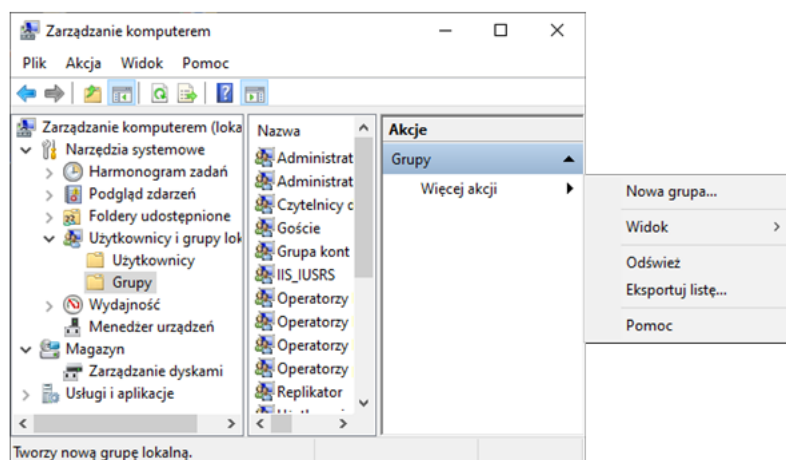
```
Microsoft Windows [Version 10.0.19045.6332]
(c) Microsoft Corporation. Wszelkie prawa zastrzeżone.

C:\Windows\system32>net user Techno2 * /ADD
Wpisz hasło dla użytkownika:
Wpisz hasło ponownie w celu potwierdzenia:
Polecenie zostało wykonane pomyślnie.
```

31. Tworzenie użytkownika Techno2 z dyspozycją net

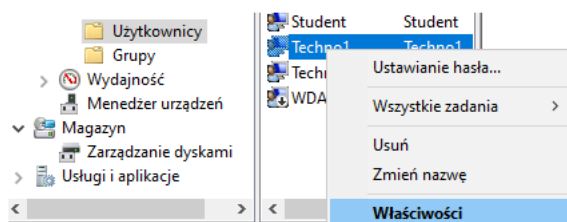
Przykład 19. Z narzędziem **Zarządzanie komputerem** utwórz nową grupę o nazwie **Technologia** i dodaj do niej konta **Techno1** oraz **Techno2**. Ponadto do grupy **Administratorzy** dołącz **Techno1**. Zaloguj się i sprawdź, czy każdy z użytkowników może utworzyć nową grupę?

1. Przejdź do Zarządzania komputerem > Użytkownicy i grupy lokalne > Grupy (il. 32).
2. Po prawej stronie okna z menu kontekstowego dla **Grupy** wybierz **Nowa grupa** (il. 32).



32. Okno zarządzania komputerem – widok zarządzania grupami

3. Wpisz nazwę **Technologia** i kliknij **Utwórz i Zamknij**.
4. Z lewej części okna wybierz **Użytkownicy** a po prawej z menu kontekstowego dla **Techno1** opcję **Właściwości** (il. 33).



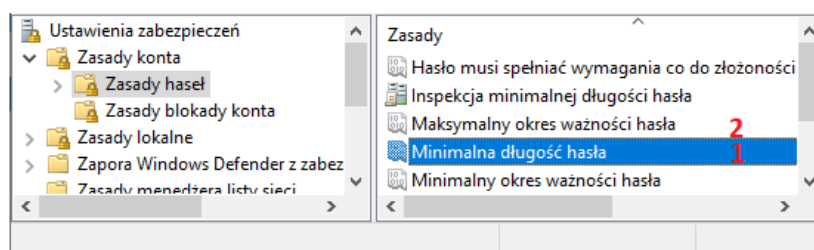
33. Fragment okna zarządzania komputerem - menu kontekstowe dla użytkownika Techno1

5. Na karcie **Członek grupy** wskaż **Dodaj**, a w kolejnych oknach dialogowych **Zaawansowane** i **Znajdź teraz**.
6. Kliknij dwa razy na grupie **Technologia**.
7. Pozamykaj okna dialogowe przyciskiem **OK**.

8. Powtórz czynności, aby dodać użytkowników do grup: **Techno1** do **Administratorzy** i **Techno2** do **Technologia**.
9. Po zalogowaniu na konto Techno1 system pozwala utworzyć nową grupę, w przypadku Techno2 nie jest to możliwe, bo pojawia się odmowa dostępu.

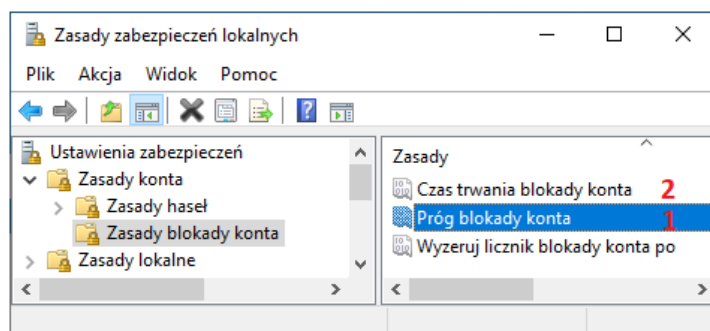
Przykład 20. Skonfiguruj system tak, aby hasło miało minimalną długość 14 znaków i było ważne tylko 30 dni. Próg blokady konta ustaw na 3 nieudane próby logowania i czas trwania blokady na 2 minuty. Sprawdź zachowanie systemu Windows po wprowadzeniu zmian i spróbuj zalogować się na konto **Techno1** podając czterokrotnie błędne hasło.

1. Wybierz **Start > Narzędzia administracyjne systemu Windows > Zasady zabezpieczeń lokalnych > Zasady konta**.
2. Wskaż **Zasady hasel** (il. 34):
 - 2.1. Minimalna długość hasła (il. 34, 1) i wprowadź liczbę 14.



34. Konfiguracja system - ustawianie hasła

- 2.2. Maksymalny okres ważności hasła (il. 34, 2) i wpisz 30.
3. Kliknij z lewej strony okna **Zasady blokady konta** (il. 35):
 - 3.1. Próg blokady konta (il. 35, 1) ustaw na 3 nieudane próby logowania.

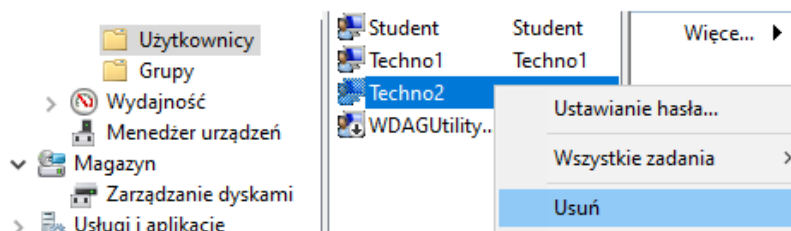


35. Konfiguracja system – blokada konta

- 3.2. Czas trwania blokady (il. 35, 2) na 2 minuty.
4. Po czterokrotnym wpisaniu błędnego hasła przy logowaniu jako użytkownik **Techno1** system Windows wyświetlił informację, że wywoływane konto jest obecnie zablokowane.

Przykład 21. Usuń konto **Techno2** z systemu z narzędziem **Zarządzanie komputerem**.

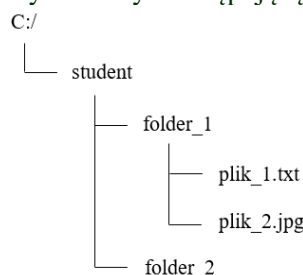
1. Otwórz **Zarządzanie komputerem**.
2. Wskaż **Użytkownicy i grupy lokalne**, a potem **Użytkownicy** (il. 36).
3. Kliknij prawym przyciskiem myszy na koncie **Techno2** i wybierz **Usuń** (il. 36).



36. Fragment okna zarządzania komputerem - usuwanie Techno2 z menu kontekstowego

4. ZADANIA

1. Oblicz:
 - 1.1. Ile bajtów zawiera 1MiB danych?
 - 1.2. Ile kibibajtów przechowuje plik, który zajmuje na dysku twardym 16384 B?
 - 1.3. Ile maksymalnie KiB danych może przesłać w ciągu sekundy łącze internetowe o przepustowości 50Mb/s?
2. Zapisz liczbę:
 - 2.1.1. Dwójkową 1000 000 000 w systemie dziesiętnym.
 - 2.1.2. Dziesiętną 68 w systemie dwójkowym.
 - 2.1.3. Szesnastkową B5F w systemie dziesiętnym.
3. Wykonaj konwersję kodowania pliku:
 - 3.1. Uruchom Notatnik i wklej tekst: **Zażółć gęślą jaźń.**
 - 3.2. Zapisz plik z nazwą **kodowanie.txt** i formatem UTF-8.
 - 3.3. Otwórz aplikację Visual Studio Code i wczytaj powyższy plik.
 - 3.4. Zmień jego kodowanie na ISO 8859-2 i zapisz.
 - 3.5. Obejrzyj go w programie Notatnik. Czy kodowanie polskich znaków jest poprawne? Jaki jest efekt przy otwieraniu tego pliku w programie Visual Studio Code?
4. Uruchom Eksploratora plików w systemie Windows:
 - 4.1. Przejdź do katalogu głównego (partycji) C:\ i skorzystaj z programów Notatnik oraz Paint, aby utworzyć następującą strukturę katalogowo-plikową (il. 37):



37. Struktura katalogowo-plikowa

- 4.2. Skopiuj **plik_1.txt** do **folder_2**.
- 4.3. Skasuj **plik_1.txt** w **folder_1**.
- 4.4. Przenieś **plik_2.jpg** do katalogu student.
- 4.5. Udostępnij folder_1 w trybie **tylko do odczytu**, a folder_2 **do odczytu i zapisu**.
- 4.6. W sali, gdzie odbywają się zajęcia sprawdź na sąsiednim komputerze udostępnione przez ciebie zasoby. Spróbuj zapisać dowolny plik do **folder_2**.
5. Dokonaj kompresji danych i utwórz plik o nazwie **zmniejszanie.zip**, który będzie zawierał katalogi z zadania 4 tj. folder_1 i folder_2 wraz z ich zawartością.
6. Usuń katalog **student**, z wyjątkiem pliku **zmniejszanie.zip**, a potem go przywróć i skontroluj zawartość całej struktury.
7. Zaloguj się na konto z uprawnieniami administratora i utwórz:
 - 7.1. Nowego użytkownika o nazwie **UWS1** z hasłem. Czy możesz utworzyć nowe konto mając uprawnienia użytkownika **UWS1**?
 - 7.2. Nowego użytkownika o nazwie **UWS2** z hasłem, które należy zmienić przy następnym logowaniu. Sprawdź działanie tej opcji.
 - 7.3. Grupę o nazwie **Studenci**. Dodaj do niej konta **UWS1** oraz **UWS2**, a **UWS1** ponadto do grupy Administratorzy. Czy każdy z tych użytkowników może tworzyć nową grupę?
8. Korzystając z narzędzia **Ustawienia zabezpieczeń lokalnych** skonfiguruj system, aby:
 - 8.1. Hasła były ważne tylko 14 dni.
 - 8.2. Minimalna długość hasła wynosiła 14 znaków.
 - 8.3. Po 2 nieudanych próbach zalogowania na konto czas trwania blokady wynosił 1 minutę.
9. Spróbuj zalogować się na konto **UWS2** podając trzykrotnie błędne hasło. Jak zareagował system Windows?

LITERATURA

Garfinkel S., Spafford G., Schwartz A., Practical UNIX and Internet Security. 3rd Edition, Wyd. O'Reilly Media, 2003.

<https://cert.pl/bezpieczne-hasla/>, data dostępu: 21.09.2024.

<https://iec.ch/homepage>, data dostępu: 10.09.2024.

<https://niebezpiecznik.pl>, data dostępu: 20.09.2024.

<https://www.passwordsgenerator.com/>, data dostępu: 21.09.2024.

https://www.youtube.com/watch?v=SbCcmLqmQSs&ab_channel=Niebezpiecznik, data dostępu: 24.09.2024.

SPIS TREŚCI

Wstęp	1
1. Podstawy pracy	1
1.1. System operacyjny i organizacja danych.....	1
1.2. Udostępnianie zasobów.....	5
1.3. Kompresja danych	6
1.4. Jednostki informacji i systemy liczbowe	7
2. Kodowanie plików tekstowych	9
3. Podstawy bezpieczeństwa komputerowego	10
3.1. Współczesne formy ataków	11
3.2. Bezpieczeństwo w systemie Windows.....	15
4. Zadania.....	21
Literatura.....	22