Nina Orzech

Akademia Wojsk Lądowych imienia generała Tadeusza Kościuszki
ORCID: 0000-0001-7363-7764

Tomasz Orzech

Akademia Nauk Stosowanych Angelusa Silesiusa
e-mail: torzech@ans.edu.pl
ORCID: 0000-0002-3225-5185

DOI: 10.71433/2025.87.1.04
JEL: O3

LOGISTYKA WOJNY – WOJNA LOGISTYKI. SYSTEMY BEZPIECZEŃSTWA INFORMACJI W SYTUACJACH KRYZYSOWYCH

Cytuj jako: Orzech, N. i Orzech, T. (2025). Logistyka wojny – wojna logistyki. Systemy bezpieczeństwa informacji w sytuacjach kryzysowych. W: B. Detyna (red.), *Branża TSL. Strategie – trendy – perspektywy. Seria: Logistyka. Współczesne Wyzwania, t. 15* (s. 48–58). Wydawnictwo Naukowe Akademii Nauk Stosowanych Angelusa Silesiusa.

Streszczenie

Przedmiot i cel pracy: Celem rozdziału jest przedstawienie ewolucji sposobów zabezpieczenia danych, od starożytności do epoki współczesnej. W tekście zaprezentowano wybrane, aktualne systemy zabezpieczeń, wykorzystywane obecnie w różnych dziedzinach.

Materiały i metody badawcze: W badaniach wykorzystano analizę literatury przedmiotu oraz dokumentacji technicznej urządzeń kodujących. Badania umożliwiły usystematyzowanie wiedzy o rozwoju zarówno techniki, jak i logistyki informacji.

Wyniki: Przedstawiono systemy bezpieczeństwa łączności na przestrzeni wieków. Ewolucja kodowania ograniczyła dostęp do wiedzy zarówno przekazywanej, jak i archiwizowanej osobom nieuprawnionym. Powstaniu szyfrów towarzyszył jednoczesny rozwój metod ich złamania zwany kryptoanalizą.

Wnioski: Każdy podmiot organizacyjny, bez względu na formę prowadzonej działalności, stara się chronić swoje dane przed nieuprawnionym dostępem. Zarówno podmioty gospodarcze, jak i gospodarstwa domowe mają swoje tajemnice.

Słowa kluczowe: bezpieczeństwo informacji, logistyka informacji

1. Wprowadzenie

Informacja zaliczana jest do kluczowych elementów rozwoju społeczeństw i zbiorowości. Jej powstawanie, przetwarzanie oraz przesył na duże odległości wykorzystywany jest przez większość gatunków zamieszkujących Ziemię. Przepływ informacji jest dla każdej formy życia podstawowym elementem przetrwania zbiorowości. To dzięki różnego typu wiadomościom poszczególne osobniki dowiadują się o zagrożeniach, pożywieniu, schronieniu oraz rozmnażaniu.

Do powiadamiania poszczególnych osobników każdej zbiorowości organizmy wykorzystują różne materiały oraz metody. Wśród ludzi transfer informacji pomiędzy poszczególnymi osobami nazywany jest komunikacją. Komunikacja jest procesem określonych znaków między nadawcą a odbiorcą. Przekaz informacji może przybierać postać zarówno werbalną, obejmującą teksty pisane oraz mówione, jak i niewerbalną, w skład której wchodzą umowne symbole, dźwięki, światła, mimika, gesty i intonacja.

2. Cel pracy i metodyka badawcza

Ludzkość od wieków chroniła informację. Bezpieczeństwo treści było istotne dla rozwoju państwowości. Celem rozdziału jest przedstawienie ewolucji ochrony najbardziej wrażliwych danych. Zmiany chronologiczne w zakresie kodowania informacji wpłynęły na rozwój komunikacji. Raz opracowane techniki kodowania informacji nigdy nie zostały wycofane z użytkowania, a celem uzupełniającym jest przedstawienie wybranych technik, które są używane do dziś.

Badanie ma na celu poznanie i zrozumienie rzeczywistości, która zapewni rozwój danej dyscypliny naukowej. Analiza może przybierać postać kumulatywną, czyli mającą formę doskonalenia, poszerzenia wiedzy, lub eliminacyjną, czyli mającą formę weryfikacji dotychczasowych osiągnięć i pozyskiwania nowych danych. Ze względu na tempo postępujących zmian osiągnięcia mogą mieć charakter ewolucyjny lub rewolucyjny (Niemczyk, 2020, s. 18).

Każde badanie powinno podlegać odpowiednim rygorom, które zalicza się do podstawowych wymogów. To rygory pozwalają na wprowadzanie do nauki różnych dowodów w postaci wyników badań, wyjaśnienia odchyleń. Aby mówić o rygorach należy uwzględnić ich podstawowe elementy. Do pierwszych należy trafność, czyli poprawność rozumowania oparta na ściśle określonych argumentach oraz algorytmach. Dzięki trafności można ustalić związki przyczynowo-skutkowe, które opierać się będą na posiadanej wiedzy. Kolejną częścią rygoru jest rzetelność, która bazuje na powtarzalności badań, z zachowaniem jednakowych technik. Badania mogą być przeprowadzone na różnych obiektach, a wyniki będą poddawane dalszej analizie z wykorzystaniem określonego wcześniej kryterium.

Jedną z najważniejszych metod badawczych jest analiza literatury. Dzięki tej technice można zdefiniować obecny stan wiedzy w danym zakresie oraz określić punkt wyjścia. Istotnym elementem analizy literatury jest postępujący rozwój informacyjny społeczeństwa. Cyfryzacja i usieciowienie wiedzy znacznie obniżają koszty pozyskania wiedzy (Czakon, 2020, s. 123).

3. Elementy systemów transferu informacji

Informacja zawsze była istotna dla ludzkości. Dzięki możliwości wykorzystania posiadanej wiedzy stała się cennym i pożądanym towarem. We współczesnym świecie nie tylko organizacje, ale również pojedyncze osoby nie są w stanie funkcjonować bez dostępu do aktualnych danych. Wszystkie informacje wynikają z procesu przetwarzania danych. Często efekt końcowy jest otrzymany dzięki operacjom logicznym i arytmetycznym, którym poddane są dane wejściowe. Zasoby te są różnorodne zarówno jakościowo, jak i ilościowo. W skład informacji niewerbalnych wchodzą różne elementy, które można odczytać za pomocą zmysłów, obrazy, dźwięk, zapach, temperatura, smak. Inną formą łączności jest komunikacja werbalna, a do niej zaliczymy mowę, filmy. Istotnymi narzędziami w procesie przetwarzania informacji jest moc obliczeniowa komputerów oraz możliwość łączenia tych urządzeń w sieć (Wrzosek, 2010, s. 99). Układ taki nie tylko zwiększa efektywność w zakresie dzielenia się wiedzą, ale również następuje wzrost liczby uczestników systemu komunikacyjnego.

Bezpieczeństwo informacji nabiera szczególnego znaczenia w przypadku wystąpienia konfliktu zbrojnego lub sytuacji kryzysowej. Logistyka wojny obejmuje zagadnienia związane z dostarczeniem danych wyłącznie adresatowi. Tylko on może rozkodować zaszyfrowaną treść. Wojna logistyki przedstawia sposoby odczytywania zakodowanych dokumentów, a skuteczność pracy służby wywiadowczej ułatwia podjęcie decyzji, czego efektem było zwycięstwo Polaków w sierpniu 1920 r. (Tłumaczenie szyfrogramu…). W rozdziale pominięto techniki zakłócania przesyłu informacji przez kontrwywiady, które również można zaliczyć do wojny logistyki.

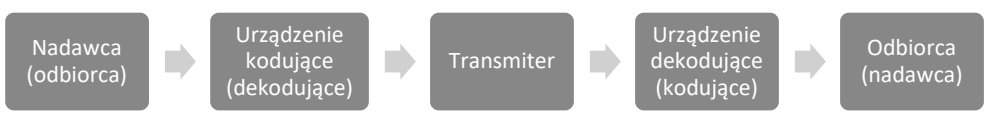
Każdy element danych, bez względu na jego źródło i rodzaj, poddawany jest odpowiedniej obróbce. Efektem przetwarzania danych wejściowych w trakcie odpowiednich zabiegów jest uzyskanie nowej wiedzy, która może być przydatna w dalszym procesie. W przypadku braku możliwości jej wykorzystania w danej procedurze nie staje się całkowicie bezużyteczna, gdyż może być użyta w innych systemach. Informacja podlega ocenie, a jej jakość jest określana według cech, takich jak:

- Pełność – określenie stopnia komplementarności wiedzy w danym zakresie. Nie uwzględnia się danych nieprzydatnych w określonym procesie, dlatego powinny być przynajmniej w znacznym stopniu zgodne z problemem. Kolejnym elementem wchodzącym w skład pełności jest czytelność danych. Muszą one być zrozumiałe dla końcowego adresata, w sposób uniemożliwiający błędną interpretację.

- Prawdziwość – informacja oparta na faktach, badaniach naukowych. Źródło wiedzy musi być wiarygodne. Musi istnieć możliwość weryfikacji danych. Do informacji zaliczamy wiedzę normatywną, opartą na przepisach oraz procedurach. Ważnym elementem jest możliwość oceny posiadanej wiedzy, przyporządkowania jej właściwych cech przydatności.
- Aktualność informacji – z uwzględnieniem upływającego czasu. Dane retrospektywne, dotyczące minionych okresów, mogą służyć do oceny minionych procesów. Bieżące dotyczą aktualnego przedziału czasowego, zaś perspektywiczne służą do oceny przyszłych stanów.
- Właściwość adresata – każda informacja powinna dotrzeć do osoby lub instytucji, która jest upoważniona do jej odbioru. Adresat nie tylko jest uprawniony do otrzymania określonej wiadomości, ale również może ją spożytkować we właściwy sposób. Niedoręczenie informacji odpowiedniej osobie prawdopodobnie zagrozi prawidłowemu przebiegowi procesu. Pozyskanie wiedzy przez osoby nieuprawnione może skutkować utratą efektu końcowego.

Ze względu na rodzaj przekazu wyróżniamy dwa podstawowe systemy – informatyczne i informacyjne. Systemy informatyczne nie zawierają człowieka. Systemy informacyjne to zbiór połączonych ze sobą elementów, zbierających i gromadzących dane, przetwarzania informacji, emisji wiedzy i zapewnienia sprzężeń zwrotnych (Keysy, 2011, s. 210).

Każdy system transferu informacji, bez względu na jego technologiczne zaawansowanie, posiada kilka podstawowych elementów, które przedstawione są na rys. 1 (prezentującym jednokierunkowy przepływ informacji). Prawie wszystkie układy umożliwiają sprzężenia zwrotne i dwukierunkowy przepływ danych, które mogą powodować powstanie relacji pomiędzy uczestnikami układu.



Rys. 1. Jednokierunkowy przepływ informacji

Źródło: opracowanie własne.

Nadawca to osoba, która tworzy informację. Wiadomość musi być wykonana w sposób zwięzły i zrozumiały dla odbiorcy. Treść przekazu powinna wykluczyć niewłaściwą interpretację. Nadawca dobiera system kodowania oraz technologię transmisyjną, chociaż często ten element jest ograniczony prawnie, technicznie oraz finansowo. Ważnym elementem jest rodzaj informacji, jaka ma zostać przekazana do odbiorcy. To nadawca określa jej treść, formę zapisu oraz sposób kodowania, jeżeli jest to wymagane pod względem prawnym, w tym bezpieczeństwa, lub technicznym.

Urządzenie kodujące i dekodujące to system zapisu oraz odczytu informacji za pomocą szyfrów. Kodowanie treści od wieków miało istotne znaczenie w systemach bezpieczeństwa oraz administrowania krajami. Kodowanie jest metodą, która powinna zapewnić bezpieczną eksploatację danych przed niepowołanym dostępem. Szyfry nie ograniczają dostępu do informacji, ale powodują, że jest ona nieczytelna dla osób nieuprawnionych.

Transmiter, zgodnie z definicją „Słownika języka polskiego PWN", to urządzenie służące do transmisji dźwięku, obrazu lub innych sygnałów za pomocą fal elektromagnetycznych (Słownik języka polskiego, b.d.). Wcześniej rolę transmitera przejmowali kurierzy i gońcy, zwierzęta, urządzenia sygnałowe, systemy pocztowe. W transporcie informacja jest najbardziej narażona na przechwycenie przez osoby niepowołane – można zobaczyć sygnały świetlne przesyłane np. za pomocą błysków, umówione obrazy – dymy, układy flag, chorągiewek, semafory, usłyszeć sygnały dźwiękowe, krzyki, mowę, przechwycić kurierów oraz zwierzęta czy sygnały radiowe.

4. Systemy szyfrowania i kodowania informacji

Każda informacja ma swoją ważność. Wraz ze wzrostem wartości przesyłanej wiadomości podnoszony jest poziom jej ochrony. Aby mieć pewność skutecznego i bezpiecznego dostarczenia danych, używa się wyrafinowanych metod szyfrowania, których podstawowe idee sięgają czasów starożytnych (Naskręcki, 2023 s. 18−19). Kodowanie informacji opiera się na zbiorach technik utrudniających ich odczyt, przez co zapewnia się odpowiedni poziom poufności. Posiadanie klucza deszyfrującego umożliwia szybkie odczytanie danych.

Techniki kryptograficzne związane z utajnianiem treści wykorzystywane są już od czasów antycznych. Samo pojęcie ,,kryptografia" pochodzi z języka greckiego, w którym *kryptos* oznacza ukryty, a *graphein* – pisanie. Starsze, egipskie formy ukrywania tekstu miały raczej znaczenie symboliczne, gdyż miały zmieniać sens treści zapisanej na grobowcach faraonów. Początki kryptografii używanej w celach politycznych miały miejsce w starożytnych Indiach (Karbowski, 2014, s. 21). Wiedza zawarta w tekście jawnym jest dostępna posiadaczowi informacji w momencie jej pozyskania. Taki dokument nazywamy jawnym (Sołtysik-Piorunkiewicz i Niklewicz, 2019 s. 127). Żeby uniemożliwić pozyskanie wiedzy, stosuje się techniki kodowania z użyciem kluczy, czyli zbiorów wartości, znaków oraz tekstów. Utajniony tekst zapisany za pomocą odpowiedniego klucza nazwany zostaje kryptogramem. Aby odtajnić ukrytą informację, należy poddać ją zabiegowi deszyfrowania (Stachowiak, 2022 , s. 18).

Wyróżnia się dwie podstawowe techniki ukrywania wiadomości w przekazie. Pierwszym jest technika symetryczna, polegająca na użyciu tego samego klucza zarówno do kodowania, jak i rozkodowania informacji. Technika ta była popularna do połowy XX wieku i charakteryzowała się prostotą użytkowania. W przypadku roz-

kodowania informacji przez osoby niepowołane istnieje możliwość wykorzystania zdobytej przez nich wiedzy, a nawet możliwość stworzenia własnej, fałszywej wiadomości. Metoda asymetryczna wykorzystuje dwa różne klucze. Pierwszy, zwany publicznym, służy do tworzenia kryptogramu. Drugi klucz, dostępny wyłącznie dla odbiorcy, nazywany jest również kluczem prywatnym (OVHcloud, b.d.).

Od starożytności popularne były dwie techniki kodowania informacji – przestawna i podstawna. System przestawny powstał w starożytnej Grecji, gdyż Spartanie do utajniania informacji używali skytale. Urządzenie to składało się z dwóch identycznie wielokątnie obrobionych podłużnie kawałków drewna z nawijanym wąskim paskiem pergaminu. Na pergaminie tworzono zapis, wykorzystując fragment powierzchni paska pergaminu o kwadratowej powierzchni, która przylegała do jednego boku drewna, jako miejsce na jedną literę. Na owiniętym pergaminie nie pozostawiano wolnych przestrzeni. Na pergaminie, mimo wykorzystania otwartego tekstu, po rozwinięciu ukazywał się chaotyczny ciąg liter. Dopiero ponowne nawinięcie pergaminu na drugi kawałek drewna dawało możliwość odczytu informacji. Ewolucja metody opracowanej przez starożytnych Spartan dziś jest wykorzystywana w informatyce (Menon i in., 2020, s. 153).

Pierwszy właściwy szyfr został stworzony na potrzeby Juliusza Cezara i od jego nazwiska przyjęto nazwę. Metoda kodowania oparta była na podstawieniu liter jawnego alfabetu inną literą. Sama technika polegała na przestawieniu litery o określoną liczbę w alfabecie. Inna technika została wykorzystana w kodzie hebrajskim Atkbasch, w którym zamianie podlegały pierwsza i ostatnia litera, druga i przedostatnia itd.

Wraz z powstawaniem szyfrów powstała dziedzina nauki zwaną kryptoanalizą, zajmująca się łamaniem szyfrów. Nauka ta rozwinęła się w VIII wieku na terenach krajów arabskich. Zgodnie z zasadą Al-Kindiego podczas ataku kryptoanalitycznego w pierwszej kolejności należy ustalić język nadawania. Następnie należy z tekstu o objętości minimum jednej strony ustalić, jak licznie występują poszczególne litery. Najczęściej występująca głoska będzie pierwszą, kolejna drugą itd. Tak opracowany alfabet nakłada się na tekst do rozszyfrowania (Singh, 2001 s. 31). Dzięki temu opracowaniu szyfry monoalfabetyczne są łatwe do złamania.

Kolejne wieki przyniosły stagnację w zakresie kryptologii (nauka o szyfrach), kryptografii (nauka o konstruowaniu i stosowaniu szyfrów) oraz kryptoanalizy. Jedynie zakony w ograniczonym zakresie stosowały zmodyfikowane szyfry Cezara. Do rozwoju szyfrów doprowadziły dopiero prace niemieckiego zakonnika Johannesa Trithemiusa (Holden, 2017, s. 56-57), który rozszerzył szyfr Cezara poprzez zastosowanie dodatkowe − nie tylko o inny alfabet, ale również o przesunięcie o kolejną literę w nowym alfabecie. W ten sposób Trithemius stworzył jeden z pierwszych szyfrów polialfabetycznych.

Ważnym elementem rozwoju kryptologii jest modyfikacja szyfru Trithemiusa wykonana przez Giovana Bellaso w XVI wieku. Jeszcze za jego życia Blaise de Vigenère zmodyfikował system kodowania wiadomości, w której jedynie wybrane wiersze utajnia się za pomocą z tablicy *tabula recta*. Wersy wybrane do szyfrowania

określone są słowem kluczem, a litery tego słowa wskazują kolejne zakodowane linijki. Szyfr Viegenère'a przez długi czas był niezłamany. Dopiero w XIX stuleciu dokonał tego Charles Babbage (Sobański, 2021, s. 5).

Inną metodą utajniania informacji jest korzystanie z książek kodowych. W przeciwieństwie do szyfrów, które za pomocą odpowiedniej techniki utajniają poszczególne litery, kody mogą ukrywać nie tylko słowa, ale również całe zdania. W przypadku połączenia książki kodowej z szyfrem powstaje wielokrotne szyfrowanie, co bardzo utrudnia kryptoanalizę. Do wad kodu należą trudności związane z zabezpieczeniem książek kodowych. Powtarzalność sygnałów oraz ograniczenie liczby symboli powodują, że przy dużej częstotliwości korzystania z tego systemu za pomocą metod statystycznych istnieje łatwa możliwość odczytania tekstu.

Innym systemem ochrony są kody jednorazowe. Układy te są tak zaprojektowane, aby w sposób oficjalny przesłać określoną treść do adresata. Może nią być zwykła rozmowa, tekst, melodia lub obraz rozpowszechniony za pomocą masowych środków przekazu. Jedynie nadawca i odbiorca znają znaczenie informacji. Bardziej rozwiniętym systemem jest kod idioty, w którym za pomocą odpowiednich otwartych tekstów przekazywane są ukryte wiadomości. W Polsce podczas walk obronnych już 3 września 1939 roku szyfry wojskowe zostały zdobyte przez Niemców. Naczelne dowództwo wydało rozkaz posługiwania się niezrozumiałym żargonem do momentu otrzymania nowego szyfru (Markowski i Miarzyński, 2007, s. 72).

Do najskuteczniejszych technik szyfrowania jednorazowego należą metody oparte na generowaniu liczb. Już w roku 1917 Gilbert Wernan opatentował szyfr bazujący na technologii dalekopisu (Zgłoszenie patentowe nr: patent USA 1,310,719…). Każda cyfra, litera czy znak interpunkcyjny posiadały elektroniczne połączenie z papierową perforowaną taśmą, dzięki czemu powstał jednorazowy system taśmowy. Dodatkowo, aby utrudnić kryptoanalizę, każdy znak zamieniany był na losowy ciąg cyfr. W połączeniu z książką kodową tak zaszyfrowana informacja jest niemożliwa do odkodowania. Do wad systemu zalicza się generowanie oraz transport fizyczny szyfrów i kodów. Utrata lub ich skopiowanie powodują, że system jest bezwartościowy.

Najsłynniejszym, a zarazem najskuteczniejszym użyciem kodu idioty było wykorzystanie języka plemienia indiańskiego Nawaho przez marynarkę Stanów Zjednoczonych. U.S. Navy podczas walk na Pacyfiku z Japonią zmobilizowało 400 Indian, którzy mówiąc w swoim rzadko spotykanym, ojczystym języku przekazywali informacje otwartym tekstem (Dahl, 2016, s. 73−74). Japońscy kryptoanalitycy nigdy nie złamali amerykańskiego kodu. Nie ustalili języka tekstu, co zgodnie z pierwszą zasadą Al-Kindiego jest podstawowym elementem kryptoanalizy.

Obecnie do szyfrowania wiadomości stosuje się różnego rodzaju oprogramowania komputerowe. W tym celu powstały algorytmy szyfrujące. Popularnym algorytmem służącym do asymetrycznego szyfrowania danych jest RSA (algorytm Rona Rivesta, Adi Shamira, Leonarda Adlemana), który do szyfrowania wykorzystuje klucze

publiczny i prywatny, obliczane na podstawie danych liczb pierwszych (Chrzęszczyk, 2010, s. 154).

Kolejnym ważnym kryptosystemem jest algorytm DES, uważany za szyfr symetryczny. DES jest szyfrem blokowym. Wykorzystuje wielowarstwową sieć podstawieniowo-przestawieniową. Posiada 64-bitowe bloki wiadomości jawnej i szyfrogramu oraz 56-bitowy klucz z ośmioma bitami parzystości (Nikodem, 2008, s. 18–19).

Pod koniec lat 80. w ETH (Szwajcaria) powstał system IDEA (International Data Encryption Algorithm). Jest to szyfr blokowy, iteracyjny. Jego układ został oparty na kilku kolejnych operacjach arytmetycznych. Typowy rozmiar bloku wynosi 128 bitów, a w jego skład wchodzą dwa 64 bitowe bloki – zaszyfrowany i otwarty.

5. Wybrane maszyny szyfrujące

Od wieków ludzkość starała się przyspieszyć i zautomatyzować proces utajnienia oraz dekodowania informacji. W średniowieczu w 1447 roku Leon Alberti stworzył dysk szyfrujący, który obsługiwał opracowany przez niego szyfr polialfabetyczny, ale wynalazek został przypisany autorstwu Blaise'a de Vigenère. Urządzenie to było zbudowane z dwóch koncentrycznie ułożonych dysków. Na zewnętrznej części litery były ułożone alfabetycznie, a na mniejszej, wewnętrznej, ułożenie liter było dowolne. Zewnętrzny dysk był dyskiem stałym i reprezentował tekst jawny, obrotowy środkowy służył do szyfrowania. Zmodernizowane wersje tego rządzenia były wykorzystywane przez różne wojska aż do wojny wietnamskiej.

Pierwsze udane mechaniczne urządzenie do kodowania stworzył późniejszy prezydent Stanów Zjednoczonych, jednocześnie sygnatariusz deklaracji niepodległości – Thomas Jefferson (Pastusiak, 1999, s. 86–93). Jego rozwiązanie opierało się na 20-elementowym cylindrze Étienne'a Bazeriesa. Po modyfikacji układ Jeffersona składał się z 36 dysków, a na każdym zapisany był alfabet w innej kolejności. Urządzenie to, pod nazwą M-94, było używane przez U.S. Army nawet podczas drugiej wojny światowej.

Innym przełomowym urządzeniem był prosty przyrząd szyfrujący Franca Baldwina z 1877 roku, składający się z trzech obrotowych tarcz na jednym dysku. Dwie zewnętrzne tarcze były zapisane literami alfabetu, z czego jedna − zgodnie z tarczą zegara, a wewnętrzna − cyframi od 0 do 25 (Zgłoszenie patentowe nr: patent US197199…).

Mocno rozwiniętym systemem kodującym była stworzona w 1917 roku przez Hugo Kocha i Arthura Scherbiusa maszyna kodująca Enigma. Urządzenie to na początku używane było przez instytucje cywilne wielu krajów. Początkowa uboga wersja maszyny była przeznaczona dla kodowania informacji przez urzędy pocztowe, a do jej użytkowników należały takie kraje, jak Polska, Stany Zjednoczone, Szwecja, Holandia, Japonia. Niektóre urządzenia pocztowe wyposażone były w specjalistyczne maszyny do pisania.

Enigma zbudowana była z kilku wirników, a ich liczba, w zależności o wersji, wynosiła od trzech do ośmiu rotorów. W ułożeniu szeregowym przypominały cylinder Jeffersona. W przeciwieństwie do wynalazku prezydenta USA każdy wirnik Enigmy w zasadzie działania przypominał dysk Baldwina. Do podobieństw należy zaliczyć 26 pól na obwodzie rotoru, a do różnic system połączeń – zamianę mechaniczno-wizualną na styki elektryczne z możliwością wydruku lub zapisu maszynowego. Połączenie pewnej liczby cylindrów oraz regulowanego dysku znacznie zwiększyło liczbę kombinacji. Podobnie działającym urządzeniem była polska Lacida z 1930 roku, której rozwiązania wykorzystano w Enigmie typu C i D, jako w protoplastach Enigmy I (Kapera, 2022, s. 33). Podobnie do Enigmy działały brytyjska maszyna Lorenza z 1940 roku, japońska Purple i amerykańska Sigaba.

Na doświadczeniach użytkowania Enigmy polskie Biuro Szyfrów podległe Ministerstwu Spraw Wewnętrznych w latach 60. XX wieku opracowało Dalekopisowe Urządzenie do Elektronicznego Kodowania. Z pierwszych liter maszyny powstał akronim DUDEK, poprzedzony skrótem rozwojowym. TgS-1 oznaczał wersję podstawową stacjonarną, a TgS-3 oparty był na systemach scalonych. Urządzenie DUDEK miało istotny wpływ na jego wojskowego odpowiednika BOCIAN-M, przy którego konstruowaniu wykorzystano doświadczenia funkcjonariuszy MSW (Malczeski i in., 2018, s. 59). Polskie systemy były pierwszą generacją urządzeń elektromechanicznych z maszyną do kodowania i dekodowania za pomocą szyfru Vernama oraz książek kodowych. Informacja była zapisywana ręcznie za pomocą klawiatury dalekopisu bądź dzięki czytnikowi rolkowemu. Z TgS DUDEK korzystały wszystkie państwa bloku wschodniego. Maszyny były rozpowszechnione na całym świecie, a w Polsce zostały wycofane dopiero w 2011 roku.

Obecnie wszystkie kraje używają z cyfrowych urządzeń kodujących i transmisyjnych. W przypadku wykorzystania polskiej techniki klucze przekazywane są fizycznie w postaci nośników elektronicznych – zmieniła się technologia, ale nie system kodujący. Wysokie koszty użytkowania powodują, że z tej techniki korzysta się bardzo rzadko, a zarazem systematycznie. W celu przekazania kluczowej informacji szyfry w rzeczywistości używane są jeden raz. W praktyce często wielokrotnie stosuje się jeden szyfr. Stan taki powoduje wykorzystanie posiadanych urządzeń, jednocześnie za pomocą słowa klucza umożliwia przekazanie informacji odbiorcy, że następna wiadomość będzie inaczej kodowana.

6. Podsumowanie

W rozdziale opisano rozwój systemów bezpieczeństwa łączności oraz informatyki na przestrzeni wieków. Ewolucja systemów kodowania spowodowała wzrost bezpieczeństwa wiedzy zarówno przekazywanej, jak i archiwizowanej. Powstaniu szyfrów towarzyszył jednoczesny rozwój metod ich złamania, zwany kryptoanalizą. Na początku budowano proste szyfry przestawieniowe, a do ich złamania służyły

techniki statystyczno-matematyczne. Wraz z rozwojem matematyki i mechaniki nie tylko przyspieszał proces kodowania informacji, ale również powstały układy trudniejsze do odczytania. Przełomem w bezpieczeństwie danych była słynna Enigma, która wykorzystała dostępne wówczas techniczne rozwiązania w zakresie szybkości kodowania. W urządzeniu zastosowano prostą technikę przestawieniową, ale liczba składowych urządzenia komplikowała odzyskiwanie danych. Dopiero maszyna obliczeniowa Turinga, wykorzystując system binarny, pozwoliła skutecznie łamać niemieckie szyfry. Obecnie cyfrowe układy rozwojowe Enigmy służą do ochrony informacji bankowej oraz podmiotów państwowych o mniejszym znaczeniu.

Kolejną innowacją jest polskie urządzenie TsG DUDEK, które wykorzystuje jednorazowy szyfr Vernama oraz książki kodowe. Mimo zmian technologicznych system ten jest stosowany do utajniania najważniejszych informacji o znaczeniu strategicznym.

Bibliografia

Chrzęszczyk, A. (2010). *Algorytmy teorii liczb i kryptografii w przykładach*. Wydawnictwo BTC.

Czakon, W. (2020). Metodyka systematycznego przeglądu literatury. W: W. Czakon (red.), *Podstawy metodologii badań w naukach o zarządzaniu*. Wydawnictwo Nieoczywiste.

Dahl, A. (2016). *The Navajo code talkers of World War II: The long journey towards recognition, Historical perspectives* (Series II, Volume XXI). Santa Clara University.

Holden, J. (2017). *The mathematics of secrets: Cryptography from Caesar Ciphers to digital encryption*. Princeton University Press.

Kapera, Z. (2022). Marian Rojewski a Enigma 1932-1939. W: W. Giermaziak (red.), *Marian Rojewski w służbie polskiej kryptologii.* Wydawnictwo Agencji Bezpieczeństwa Wewnętrznego.

Karbowski, M. (2014). *Podstawy kryptografii, wydanie III.* Wydawnictwo Helion.

Keysy, M. (2011). Informacja i systemy informacyjne w działalności gospodarczej. *Dydaktyka Informatyki*, (6), 205−221.

Malczewski, M., Michniak, J. Oszywa, W., Pakuła, M., Lenert, M., Kosobucki, Z., Rudnicki L., Kałamaga, R., Gulina, J., Jakóbczak, M., Marecki, J., Gronowski, L., Turek, M. (2019). *70 lat z historii i dorobku Wojsk Łączności i Informatyki Wojska Polskiego.* Wydawnictwo ŚZPŻŁ. https://szpzl-zegrze.waw.pl/szpzl/pdf/70_lat_historii.pdf

Markowski, S., Miarzyński, Z. (red.). (2007). *Studium łączności w kampanii polskiej 1939 roku. Przegląd Łączności i Informatyki*, (3). https://szpzl-zegrze.waw.pl/szpzl/pdf/przeglad_4.pdf

Menon, U., Hudlikar, A., Panda, D. (2020). *Scytale – an evolutionary cryptosystem V.8.* Akanksha Building, Mumbai Highway.

Naskręcki, B. (2023). Czym jest szyfrowanie. *Magazyn Polskiej Akademii Nauk,* (4/76). https://www.researchgate.net/publication/376666046_Czym_jest_szyfrowanie

Niemczyk, J. (2020). *Metodologia nauk o zarządzaniu.* W: W. Czakon (red.). *Podstawy metodologii badań w naukach o zarządzaniu*. Wydawnictwo NieOczywiste.

Nikodem, M. (2008). *Metody ochrony przed kryptoanalizą z uszkodzeniami* [niepublikowana rozprawa doktorska]. Politechnika Wrocławska. https://www.dbc.wroc.pl/dlibra/publication/2245/edition/2297?language=pl

OVHcloud. (b.d.). Pobrano 12 maja 2024 z https://www.ovhcloud.com

Pastusiak, L. (1999). *Prezydenci Stanów Zjednoczonych Ameryki Północnej.* Iskry.

Singh, S. (2001). *Księga szyfrów.* Albatros.
Słownik języka polskiego. (b.d.). *Transmiter*. Pobrane 18 marca 2024 z https://sjp.pwn.pl/sjp
Sobański, K. (2021). Od Cezara przez Sanatorium do Sobieskiego, czyli odkrywanie metody i klucza szyfrowania w protokołach akcji „Iskra-Dog". *Z Archiwum Instytutu Zachodniego*, (30). https://www.iz.poznan.pl/archiwum/2021/05/21/iskra-dog_szyfry-nr-30-2021/
Sołtysik-Piorunkiewicz, A., Niklewicz, P. (2019). Metody kryptograficzne we współczesnej kryptoanalizie – założenia, wyzwania, problemy. *Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach, „Informatyka i Ekonometria", 15*(390). http://bazekon.icm.edu.pl/bazekon/element/bwmeta1.element.ekon-element-000171595197?q=bwmeta1.element.ekon-element-19ce24ac-3d04-31ed-ba8f-a5b167eccc64;8&qt=CHILDREN-STATELESS
Stachowiak, S. (2022). *SAT – kryptoanaliza wybranych algorytmów kryptografii Symetrycznej*. Szkoła Główna Gospodarstwa Wiejskiego.
Tłumaczenie szyfrogramu: od Szt. 3 Korp. Kaw. Do IV Armji przejęty 9/8 odczytano 10/8 nr 370 [pisownia oryginalna].
Wrzosek, M. (2010). Wiedza w zarządzaniu organizacją wojskową. *Organizacja i Zarządzanie,* (12). https://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.baztech-article-BSL2-0025-0036
Zgłoszenie patentowe nr: patent USA 1,310,719 z 1919 roku.
Zgłoszenie patentowe nr: patent US197199 z 1877 roku.

War Logistics – Logistics of War. Information Security Systems in Crisis Situations

Abstract

Subject and purpose of the study: The purpose of the research is to present the evolution of data protection methods, from ancient times to the modern era. Selected current security systems used in various fields are also presented.

Materials and research methods: The research utilized an analysis of literature on the subject as well as technical documentation of encoding devices. This study enabled the systematization of knowledge concerning both technological development as well as logistics of information.

Results: The study presents communication security systems throughout history. The evolution of encryption has restricted access to both transmitted and archived knowledge from unauthorized individuals. The development of ciphers was accompanied by the simultaneous evolution of methods to break them, known as cryptanalysis.

Conclusions: Every organizational entity, regardless of the form of its operations, seeks to protect its data from unauthorized access. Both businesses and households have their secrets.

Keywords: information security, information logistics