BEZPIECZEŃSTWO INFORMACYJNE

Cyberterroryzm, przestępczość komputerowa

Jerzy Kuck

BEZPIECZEŃSTWO INFORMACYJNE

Cyberterroryzm, przestępczość komputerowa

Jerzy Kuck

Wydawnictwo Państwowej Akademii Nauk Stosowanych
im. ks. Bronisława Markiewicza w Jarosławiu

Wydawnictwo UNUM

Jarosław–Kraków 2025

Recenzja wydawnicza
dr hab. Danuta Kaźmierczak, prof. UKEN

Korekta
Katarzyna Trusewicz

Łamanie
Sławomir Karetko

ISBN 978-83-65823-76-2 (druk)

Wydawnictwo Państwowej Akademii Nauk Stosowanych
im. ks. Bronisława Markiewicza w Jarosławiu
37-500 Jarosław, ul. Czarnieckiego 16
wydawnictwo@pansjar.edu.pl
+48 16 624 40 65

ISBN 978-83-7643-269-4 (online)

DOI: https://doi.org/10.21906/9788376432694

Wydawnictwo UNUM
31-002 Kraków, ul. Kanonicza 3
unum@ptt.net.pl
+48 (12) 422 56 90

SPIS TREŚCI

Ile jest warta informacja wie ten, kto ją stracił (ujawnił) autor

WSTĘP

Historia informacji - jej pozyskiwania, gromadzenia, przechowywania i przekazywania sięga prawdopodobnie samego początku gatunku *homo sapiens*. Prawdopodobnie, bo obecnie nikt nie jest w stanie temu wiarygodnie zaprzeczyć lub to potwierdzić[1]. W okresie XIX-XX wieku ludzie przekazywali sobie wiadomości pisząc listy, stosując alfabet morsa i słuchając radia. Większych zastrzeżeń nie budzi stwierdzenie, że istotnym elementem każdej społeczności, nie tylko ludzkiej, ale i zwierzęcej, jest komunikacja (przekazywanie informacji). Bez takiej czy innej formy komunikacji nie można mówić o społeczności, lecz, co najwyżej, o jakimś luźnym zbiorowisku. Społeczność bowiem wymaga współdziałania, współpracy, a tych nie będzie bez komunikacji. Komunikat może mieć różną formę i być skierowany do wszystkich zmysłów. Zbiór osób, tworzących społeczeństwo ludzkie, potrzebuje wielu zróżnicowanych form przekazywania informacji.

Gromadzenie i przekazywanie informacji miało miejsce niemal od zawsze. Informacja to (łac. *informatio*), wyobrażenie, wyjaśnienie, zawiadomienie. Omawiane pojęcie, w zasadzie niedefiniowalne ze względu na jego pierwotny, elementarny charakter, rozpatrywane jest najczęściej w trzech aspektach:

- **syntaktycznym** – dotyczy ilości informacji, jaka może być potencjalnie zawarta w danej **wiadomości**. W tym przypadku definiuje się informację

[1] https://www.komputerswiat.pl/recenzje/sprzet/komponenty-pc/zarys-historii-nosnikow-informacji-czesc-pierwsza-wczoraj/w4peyq2 [dostęp: 27.03.2024].

albo poprzez ilość (miarę) informacji **(informacji - teoria)**, albo jako synonim pojęcia dane;
- **semantycznym** – znaczenia i zawartości treściowej wiadomości;
- **pragmatycznym** – przydatności informacji, tj. wartości informacji zawartej w wiadomości ze względu na realizowany przez odbiorcę cel[2].

Literatura przedmiotu oferuje szereg definicji informacji odmiennie pojmowanej w obrębie nauk humanistycznych, biologicznych, matematycznych, technicznych czy ekonomicznych[3]. Jacek Janowski uważa, że nie jest możliwe zdefiniowanie informacji na poziomie ogólnonaukowym i zaproponował trzy metody skutecznego posługiwania się tym terminem:
- **podejście opisowe** – posługiwanie się terminem „informacja" za pomocą wskazania jej cech lub funkcji;
- **podejście intuicyjne** – traktowanie informacji jako pojęcia niedookreślonego, rozumianego w sposób intuicyjny, umożliwiającym formułowanie bardziej złożonych definicji;
- **podejście systemowe** – posługiwanie się terminem „informacja" na podstawie istniejących już definicji, w obrębie konkretnej dziedziny, sytuacji.

W obszarze badań nad informacją stosowane są elementy wszystkich wskazanych metod. Powszechnie przyjęto podział na obiektywny i subiektywny (kognitywistyczny) model ujmowania informacji[4]. Podział ten związany jest z przytoczonym powyżej rozróżnieniem na syntaktyczny, semantyczny oraz pragmatyczny aspekt informacji. Subiektywny punkt widzenia informacji częściej znajduje zastosowanie w ramach nauk humanistycznych, biologicznych, ekonomicznych oraz prawnych. Natomiast obiektywny punkt widzenia informacji stanowi głównie domenę nauk ścisłych, w których informacja jest definiowana poprzez parametry fizyczne lub strukturalne obiektów[5].

---

[2] Hasło: „Informacja", Encyklopedia PWN: źródło wiarygodnej i rzetelnej wiedzy, https://www.bing.com/search?q=informacja&form=ANSPH1&refig=792fd7d423674e7e9be7cb9d9936f537&pc=U531 [dostęp: 05.01.2023].

[3] M. Barański, *Informacja w ujęciu prawnym przez pryzmat zagadnień terminologicznych*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2017, s. 19-24.

[4] J. Janowski, *Technologia informacyjna dla prawników i administratywistów. Szanse i zagrożenia elektronicznego przetwarzania danych w obrocie prawnym i działaniu administracji,* wyd. Difin, Warszawa 2009.

[5] P. Przybyłowicz, *Wstęp do teorii informacji i kodowania*, wstep_do_teorii_informacji - [PDF Document] (vdocuments.mx) [dostęp: 20.04.2024].

Na potrzeby niniejszego opracowania właściwe wydaje się przywołanie definicji cybernetycznej, która, jak zauważa Maciej Kłodawski, pozwala na szerokie ujmowanie informacji[6]:

Informację stanowi nie tylko wszelki opis, lecz także nakazy, zakazy, polecenia, dyrektywy działania. Z punktu widzenia formy informacja może być wyrażona nie tylko w dowolnym języku, lecz także za pomocą dowolnego kodu, np. kodu genetycznego, kodu impulsów elektronicznych, kodu impulsów nerwowych, kodu hormonów itd. To ujęcie informacji umożliwia potraktowanie jako jej nadawcy i odbiorcy zarówno człowieka, jak i organizmów żywych, ich organów, a także maszyn i organizacji[7].

Dla analizy bezpieczeństwa informacji podjętej w tym opracowaniu ważna jest także ilościowa teoria informacji Shannona (1948), która zakłada, że cechą informacji jest zmniejszanie entropii (niepewności, niewiedzy) odbiorcy. Shannon nie definiuje samej informacji, a jedynie jej ilość, utożsamia informację z danymi. Natomiast Langefors (1973) rozróżnia informację od danych i zwraca uwagę na uwzględnienie wymagań użytkowników informacji. Uważa, że informacja może jedynie powstać w umyśle człowieka jako proces interpretacji danych. Opracował tzw. równanie infologiczne, wyrażające się wzorem:

$$I = i\,(D,S,t)$$ gdzie:

I – informacja, i – proces interpretacji, D – dane, S – przedwiedza, t – czas

Według podanego wzoru informację należy definiować jako „proces interpretacji danych w oparciu o posiadaną wiedzę a priori w czasie". Informacja ma subiektywny charakter, co oznacza, że z określonych danych różni ludzie mogą odczytać różne informacje[8].

W dzisiejszych czasach coraz bardziej jesteśmy zależni od rozwoju techniki i informacji. Informacja stała się walutą (posiada swoją wartość), przynosząc korzyści temu, kto jest w jej posiadaniu. Informacja, posiadając swoją wartość, zachęca człowieka do tego, aby nie zawsze wykorzystywał ją zgodnie

---

6 M. Kłodawski, *Pojęcie informacji w naukach teoretycznoprawnych*, w: Z.E. Zieliński (red.), *Rola informatyki w naukach ekonomicznych i społecznych. Innowacje i implikacje interdyscyplinarne*, „Portal Innowacyjnego Transferu Wiedzy w Nauce" 2012, t. 2, Wydawnictwo Wyższej Szkoły Handlowej Kielce, s. 379-390.

7 J. Wróblewski (red.), *Wstęp do informatyki prawniczej*, Państwowe Wydawnictwo Naukowe, Warszawa 1985, s. 6.

8 M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie", 2009, nr 798, s. 99-116.

z przeznaczeniem. Przestępcy internetowi wykorzystując słabe zabezpieczenia, brak przestrzegania ustalonych zasad bezpieczeństwa przez użytkowników, a czasem naiwność czy zwykłą głupotę, kradną nasze dane, pieniądze i różne informacje, które mogą sprzedać lub wykorzystać do własnych potrzeb.

W Polsce Ustawa o Krajowym Systemie Cyberbezpieczeństwa określiła sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy zdefiniowanych w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. W ustawie określono obowiązki operatorów usług kluczowych, zasady wdrożenia systemu zarządzania bezpieczeństwem w systemach informacyjnych. Dla przykładu poprzez świadczenie usługi kluczowej możemy zapewnić w systemie informacyjnym:

- prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzania tym ryzykiem;
- wdrażanie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych;
- zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatności do sprawnego wdrożenia i użytkowania nowych rozwiązań informatycznych. Takie działanie skutkować powinno pozyskaniem wysoko kwalifikowanego personelu, który zapewni bezpieczeństwo systemów informacyjnych.

Zasadniczym celem pracy jest przeanalizowanie i usystematyzowanie zagrożeń związanych z cyberterroryzmem i przestępczością komputerową oraz ustalenie jakie rozwiązania (metody) należy zastosować w celu ochrony przed tymi zagrożeniami.

W pracy założono następującą **hipotezę roboczą:** Cyberterroryzm i przestępczość komputerowa stanowią zagrożenie dla państw, organizacji i instytucji oraz firm, a tym samym i obywateli. Zagrożenia te można identyfikować i poszukiwać nowoczesnych, skutecznych rozwiązań (biometria i kryptografia) dla zapewnienia odpowiedniego poziomu bezpieczeństwa informacyjnego (informatycznego). Istniejące akty prawne w Polsce zapewniają odpowiedni poziom bezpieczeństwa informacyjnego, a instytucje odpowiedzialne za jego utrzymanie powinny realizować zawarte w nich ustalenia.

W pracy przeprowadzono **analizę** zagrożeń związanych z cyberterroryzmem i przestępczością komputerową. Dokonano **analizy** dostępnych rozwiązań z biometrii i kryptografii oraz roli i zadań administratora systemu informatycznego. Założono, że zastosowanie tych rozwiązań może zapewnić skuteczną walkę

z zagrożeniami i zabezpieczyć organizacje, instytucje i firmy oraz użytkowników przed kłopotami i stratami finansowymi.

Drugą metodą badawczą zastosowaną w pracy jest **synteza**. Metoda ta pozwoliła opracować wnioski generalizujące dotyczące zagrożeń z jednoczesnym wskazaniem dostępnych na rynku rozwiązań, które mogą zapewnić bezpieczne korzystanie z systemów informacyjnych. W pracy przeanalizowano także akty prawne i rozwiązania pozwalające zapewnić odpowiedni poziom bezpieczeństwa informacyjnego.

Praca, w której przeprowadzono analizę zagrożeń cyberterrorystycznych i przestępczości komputerowej oraz zaproponowano wykorzystanie nowoczesnych rozwiązań zapewniających bezpieczeństwo informacji, składa się ze wstępu, siedmiu rozdziałów i zakończenia.

We wstępie dokonano wprowadzenia do tematyki pracy, ustalono cel pracy, hipotezę roboczą oraz przedstawiono metody badawcze (analizę i syntezę).

Pierwszy rozdział wprowadza zagadnienia bezpieczeństwa na płaszczyźnie informacyjnej. Przedstawia strategie, źródła i rodzaje informacji strategicznych oraz opisuje koncepcje systemu informatycznego jako istotnego ogniwa strategii organizacji. W rozdziale tym zwrócono uwagę na rosnącą rol**ę** bezpieczeństwa informacyjnego w państwie w podmiotach gospodarczych oraz wśród obywateli. Opisano kształtowanie i zarządzanie oceną bezpieczeństwa informacyjnego.

W drugim rozdziale przedstawiono sposoby pozyskiwania informacji jako elementów wojny elektronicznej. Analizie poddano mechanizmy wojny informacyjnej, cyberterroryzmu i przestępczości komputerowej oraz ustalono jak kształtuje się polityka bezpieczeństwa informacji.

W rozdziale trzecim dokonano charakterystyki cyberterroryzmu i przestępczości komputerowej jako zagrożenia bezpieczeństwa.

W rozdziale czwartym zaprezentowano współczesne zagrożenia cybernetyczne i ustalono co stanowi teleinformatyczne rezerwy (zasoby) strategiczne państwa polskiego. Dokonano charakterystyki potencjału teleinformatycznego ze szczególnym opisem sieci komputerowych, systemów, sprzętu i oprogramowania oraz specjalistów i firm, które stanowią potencjał infrastruktury krytycznej**.** Ponadto przedstawiono wykorzystanie potencjału teleinformatycznego organizacji i instytucji odpowiedzialnych za zapewnienie bezpieczeństwa do przeciwdziałania cyberterroryzmowi i przestępczości komputerowej, W końcowej części tego rozdziału analizowano bezpieczeństwo teleinformatyczne Polski w systemie UE i NATO.

W rozdziale piątym dokonano analizy biometrii jako metody identyfikacji niepowtarzalnych cech człowieka i wskazano obszary i wybrane rozwiązania, które można wykorzystać do zapewnienia bezpieczeństwa informacyjnego.

W kolejnym rozdziale analizie poddano kryptografię. Przedstawiono historyczne przykłady, w których kryptografia miała znaczący wpływ na bezpieczeństwo informacji, a przez to znaczący wpływ na losy konfliktów zbrojnych. Szczegółowa analiza pokazuje, że również w obecnych czasach znajduje zastosowanie w wielu dziedzinach, zapewniając bezpieczeństwo informacyjne.

Rozdział siódmy omawia rolę i zadania administratora systemu informatycznego i jego wpływ na bezpieczeństwo informacji.

W zakończeniu podsumowano przeprowadzone badania, ustalono, czy cel pracy został osiągnięty i, wykorzystując metodę badawczą syntezę, zdefiniowano wnioski generalizujące.

Szybki rozwój technologii informacyjnych (informatycznych) przynosi nieograniczony dostęp do wielu informacji, a przez to do szeregu udogodnień. Wraz z rozwojem nowoczesnych technologii informacyjnych nastąpił wzrost cyberterroryzmu i przestępczości komputerowej. Opracowanie to jest próbą, w której dokonano analizy korzyści, jak i strat, jakie niesie ze sobą rozwój nowoczesnych technologii informacyjnych. Autor ma świadomość, że nie wszystko udało się zidentyfikować, tym samym poddać analizie i opisać, ponieważ różne zagrożenia powstają niemal codziennie. Te zagrożenia cyberterrorystyczne i związane z przestępczością komputerową czekają na dalsze badania i analizy, być może w następnej publikacji.

The value of information is appreciated by those who lost (revealed) it.

INTRODUCTION

History of information, its collecting, processing and distributing probably dates back to the beginnings of homo sapiens. Probably, as nobody can reliably deny or confirm that thesis[9]. From the 19th to 20th century people passed information writing letters, with Morse alphabet or by the radio. It not a surprising that the crucial element of every community, not only human but also animals is communication (information dissemination). The group of people without communication in that form or another cannot be defined as a community but only a loose gathering. Community is created by collaboration and cooperations which involve communication. The announcement can have various forms and affect various senses. The group of people who create a community requires variety of forms of information dissemination.

Collecting and disseminating information have been known for ages. The term information (Lat. Informatio) - notion, explanation, announcement is generally not defined because of its basic, primary nature and is analyzed in terms of:

- Syntax (amount of information potentially included in a message), information is defined by quantity (amount) of information or as a synonym of data.
- Semantics (meaning and content of a message)
- Pragmatics (usefulness of information, i.e., value of information included in a message, measured by the aim of a recipient)[10].

[9] https://www.komputerswiat.pl/recenzje/sprzet/komponenty-pc/zarys-historii-nosnikow-informacji-czesc-pierwsza-wczoraj/w4peyq2 [dostęp: 27.03.2024].

[10] Keyword ,,Informacja", Encyklopedia PWN: źródło wiarygodnej i rzetelnej wiedzy, https://www.bing.com/search?q=informacja&form=ANSPH1&refig=792f d7d423674e-7e9be7cb9d9936f537&pc=U531 [accessed: 05.01.2023].

Literature provides variety of definitions. Information is differently defined in humanities, biology, mathematics, technical science or economics. Jacek Janowski notices that it is impossible to define information on the general scientific level and suggests three methods of using the term:

- **Descriptive approach** – using the term "information" by indicating its characteristics and functions;
- **Intuitive approach** – information is considered as not define term, understood intuitively and allows to elaborate more complex definitions.
- **Systemic approach** – using term "information" referring to already existing definitions in the specific scientific field and situation.

All these methods are applied in the studies on information. Generally applied models of how the information is considered, are divided into objective and subjective (cognitive) ones[11]. This division builds on the previously discussed syntactic, semantic and pragmatic aspects of information. Subjective perceptions of information in more often applied in humanities, biology, economics and law. Whereas an objective perception is typical of science which defines the information by its structural and physical parameters[12].

For this analysis referring to cybernetic definition of information seems to be useful, as it, in Maciej Kłodawski opinion[13], gives the wider perspective: Information does not mean only a description but also orders, bans, instructions, directives. For its form, information can be expressed not only in any languages but also with any code, e.g.: genetic code, electromagnetic impulse code, electronic code, neural impulse code, hormone code, etc. In this approach to information, its sender and its receiver can be human, living organism, their organs, machines and organizations"[14].

For the analysis of information security conducted in this book, Claude Shannon's information theory (1948) is crucial, as it assumes that the basic

[11] M. Barański, *Informacja w ujęciu prawnym przez pryzmat zagadnień terminologicznych*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2017, s. 19-24.

[12] J. Janowski, *Technologia informacyjna dla prawników i administratywistów. Szanse i zagrożenia elektronicznego przetwarzania danych w obrocie prawnym i działaniu administracji,* Wyd. Difin, Warszawa 2009.

[13] P. Przybyłowicz, *Wstęp do teorii informacji i kodowania*, https://www.scribd.com/document/49766365/wstep-do-teorii-informacji [accessed: 10.02.2023].

[14] M. Kłodawski, *Pojęcie informacji w naukach teoretycznoprawnych*, w: Z.E. Zieliński (red.), *Rola informatyki w naukach ekonomicznych i społecznych. Innowacje i implikacje interdyscyplinarne*, „Portal Innowacyjnego Transferu Wiedzy w Nauce", 2012, t. 2, Wydawnictwo Wyższej Szkoły Handlowej Kielce, s. 379-390.

function of information is minimizing a receiver's entropy (uncertainty, ignorance). Shannon does not define information itself, only its quantity and equates it with data. Whereas Börje Langefors (1973) differentiates information and data and emphasizes needs of information users. He claims that information can be created only in human's mind as a process of data interpretation and elaborated the infological equation:

$$I = I\,(D, S, t)$$

Where: I – information, I – interpretation, D- data, S- prior knowledge, t- time.

According to this equation information should be defined as "a process of data interpretation based on the previously gained knowledge in a specific time"[15].

Nowadays societies depend more and more on technology and information development. Information has become an asset (it has its value) benefits its owner. Information which is valuable encourages a human to use it not with its intended purpose. Cyber criminals prey on weak protection, braking defined security procedures by users and sometimes users' gullibility or ignorance. They steal data, money and various information which they can sell or use for their private purposes.

In Poland *Law on National Cyber-Defense System* defines the way how to supervise and control implementation and execution of regulations of Cybersecurity Strategy of The Republic of Poland. This law specifies the responsibilities of key services operators, procedures for implementation of security system management in information systems, e.g.: providing key service ensures:

- Regular risk assessment of incidents and risk management;
- Implementing technical and organizational measures proportionate to assessed risk;
- Collecting information about cyber threats and vulnerabilities to implement and use new, effective IT solutions. This should consequently initiate recruiting the highly qualified personnel for securing information systems.

The main aim of this book is to analyze the literature, provide deeper insight into threats of cyberterrorism, cybercrime and identify what solutions (methods) can be used to protection information against them.

[15] J. Wróblewski J., *Wstęp do informatyki prawniczej*, Państwowe Wydawnictwo Naukowe, Warszawa 1985, s. 6.

The working hypothesis is: Cyberterrorism and cybercrime pose a threat to states, organizations, institutions, companies and citizens. These threats can be identified and new, effective solutions (biometrics, cryptography) can be adopted to provide the expected level of information and computer security. The existing legal acts in Poland support the expected level of information security and the institutions responsible for information security should implement them.

The book includes the analysis of cyberterrorism and cybercrimes, the latest biometric methods, cryptographic techniques and tasks of administrators in the field of information systems security. It is assumed that the analyzed solutions can fight the frets effectively and protect organizations, institutions, companies and users against troubles and financial loss. The book includes also the analysis of the legal acts and regulations for ensuring an adequate level of information systems security. The second method used in the research is synthesis to elaborate general conclusions about threats and indicating available solutions which ensure the secure information systems exploitation.

The effect of research ordered in introduction, seven chapters and conclusion. Introduction presents the problem, aim of the research, working hypothesis and research methods.

The first chapter introduces problem of information security, strategies, sources and kinds of strategic information as well as the conception of the information system as the crucial element of the organizational strategy. It draws attention to a growing role of information security for a state, business entities and citizens. The chapter describes how information security is shaped and managed.

The second chapter presents the ways of information acquisition as elements of electronic warfare. The information warfare, cyberterrorism and cybercrime are characterized and analyzed as well as information security policy is discussed.

The third chapter characterizes cyberterrorism and cybercrimes as a security threats.

The fourth chapter discusses contemporary cyberthreats and identifies the strategic tele-informatics reserves (assets) of Poland. The characteristic of tele-informatics capacity includes the detailed description of computer networks, systems, equipment and software as well as experts and companies who are the part of a critical infrastructure capacity. Moreover, it presents how the tele-informatics capacity of organization and institutions responsible for security, is exploited to

prevent cyberterrorism and cybercrime. The end of the chapter includes the analysis of ICT security of Poland in the UE and NATO systems.

The fifth chapter analyzes biometrics as a method of identification of the unique features of a person and indicates the areas and selected solutions for providing information security.

The next, sixth chapter analyzes cryptography, presents historical examples when the cryptography play the significant role in information security and consequently in military conflicts. It proves that also in present times cryptography is applied in many areas for information security.

The seventh chapter presents the role and tasks of administrator of an information system, their influence of information security.

In conclusion the summary of the research proves that the aim has been achieved. The general findings were formulated with synthesis as a method.

The rapid development of information (computer) technologies gives the unlimited access to information and also conveniences. Along the development of new ICT technologies, the cyberterrorism and cybercrime has been growing. The book is an attempt of the benefits and losses analysis of ICT development. The Author is aware that it was impossible to identify, analyze and describe all problems as new threats are being created almost every day. They are to be analyzed in the next research.

1. BEZPIECZEŃSTWO NA PŁASZCZYŹNIE INFORMACYJNEJ

1.1. Od danych do informacji – z teorii problemu. Informacja a społeczeństwo

„… by zachować posiadaną tajemnicę nie wystarczy samo milczenie”.
Paul Claudel

Komunikacja jest jednym z najstarszych procesów społecznych, towarzyszącym człowiekowi od chwili, gdy zaczął żyć w grupach. Przykłady z historii: Wielki Mur Chiński jest jednym z najznakomitszych i najbardziej morderczych dokonań budowlanych wszechczasów. Jego budowa została rozpoczęta po roku 220 p.n.e. i trwała około 10 lat, a jej pomysłodawcą był pierwszy władca zjednoczonych Chin – okrutny despota, założyciel dynastii Cin, Szy Huang-ti (Czeng). Mur wił się, wznosząc i opadając, wśród gór, pustkowi i moczarów. Zbudowano go na kamiennych fundamentach, z ziemi pokrytej cegłą. Sygnały dymne, a w nocy ogniska, pozwalały z niesamowitą szybkością przesyłać informacje z wież strażniczych przez cały kraj.

Do przesyłania wiadomości w starożytnej Persji i Egipcie zastosowano gołębie pocztowe. W Grecji wykorzystywano je najczęściej do przekazywania wiadomości o zwycięzcach Olimpiad. W XII wieku muzułmanie w wojnach z Królestwem Jerozolimskim używali ich do wzywania pomocy. Gołębie te powszechnie wykorzystywano w czasie I wojny światowej.

Już wiele lat temu Sun Tzu stwierdził, że wojna to sztuka wprowadzania przeciwnika w błąd. Niewiele zmieniło się przez wieki. Dlatego równie aktualne

jest stwierdzenie, że pierwszą ofiarą wojny pada prawda. Gdy rozpoczynają się wojny gospodarcze strony usiłują dezinformować przeciwnika. Każda stosuje różne fortele i pozoracje, które mają zmylić przeciwnika, przerzucają się też oskarżeniami o spowodowanie strat własnych i korzyściach strony przeciwnej. Na końcu okazuje się zawsze, że wszyscy kłamali, tyle że zwycięzcy – jak często sami twierdzą – nie podlegają osądzeniu.

Istnienie społeczeństwa polega na komunikowaniu się (wymianie informacji między ludźmi) oraz na przekazywaniu dziedzictwa kulturowego z pokolenia na pokolenie. Bezpośrednim celem komunikowania się zbiorowego jest doinformowanie i dowartościowanie członków grupy na zasadzie pełnego partnerstwa w nadziei, że przyczyni się ono do stwarzania klimatu wzajemnego zaufania i zrozumienia między nadawcą a odbiorcami informacji. Dzięki temu osiągniemy lepszą motywację i pozytywne zachowania każdego na rzecz całej grupy[16].

Przeprowadzona analiza wskazuje, że na przełomie wieków występowały różne formy komunikowania się. Komunikacja (z łac. *communicatio*) to: wymiana, łączność, rozmowa. Możemy tutaj wyróżnić następujące rodzaje komunikacji międzyludzkiej:

- **komunikacja interpersonalna:**
  - ✓ bezpośrednia („twarzą w twarz”);
  - ✓ pośrednia (telefon, SMS, faks, list, Internet).
- **komunikacja zbiorowa (społeczna):**
  - ✓ bezpośrednia (wykład, dyskusja, lekcja, kazanie, obrzędy, uroczystości, spektakl teatralny);
  - ✓ pośrednia (masowe środki przekazu: prasa, radio, TV, płyty, książki, Internet: grupy dyskusyjne, portale społecznościowe, e-learning).

O formach tych obecnie możemy powiedzieć, że były bardzo niedoskonałe, a ich najbardziej charakterystyczną cechę stanowiło to, że docierały do odbiorców wolno i w ograniczonym zasięgu. Do zasadniczych sposobów komunikacji zaliczamy w[17]:

- gesty, miny, obrazy;
- sygnały dźwiękowe (tam-tamy, gwizdki, tuby, trąbki);
- sygnały dymne;
- gołębie pocztowe;

[16] H. Bieniok, *Sztuka komunikowania się, negocjacji i rozwiązywania konfliktów,* AE, Katowice 2005, s. 12.

[17] https://mfiles.pl/pl/index.php/Warunki_efektywnej_komunikacji [dostęp: 27.03.2024].

- rozmowy, konwersacje, dyskusje;
- listy, teksty (książka, gazeta, broszura, ulotka, folder reklamowy, wizytówka);
- telegraf, faks, rozmowy telefoniczne;
- znaki wyryte w kamieniach, tablicach kamiennych czy metalach;
- znaki, np. drogowe;
- piktogramy;
- komunikacja internetowa (poczta e-mail, strona internetowa, komunikatory i in.).

Rozwój komunikacji międzyludzkiej obejmuje następujące okresy:

- era znaków i sygnałów wizualnych oraz dźwiękowych – od ok. 1,6 mln lat temu (*homo erectus*);
- **rozwój mowy artykułowanej** – ok. 100-35 tys. lat temu (*homo sapiens*);
- **znaki i rysunki naskalne** – ok. 60-30 tys. lat temu;
- **era pisma** – ok. 8-6 tys. lat temu (Chiny, dorzecze Eufratu i Tygrysu);
- **era druku i komunikacji masowej:**
  - od XV do XVIII wieku – drukarstwo rękodzielnicze, pojawienie się prasy;
  - od początku XVIII wieku – drukarstwo zmechanizowane;
  - od lat 30. XIX wieku – prasa masowa.
- **era telekomunikacji i informatyzacji:**
  - druga połowa XIX wieku: fotografia, telegraf, telefon, fonograf, film;
  - pierwsza połowa XX wieku: radio, gramofon elektryczny, kolorowa prasa, telewizja.
- **druga połowa XX wieku:**
  - telewizja satelitarna, kablowa, cyfrowa;
  - płyty CD, DVD, dyski twarde;
  - taśmy i kasety analogowe i cyfrowe;
  - komputery: strony www, książki elektroniczne, multimedia;
  - Internet: poczta elektroniczna, grupy dyskusyjne, nauczanie na odległość.

XXI wiek określany jest wiekiem społeczeństwa informacyjnego. W okresie tym wzrosło uzależnienie instytucji państwowych, komercyjnych, podmiotów gospodarczych a nawet jednostek od szybkiego, niezawodnego, a przede wszystkim bezpiecznego przetwarzania ogromnej ilości informacji[18]. Termin „społeczeń-

[18] Słowo „informacja" pochodzi od łacińskiego słowa *informatio* i może być używane w dwóch kontekstach – jako akt kształtowania umysłu i jako akt przekazywania wiedzy.

stwo informacyjne" pojawił się w latach sześćdziesiątych XX wieku w Japonii. Użył go po raz pierwszy w 1963 roku Tadeo Umesao[19] na oznaczenie gospodarki opartej na informacji i technologii informacyjnej. Powstały termin miał oznaczać typ społeczeństwa charakteryzującego się dominacją pracy w sferze usług, cyfrowej rewolucji, znacznego przepływu informacji, zastosowania i wykorzystaniu w różnych dziedzinach gospodarki mediów i usług teleinformatycznych. W 1973 roku D. Bella[20] sformułował podstawowe cechy społeczeństwa informacyjnego, do których zaliczył:

- **dominacja naukowców**, specjalistów w sferze zawodowej;
- **wzrost znaczenia wiedzy teoretycznej** jako źródła innowacji;
- **nastawienie na sterowany rozwój techniki**;
- **tworzenie nowych technologii** jako podstaw podejmowania decyzji politycznych i społecznych.

Znacznie szerzej do problemu społeczeństwa informacyjnego podszedł M. Castells[21]. W trzytomowym dziele zatytułowanym *The Information Age: Economy, society and culture* przedstawił koncepcję społeczeństwa sieciowego. Zauważył on, że źródłem współczesnych przemian są trzy niezależne od siebie procesy:

- **rewolucja informatyczna**;
- **rozwój kulturowych ruchów społecznych**;
- **kryzys gospodarczy kapitalizmu oraz radzieckiego socjalizmu**, a nie tylko intensywny rozwój narzędzi informatycznych.

[19] Jak podaje Wikipedia, termin ten został użyty przez T. Umesao w artykule *O teorii ewolucji społeczeństwa opartego na technologiach informatycznych*, https://pl.wikipedia.org/wiki/Daniel_Bell [dostęp: 2.04.2024].

[20] D. Bell, amerykański socjolog, jeden z twórców koncepcji społeczeństwa poprzemysłowego oraz „końca wieku ideologii", podano za: http://pl.wikipedia.org/wiki/Daniel_Bell [dostęp: 27.03.2024].

[21] M. Castells, socjolog hiszpański, bada kondycję człowieka i społeczeństwa w kontekście procesów usieciowienia życia społecznego. Problematyce zmiany społecznej wprowadzonej przez rewolucję technologiczną poświecił monumentalną trylogię *The Information Age: Economy, Society and Culture*, tom pierwszy *The Rise of the Network Society* (1996, uzupełniona 2000), tom drugi *The Power of Idenity* (1997), tom trzeci *End of Millennium* (1998, uzupełniona 2000). Trylogia została przetłumaczona na 12 języków, wzbudziła wiele dyskusji i stanowi źródło inspiracji dla naukowców, zainteresowanych zmianami zachodzącymi we współczesnym społeczeństwie globalnym. W 2001 napisał książkę popularyzującą idee zawarte w *The Information Age*, *Galaktykę Internetu*, której tytuł był nawiązaniem do dzieła Marshalla McLuhana *Galaktyka Gutenberga* (podano za http://pl.wikipedia.org/wiki/Manuel_Castells [dostęp: 10.02.2024].

Procesy te wpływają na powstanie nowego modelu społeczeństwa, którego podstawą jest sieć. W Europie inicjatywa budowy społeczeństwa informacyjnego należała do Rady Europy. Określenie społeczeństwa informacyjnego zostało spopularyzowane przez raport D. Bangemanna ***e-Europa i społeczeństwo globalnej informacji***[22], który określił społeczeństwo informacyjne jako rewolucję opartą na informacji oraz rozwoju technologicznym pozwalającym gromadzić, przetwarzać, przekazywać i odzyskiwać informacje w dowolnej formie, bez względu na odległość, czas, wielkość. W raporcie tym Bangemann zalecał, aby podstawą tworzenia społeczeństwa informacyjnego były finanse sektora publicznego i mechanizmy rynkowe, natomiast sektor publiczny powinien skupić się na regulacjach prawnych, ochronie obywateli i podnoszeniu świadomości społeczeństwa. Ponadto przedstawił 10 inicjatyw w celu rozwoju nowoczesnych technik teleinformacyjnych w zakresie:

- szkoleń na odległość (e-learningu);
- sieci teleinformatycznych;
- jednostek badawczych;
- telepracy;
- zapewnienia powszechnego dostępu do usług teleinformatycznych;
- dostępu do usług dla małych i średnich przedsiębiorstw;
- kontroli ruchu lotniczego;
- sieci na użytek sektora zdrowia;
- komputeryzacji sektora zamówień publicznych;
- transeuropejskiej sieci administracji publicznej;
- infostrad dla obszarów miejskich;
- ochrony prywatności i bezpiecznego przepływu informacji[23].

W drugiej połowie XX wieku pojawiły się środki masowej komunikacji (media), które docierały niemal wszędzie. Było to możliwe dzięki rozwojowi techniki. To niezwykle ułatwiło komunikację społeczną, poszerzyło społeczności, powiększyło liczbę spełnianych społecznie zadań i przyspieszyło sam obieg informacji. Równocześnie jednak te udogodnienia i skuteczność komunikacyjna stały się pokusą do sterowania ludźmi w skali dotąd niespotykanej. **Komunikacja**

[22] D. Bangemann, *e-Europa i społeczeństwo globalnej informacji,* http://www.silesia.org.pl/upload/Nowak_Jerzy__Spoleczenstwo_informacyjnegeneza__i_definicje. pdf [dostęp: 10.01.2023].

[23] https://www.bing.com/search?q=10+inicjatyw+w+celu+rozwoju+nowoczesnych+technik+teleinformacyjnych+w+zakresie%3A+&form=ANSPH1&refig=1A43EA29F02C44B9AC243173D4AC582A&pc=U531 [dostęp: 10.02.2024].

oznacza pobieranie, gromadzenie, przesyłanie, przetwarzanie danych i informacji, może następować przez[24]:

- porozumiewanie się pracowników;
- współdziałanie pracownik – kierownik – dyrektor;
- współpracę między kierownikami niższych szczebli a kierownictwem firmy;
- współpracę człowiek – komputer – system przetwarzania danych;
- współpracę pracowników w sieciach komputerowych;
- aktywne kreowanie danych, informacji i przestrzeganie poufności danych i tajemnicy obowiązującej w firmie;
- komunikowanie się kierowników z doradcami i ekspertami;
- korzystanie przez pracowników z baz danych, banków informacji, Internetu;
- stosowanie w komunikacji nowych środków łączności: pagery, telefony, faxy, e-mail, telefony komórkowe, urządzenia kopiujące;
- stale rozwijaną umiejętność obsługi komputerów osobistych i programów służących zarządzaniu przedsięwzięciami inwestycyjnymi (np. MS Projekt, CIS, CIM).

Media jako środki masowego przekazu oddziaływają na człowieka, który odbiera je zazwyczaj indywidualnie, gdyż słucha ich lub ogląda komunikaty w domu. Ponieważ jednak odbiera je indywidualnie, nie widzi masowej reakcji innych ludzi. Świadomość tego faktu dała niesłychaną przewagę tym, którzy zajmują się mediami, ponieważ planują oni reakcję masową, a odbiorca nie widzi, że jest częścią masy: odbiera indywidualnie – reaguje masowo. W ten sposób utworzyło się pole możliwości niewidzialnego sterowania ludźmi w skali masowej.

Informacja (łac. *informatio* – wyobrażenie, pojęcie) to pojęcie definiowane w różnych dziedzinach. Zasadniczo informację postrzega się na dwa sposoby.

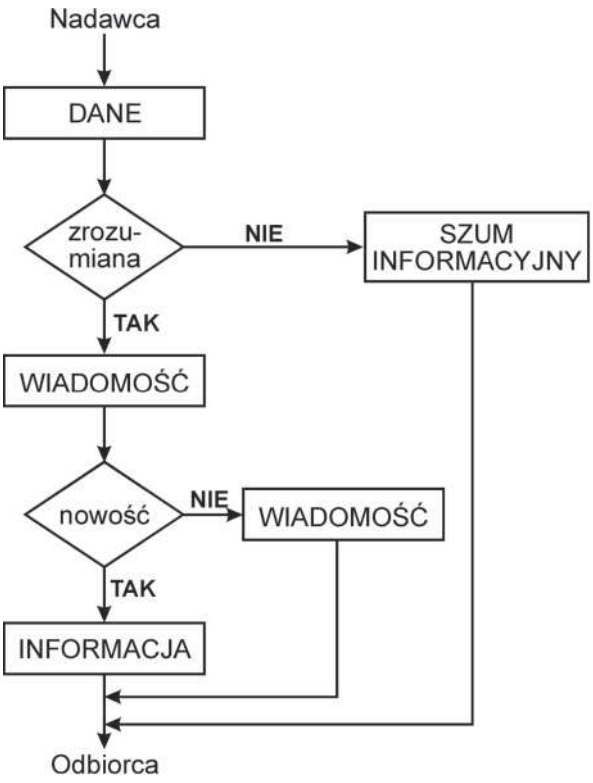
Pierwszy można nazwać *obiektywnym*. Wywodzi się z fizyki i matematyki, w których informacja oznacza pewną własność fizyczną lub strukturalną obiektów.

Zgodnie z drugim, *subiektywnym* (kognitywistycznym), informacją jest to, co umysł jest w stanie przetworzyć i wykorzystać do własnych celów.

Informacja określana jest tym, co zmienia i wspomaga zrozumienie, natomiast dane stanowią wejście kanału komunikacji. Dane są materialne i składają się z numerów, słów, rozmów telefonicznych lub wydruków komputerowych

[24] W.M. Grudzewski, I. K. Hejduk, *Zarządzanie wiedzą w przedsiębiorstwach,* Difin, Warszawa 2004 , s. 143.

wysłanych lub otrzymanych. Dane nie staną się informacją dopóki ludzie nie wykorzystają ich do poprawy swojego zrozumienia.



Rys. 1. Dane, wiadomości, informacje

Źródło: http://www.uci.agh.edu.pl/uczelnia/tad/PSI11/art/Dane_informacje_wiedza.pdf [dostęp: 12.12.2022].

Informacje w organizacji stanowią podstawę budowania wiedzy wszystkich osób zaangażowanych w proces jej pozyskiwania i wykorzystywania. Kształtują świadomość o zjawiskach zachodzących w samym przedsiębiorstwie, firmie czy instytucji oraz ich otoczeniu. Pozwalają na dostosowywanie do zmieniającej się rzeczywistości i umożliwiają przekształcanie tej rzeczywistości w celu sprawnego funkcjonowania. Dzięki informacjom organizacja, instytucja, przedsiębiorstwo czy firma może uzmysłowić sobie istniejące problemy i szukać ich rozwiązania.

Pojęcia danych, informacji i wiedzy należą do terminów trudno definiowalnych z uwagi na swój pierwotny charakter. W języku potocznym używamy

ich zamiennie, często stosownie do obowiązującej mody. W sposób szczególny zajmują się nimi dwie dziedziny: zarządzanie wiedzą i teoria informacji. W zależności od wymienionej dziedziny hierarchia pojęć poznawczych nosi nazwę piramidy lub hierarchii wiedzy lub ewentualnie piramidy lub hierarchii informacji. Można również spotkać się z terminem DIKW (skrót pochodzący od pierwszych słów poszczególnych składowych[25]):

- *Data* (dane);
- *Information* (informacja);
- *Knowledge* (wiedza);
- *Wisdom* (mądrość).

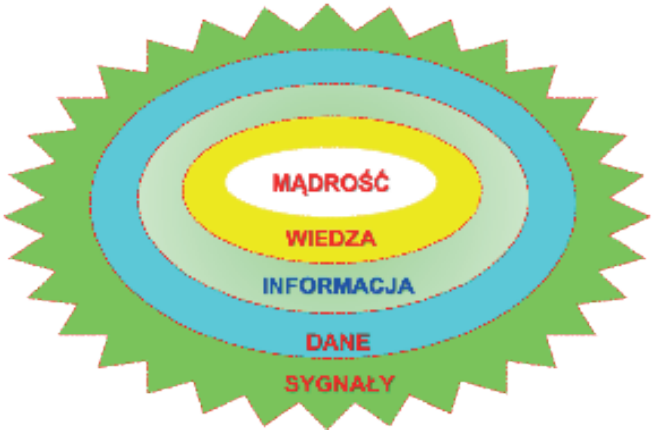
Omówienia istoty informacji jako pierwszy podjął się Claude Elwood Shannon (1948). Rozważania Shannona dotyczyły zagadnień transmisji sygnału przez kanał informacyjny, z uwzględnieniem szumu informacyjnego, stochastycznego charakteru procesu oraz cech odbiorcy komunikatu. Badacz uważa, że ilościowa teoria informacji jest w zasadzie teorią komunikacji. Shannon zainspirowany pojęciem entropii, zaczerpniętym z termodynamiki, uważa, że cechą informacji jest zmniejszanie entropii (niepewności, niewiedzy) odbiorcy.

Rozpatrując rolę i znaczenie informacji dla odbiorcy należy stwierdzić, że istotnym czynnikiem jest jej jakość, która wynika z takich cech, jak:

- **celowość** – informacja musi komuś i czemuś służyć, musi istnieć racjonalna przesłanka, gromadzenia i wykorzystywania informacji;
- **rzetelność** – dotyczy prawdziwości zarówno źródła informacji, jak i jej zawartości;
- **aktualność** – informacja musi dotyczyć okresu decyzyjnego i być dostarczona w odpowiednim czasie;
- **kompletność** – informacja nie może być wyrywkowa, musi uwzględniać kontekst decyzyjny;
- **wszechstronność** – powinna przedstawiać sytuację decyzyjną z wielu różnych punktów widzenia;
- **odpowiednia dokładność** – informacja nie za szczegółowa i nie za ogólna;
- **uzasadnione nakłady finansowe** – wykorzystanie informacji musi przynosić korzyści przynajmniej pokrywające nakłady poniesione na jej zdobycie[26].

[25] https://mfiles.pl/pl/index.php/Dane [dostęp: 02.02.2024].
[26] https://czakalaka.pl/informacja-definicja-charakterystyka-rodzaje/[dostęp: 10.01.2023].

Informacja stanowi jeden z najważniejszych elementów podejmowania decyzji. Z kolei **informacja i wiedza** są obecnie uważane za nowy towar na rynku, podobny do dóbr materialnych czy energii. Równocześnie, ze względu na Internet i inne nowoczesne środki przekazu informacji, społeczeństwo nazywane jest często społeczeństwem informacyjnym (ang. *Information Society*). Tak zastosowane pojęcie informacji dotyczy również wiedzy faktycznej lub domniemanej, a także reguł preferencji w różnych dziedzinach ważności i użyteczności. W tym sensie, *informując* kogoś o kimś lub czymś, zawiadamiamy go o faktach lub dzielimy się naszą wiedzą albo preferencjami na dany temat. **Informacja** jest przekazywana przez ludzi, może być także zdobywana samodzielnie przez studiowanie, naukę, poszukiwanie w zasobach bibliotecznych (tradycyjnych i informatycznych). Zdobywanie, posiadanie i wykorzystanie informacji następuje zarówno w sposób świadomy, jak i podświadomie. Dlatego do podstawowych pojęć w obszarze informacji można zaliczyć sygnały, dane, informacje, wiedzę oraz mądrość.



Rys. 2. Zakres i powiązania pojęć: sygnały, dane, informacje, wiedza, mądrość

Źródło: oprac. na podst. R. Szpyra, *Militarne operacje informacyjn*e, AON, Warszawa 2003, s. 72.

- **sygnały** – niosą informacje o naturze badanych zjawisk lub systemów. Sygnał oznacza przepływ strumienia informacji, przy czym przepływ może odbywać się w jednym lub w wielu wymiarach;
- **dane** – uporządkowany zbiór nazw, wartości i informacji opisujących określony obiekt (system, proces, zdarzenie);
- **informacje** – zbiór uporządkowanych danych zgodnie z potrzebami odbiorcy (użytkownika), określający jego potencjalne (lub realne) działanie;

- **wiedza** – zbiór informacji wykorzystywanych przez użytkownika w procesie działania;
- **mądrość** – wiedza, dzięki której podmiot (użytkownik) realizuje określone cele, uwzględniając przyjęty system wartości[27].

Informacje możemy klasyfikować również przyjmując inne kryteria, takie jak: dziedzinę wiedzy, rodzaj i stopień przetworzenia, sposób gromadzenia, przechowywania i dystrybucji, częstotliwość wykorzystywania oraz szereg innych czynników.

System informacyjny – posiadająca wiele poziomów struktura pozwalająca użytkownikowi na przetwarzanie, za pomocą procedur i modeli, informacji wejściowych w wyjściowe. Natomiast **system informatyczny** jest wydzieloną, skomputeryzowaną częścią systemu informacyjnego[28]. Nowe technologie wspierające systemy informacyjne są coraz powszechniejszym sposobem zwiększenia sprawności działania systemu zarządzania, ponieważ mimo początkowych wydatków na szkolenia, oprogramowanie i wdrożenie, system informatyczny umożliwia formalizację struktury organizacyjnej, zwiększenie rozpiętości kierowania, automatyzowanie zadań, dostarcza niezwłocznie żądanych informacji, ułatwia pracę grupową w przedsiębiorstwach posiadających wiele oddziałów[29].

W teorii zarządzania **system informacyjny** to zespół środków materialnych, finansowych, algorytmów i ludzi, zapewniający sprawne zarządzanie przedsiębiorstwem. Na gruncie ekonomiki informacji system informacyjny definiowany jest jako kompleks powiązanych ze sobą procesów informacyjnych. System informacyjny jest specyficznym systemem społeczno-gospodarczym, który, obok procesów informacyjnych, zawsze współtworzą także zasoby oraz informacja[30].

Podziału informacji możemy dokonać uwzględniając różne czynniki. W przypadku roli jaką pełnią w zarządzaniu organizacją informacje dzielimy na[31]:

---

[27] M. Wrzosek, *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, AON, Warszawa 2010, s. 24.

[28] J. Kisielnicki, H. *Sroka, Systemy informacyjne biznesu. Informatyka dla zarządzania*, Placet, Warszawa 2005, s. 18.

[29] N. Jabnoun, S. Sahraoui, *Enabling a TQM structure through information technology*, „Competitiveness Review" 2004, nr 1-2, American Society for Competitiveness, Pittsburg.

[30] J. Kuck, *Nowoczesność efektywność i bezpieczeństwo współczesnej logistyki*, AON, Warszawa 2014, s. 31.

[31] M. Strzoda, *Zarządzanie informacją w organizacji*, AON, Warszawa 2004, s. 26.

- **planistyczne** – inspirujące procesy decyzyjne oraz wykorzystywane do opracowania dokumentów planistycznych i dyrektywnych;
- **organizacyjne** – przyczyniające się do stworzenia struktury przyszłego działania;
- **kontrolne** – pozwalające na korektę realizowanych planów oraz dopasowanie ich do zmieniających się warunków otoczenia i organizacji;
- **koordynacyjne** – pozwalające na realizacj**ę** i dopasowanie działania poszczególnych elementów organizacji.

Do prawidłowego zarządzania organizacją można zdefiniować także podstawowe grupy informacji, często określane mianem informacji biznesowych[32]:

- **pokrzepiające** – dotyczące bieżącej sytuacji w organizacji, których celem jest zapewnienie, że wszystko przebiega zgodnie z przyjętymi założeniami;
- **rozwojowe** – związane z oceną stanu lub przebiegu jakiegoś zjawiska lub procesu oraz wykazaniem ewentualnych trudności związanych z jego realizacją;
- **ostrzegawcze –** sygnalizują, iż wystąpiły określone zagrożenia w wyniku realizacji działalności organizacji lub też, że mogą one w najbliższym okresie wystąpić;
- **planistyczne** – odnoszące się do poziomu lub stanu przyszłego zjawiska lub procesów gospodarczych (biznesowych);
- **operacyjne** – określają działanie własnej organizacji i pozwalają na jej umiejscowienie na „mapie" działalności innych podobnych organizacji;
- **opiniodawcze** – dotyczą informacji o najbliższym oraz dalszym otoczeniu organizacji;
- **kontrolne –** mają być przekazane otoczeniu (bankom, mediom, itp.) o działalności organizacji.

Informacje mogą być pozyskiwane z różnych źródeł, w tym z zasobów informacyjnych dostępnych w otoczeniu. Zakres i powiązania pojęć obejmujących sygnały, dane, informacje, wiedzę i mądrość przedstawiono na rys 1.

Informacja może też być określana za pomocą takich mierników jak **ilość, jakość** oraz **wartość.** Stanowi zbiór wielkości opisujących obiekty dowolnej natury, zawarty w określonej wiadomości i wyrażony w takiej formie, że pozwala określonemu obiektowi, do którego one dotarły, ustosunkować się do zaistniałej

[32] Tamże, s. 26 – 27.

dzięki temu sytuacji i podjąć odpowiednie działania. Powyższe stwierdzenie pozwala na wskazanie, że[33]:

- **informacje dotyczą obiektów dowolnej natury** – realnych (rzeczy, zdarzenia, fakty) i abstrakcyjnych (także wirtualnych), organicznych (biologicznych) i nieorganicznych (fizycznych), żywych i sztucznych, itp.;
- **informacje wyrażają w określony sposób cechy** (własności, właściwości, stany) obiektu, których uzyskanie przez inny obiekt może zmienić jego sytuację;
- **obiekt odbierający informację może być dowolnej miary**, lecz siłą rzeczy rozumiemy go jako osobę lub grupę osób – społeczny aspekt pozwala na lepsze wyrażenie jej istoty;
- **zmiana sytuacji obiektu uzyskującego informacje może oznaczać zmianę postawy** (dzięki zmniejszeniu nieokreśloności i niepewności będącej jego udziałem) i podjęcie działań umysłowych bądź fizycznych;
- **istotne znaczenie ma postać (forma informacji**), tak aby spełniała wymagania i oczekiwania odbiorcy;
- **informacje mogą różnić się także ze względu na przeznaczenie**, charakter fizyczny czy warunki metrologiczne.

W procesach decyzyjnych sprawne działanie zależy od wielu czynników. Jednym z istotnych jest informacja. Do sprawnej i efektywnej realizacji procesu decyzyjnego informacja może być[34]:

- **pozyskiwana** (zdobywana) i dotyczyć określonych obiektów;
- **przesyłana** pomiędzy co najmniej dwoma użytkownikami;
- **przechowywana** (magazynowana);
- **przetwarzana**;
- **udostępniana** (rozpowszechniana).

Proces informacyjny stanowi jeden z elementów decydujących o sprawności funkcjonowania każdej organizacji. Zasadniczym celem procesu informacyjnego jest zaspokojenie potrzeb informacyjnych określonych użytkowników. System informacyjny, w którym występuje informacja jako produkt związany jest z człowiekiem, posiada określoną strukturę i składa się z kilku części:

- **informacyjnej** – odpowiadającej na pytanie: jak? dlaczego? po co? o czym? kogo? i jak często informować?;

[33] P. Sienkiewicz, *Systemy kierowania*, PWWP, Warszawa 1989, s. 128.
[34] J. Kuck, *Nowoczesne technologie w logistyce*, AON, Warszawa 2013, s. 14.

- **przestrzennej** – określającej miejsca powstania informacji oraz ich przeznaczenia, czyli użytkowników końcowych;
- **technologicznej** – odpowiadającej na pytanie dotyczące sposobów, metod i technik stosowanych w zbieraniu, utrzymaniu, przetwarzaniu i transferze informacji;
- **technicznej** – określającej architekturę stosowanego sprzętu komputerowego;
- **organizacyjnej –** której celem jest zapewnienie spójności wszystkich wyżej wymienionych struktur[35].

Przedstawiona ogólna charakterystyka oraz znaczenie systemu informacyjnego pokazuje jego wpływ i oddziaływanie w procesie zmian związanych z przechodzeniem do nowej epoki rozwojowej (cywilizacji informacyjnej). Wzrost znaczenia informacji przynosi wymierne korzyści, jednocześnie powoduje nowe zagrożenia, które wcześniej nie występowały.

1.2. Strategia, źródła i rodzaje informacji strategicznych

Strategia w znaczeniu ogólnym oznacza naczelną orientację gospodarczą, społeczną, militarną, która wyraża dominujący kierunek działania danego systemu. Ta naczelna orientacja jest główną linią i zarazem wytyczną postępowania kierownictwa systemu w związku z sytuacjami, jakie zachodzą w otoczeniu i przy uwzględnieniu własnego potencjału kadrowego, organizacyjnego, finansowego i techniczno-produkcyjnego[36]. Strategia to ogólny plan działania. W przypadku potrzeby pozyskania informacji strategicznych należy:

- pomyśleć, jakie źródła informacji są dostępne i z których najlepiej skorzystać;
- wybrać najbardziej efektywne techniki wyszukiwania i pozyskiwania informacji.

W gospodarce opartej na wiedzy, zasobem zyskującym coraz to większe znaczenie, który jest wykorzystany w procesie zarządzania, jest informacja. W tym kontekście rzetelna, wyczerpująca informacja pozyskana w odpowiednim momencie prowadzi do przewagi konkurencyjnej w krajowym czy międzynarodowym środowisku. Dodatkowo informacja ma kluczowe znaczenie dla procesu zarządzania strategicznego. **Zarządzanie strategiczne** można przedstawić jako

[35] W. Flakiewicz, *Systemy informacyjne w zarządzaniu*, Wydawnictwo C.H. Beck, Warszawa 2002, s. 34.

[36] http://pl.wikipedia.org/wiki/Strategia_organizacji [dostęp: 27.03.2024].

proces złożony z etapów: analizy, planowania, zarządzania rozumianego jako etap realizacji opracowanej strategii. W sensie czynnościowym analiza strategiczna jest zbiorem działań diagnozujących organizację i jej otoczenie w zakresie umożliwiającym zbudowanie planu strategicznego i jego realizację[37].

Proces ten i towarzyszące mu analizy strategiczne wymagają wszechstronnego poznania funkcjonowania państwa, organizacji, firmy i ich otoczenia, a to pozwala na określenie sytuacji w stosunku do konkurentów oraz szans i zagrożeń wynikających z działalności na międzynarodowym rynku. Strategia powinna być zapisana w formie jednolitego dokumentu. Informacje o znaczeniu strategicznym dotyczą podstawowych kwestii wpływających na funkcjonowanie państwa. Są to informacje o:

- nowych produktach i technologiach na rynku;
- sytuacji gospodarczej;
- nowych kontraktach;
- zmianach w prawie;
- konkurentach;
- zmianach na rynku dostawców i podwykonawców;
- obecnych klientach;
- nowych sposobach finansowania;
- otoczeniu międzynarodowym.

System informacji strategicznej jest niezwykle ważnym czynnikiem w procesie pozyskiwania informacji i umożliwia łatwe ich wykorzystanie w trakcie podejmowania decyzji. W konsekwencji warunkuje to ich racjonalność wykorzystania i wpływa na efektywność całego procesu zarządzania strategicznego. W związku z tym, że większość podejmowanych decyzji strategicznych powtarza się w cyklach rocznych lub wieloletnich, uzasadnionym jest, by zasób informacji niezbędny do ich podejmowania nie był pozyskiwany w sposób jednorazowy. Racjonalnym jest, aby stanowił wewnętrznie spójny, stale odnawiany system, tworzony przez państwo na własne potrzeby. **Taki system nazywamy systemem informacji strategicznej – SIS**[38]. Zadaniem systemu jest pozyskiwanie, gromadzenie, przetwarzanie, kopiowanie, przechowywanie, ochrona i przekazywanie, przesyłanie (udostępnianie) informacji dla potrzeb powtarzalnych

[37] G. Gierszewska, M. Romanowska, *Analiza strategiczna przedsiębiorstwa*, PWE, Warszawa 1994, s. 13.

[38] http://mfiles.pl/pl/index.php/System_informacji_strategicznej [dostęp: 11.01.2023].

decyzji strategicznych. Dobrze zorganizowany, na bieżąco aktualizowany, odnawiany i dostosowywany system informacji strategicznej pozwala wspierać decyzje strategiczne i ograniczyć ryzyko występujące przy ich podejmowaniu. Zależność między funkcjami systemu informacji strategicznej i procesem podejmowania powtarzalnych decyzji strategicznych obejmują:

- dostarczenie informacji do podejmowania poszczególnych rodzajów decyzji;
- informacje o efektach uzyskanych dzięki realizacji poszczególnych decyzji, wzbogacają istniejące zasoby informacyjne (bazy danych) systemu.

Umożliwia to wykorzystanie informacji przy podejmowaniu podobnych decyzji w przyszłości. Mimo, że każda z powtarzalnych decyzji strategicznych wymaga posiadania odrębnie dobranych zasobów informacji, można mówić o pewnym wspólnym obszarze informacyjnym, wykorzystywanym w trakcie podejmowania wszystkich powtarzalnych decyzji strategicznych. Obszar ten stanowi bazę informacyjną systemu informacji strategicznej[39].

Zakres najważniejszych informacji, które powinny się znaleźć w każdym systemie informacji strategicznej, obejmuje[40]:

- informacje o strategicznych zamiarach instytucji centralnych mających wpływ bezpośredni lub pośredni na funkcjonowanie branży i sektora;
- informacje o postępie naukowo-technicznym w branży i sektorze, pracach badawczych;
- informacje o rozwoju międzynarodowych stosunków gospodarczych i handlowych, mających wpływ na sektor;
- informacje o ekonomiczno-finansowych uwarunkowaniach gospodarki, w zakresie branży i sektora (poziomach cen, stawkach celnych itp.);
- informacje o poziomie atrakcyjności i możliwościach rozwoju danego sektora i branży, konkurentach, dostawcach i klientach, itp.;
- informacje o potencjalnych nowych rynkach, poziomie ich atrakcyjności oraz barierach, jakie tam funkcjonują;
- informacje o sytuacji wewnętrznej konkurentów, ich zamierzeniach, realizowanych strategiach;

[39] J. Czermiński, *Budowanie systemu informacji strategicznej*, Wyd. Dom organizatora, Toruń – Gdańsk 2002, s.196-197.

[40] Tamże.

- informacje o własnych zasobach i środkach, mocnych i słabych stronach przedsiębiorstwa;
- informacje o przebiegu wdrażania wybranej strategii działania oraz trudnościach i sposobach ich rozwiązania.

Powyższy zakres informacji obejmuje określenie pozycji na rynku, pozycji kosztowej, oceny rentowności i potencjału finansowego, poziomu umiejętności technologicznych, pozycji wobec dostawców i odbiorców, image firmy oraz poziom organizacji i zarządzania u konkurentów. Przedmiotem systemu informacji strategicznej jest zbiór zmiennych, określony różnorodnymi potrzebami informacyjnymi użytkowników[41]:

- zmienne te odwzorowują realne procesy i otoczenie, w jakim zachodzą (istnieje możliwość ich podziału);
- podzbiór zmiennych może stanowić wzorzec (normę postępowania, stany pożądane) i może być wprowadzony spoza miejsca w którym zachodzą;
- między zmiennymi są ujawnione powiązania (relacje) niezmienne w czasie. Mogą być to powiązania typu współzależność, korelacja itp.;
- założenie niezmienności relacji na tle czasu, przestrzeni, klasy, populacji stanowi istotny element wiedzy potrzebnej do podejmowania decyzji;
- zmiennymi pomocniczymi, parametrami stanowiącymi bazę odniesienia są czas, przestrzeń, klasa populacji itp.;
- operowanie zmiennymi jest niezbędnym elementem dla określenia dynamiki rozwoju i to w połączeniu z przyjętą bazą odniesienia;
- poziom rozdzielczości jest określony dla zbioru zmiennych pomocniczych i pozwala na określenie dokładności z jaką system informacji strategicznej obserwuje zachowania w trakcie realizacji strategii i reakcji otoczenia;
- ustanowiona hierarchia dla przyjętych poziomów rozdzielczości pozwala na generalizację bądź dekompozycję informacji w potrzebnych układach;
- zmienne dają obraz jakiejś cechy charakteryzującej wybrany aspekt obserwowanego procesu lub obiektu;
- obraz badanej cechy występuje zawsze w kontekście (relacji) do innych wielkości;
- obserwowalność zmiennych jest związana ze skończonym zbiorem wartości stanów, który reprezentuje zakres przejawiania się odpowiedniej cechy;

[41] Tamże.

- jeżeli przebieg zmiennych odbywa się w granicach pewnych stanów pożądanych, to jest to oceniane przez system decyzyjny pozytywnie – nie wymaga interwencji, korekty itp.;
- stany mogą mieć pewną właściwość matematyczną, np. uporządkowanie, odległość, związanie z upływem czasu;
- powiązania pomiędzy zmiennymi mają różnorodny charakter: logiczny, matematyczny, probabilistyczny, rozmyty i lingwistyczny.

Dla przykładu w naszym kraju dokument Priorytety zarządzania portfelem podmiotów nadzorowanych przez Ministra Skarbu Państwa do roku 2015 określa nadzór i budowę podmiotów ważnych dla ekonomicznego bezpieczeństwa państwa, jednocześnie zmniejszając zaangażowanie państwa w obszarach, w których jego udział nie jest niezbędny. Dokument zawiera także listę spółek o strategicznym znaczeniu dla gospodarki. To spółki, które budują wartość dla akcjonariuszy, odgrywają ważną rolę w procesie tworzenia silnej gospodarki kraju oraz współtworzą bezpieczeństwo ekonomiczne państwa.

Podmioty zamieszczone na liście mają wspierać proces rozwoju gospodarczego, innowacyjności oraz bezpieczeństwa państwa, ze szczególnym uwzględnieniem bezpieczeństwa energetycznego. Nie będą przy tym prywatyzowane. Do podmiotów o znaczeniu strategicznym zostały zaliczone[42]:

- Agencja Rozwoju Przemysłu;
- Bank Gospodarstwa Krajowego;
- Grupa Azoty;
- Grupa LOTOS od 1 sierpnia 2022 roku fuzja z PKN ORLEN;
- KGHM Polska Miedź;
- PGE Polska Grupa Energetyczna;
- Polska Wytwórnia Papierów Wartościowych;
- Polska Grupa Zbrojeniowa;
- Polski Koncern Naftowy ORLEN;
- Polskie Górnictwo Naftowe i Gazownictwo;
- Polskie Inwestycje Rozwojowe;
- Polskie Radio;
- Powszechna Kasa Oszczędności Bank Polski;
- Powszechny Zakład Ubezpieczeń;

[42] http://tvn24bis.pl/wiadomosci-gospodarcze,71/oto-22-strategicznych-spolek-rzad-poznal-ich-liste,456522.html [dostęp: 20.02.2021].

- Przedsiębiorstwo Eksploatacji Rurociągów Naftowych PRZYJAŹŃ;
- Przedsiębiorstwo Przeładunku Paliw Płynnych NAFTOPORT;
- TAURON Polska Energia;
- Telewizja Polska;
- Totalizator Sportowy;
- Zarząd Morskich Portów Szczecin i Świnoujście;
- Zarząd Morskiego Portu Gdańsk;
- Zarząd Morskiego Portu Gdynia.

Informacje strategiczne mogą być pozyskiwane z różnych źródeł, w tym z zasobów informacyjnych dostępnych w otoczeniu. Administracja państwowa najczęściej poszukuje informacji w instytucjach finansowych (33%), urzędach skarbowych (25%) i w Głównym Urzędzie Statystycznym (22%). Przedsiębiorcy w instytucjach finansowych szukają głównie informacji o nowych sposobach finansowania, sytuacji gospodarczej czy o klientach (zarówno potencjalnych, jak i obecnych). Z urzędów skarbowych firmy pozyskują informacje na temat zmian w prawie, a z Głównego Urzędu Statystycznego o obecnej sytuacji gospodarczej. Instytucje z otoczenia biznesu mają ogromny potencjał informacyjny, który nie jest w pełni wykorzystywany przez przedsiębiorców. Chodzi m.in. o inkubatory przedsiębiorczości, Komisję Europejską, Narodowy Bank Polski, Polski Komitet Normalizacyjny, samorządy gospodarcze. Odpowiednio do swoich kompetencji instytucje te upubliczniają informacje, które powinny być dla przedsiębiorstw użyteczne w trakcie planowania strategicznego. Jednak często przedsiębiorcy[43]:

- nie wiedzą o dostępności tych informacji;
- nisko oceniają ich praktyczną przydatność;
- nie wiedzą, w jaki sposób mogłyby one stać się użyteczne.

Szczególnie ciekawe źródło stanowi Komisja Europejska. Na podstawie informacji uzyskanych z tej instytucji można przewidywać zmiany w krajowym prawie, nawet kilka lat do przodu. Jest to istotne w planowaniu długookresowym, a szczególnie w identyfikowaniu nadchodzących szans i zagrożeń, które mogą wypływać ze zmian legislacyjnych. Eksperci ocenili, że informacje uzyskane z izb handlowych, następnie z Polskiej Agencji Rozwoju Przedsiębiorczości i urzędów wojewódzkich posiadają zadawalającą użyteczność[44]. Jako dobrą

[43] http://www.parp.gov.pl/index/more/14837 [dostęp: 20.03.2022].

[44] R. Maik, A. Gołoś, K. Szczerbacz, P. Walkiewicz, *Strategiczne źródła informacji w działalności przedsiębiorstw*, PARP, Warszawa 2010.

praktykę można przedstawić publikowanie przez urzędy pracy kompleksowych prognoz na temat lokalnego rynku pracy, zacieśnieniu współpracy z przedsiębiorcami. Należy również wskazać wprowadzenie systemu, za pomocą którego pracownik urzędu na bieżąco opiekuje się grupą ok. 20-30 przedsiębiorców, przeprowadzając ich przez cały proces pozyskania dofinansowania w ramach funduszy europejskich – od informacji wstępnej po przypominanie o poszczególnych terminach składania wniosków o dofinansowanie[45].

1.3. Koncepcja systemu informatycznego jako istotnego ogniwa strategii organizacji

W tej części opracowania przedstawiony zostaje zarys systemu informatycznego jako istotnego ogniwa strategii organizacji[46].

Budowa systemu (rozwiązania) informatycznego, wspomagającego działalność organizacji firmy czy przedsiębiorstwa w obszarze międzynarodowym, narodowym, wewnętrznym, obejmuje przedsięwzięcia daleko wykraczające poza sferę czysto techniczną i wymaga wieloaspektowego ujęcia. **Rozwiązanie to umożliwia obniżenie kosztów, a także poprawia efektywność gospodarki posiadanymi zasobami**. Ponadto zapewnia pełną kontrolę poszczególnych procesów podejmowania optymalnych i racjonalnych decyzji. Najbardziej ogólnie na system taki składają się[47]:

- dynamiczne procesy, realizowane w organizacjach, połączone z funkcjami poszczególnych jej części (architektura procesów);
- metody oceniania efektywności działań poszczególnych komponentów organizacyjnych (architektura efektywności);
- struktura organizacyjna – w powiązaniu z rolami i zadaniami ludzi tworzy organizację;

[45] Na podstawie raportu *Strategiczne źródła informacji w działalności przedsiębiorstw* autorstwa R. Maika, A. Gołosia i K. Szczerbacza. P. Walkiewicza. Badanie zrealizowano przez konsorcjum firm ARC Rynek i Opinia oraz Synergia na zlecenie Polskiej Agencji Rozwoju Przedsiębiorczości. Badanie realizowane w ramach projektu systemowego „Znaczenie wiedzy i informacji w zarządzaniu MSP" współfinansowanego przez Unię Europejską w ramach Europejskiego Funduszu Społecznego.

[46] Pełne opracowanie zawarłem w książce: *Nowoczesne technologie w logistyce*, Wyd. AON, Warszawa 2013, s. 95-119.

[47] D. Samól, J. Kuck, *Współczesne metody wsparcia informatycznego dla logistyki, kadr i finansów*, w: *Perspektywy informatyzacji logistyki wojska polskiego*, „Logis. Wewn." 2006, nr 4, s. 46.

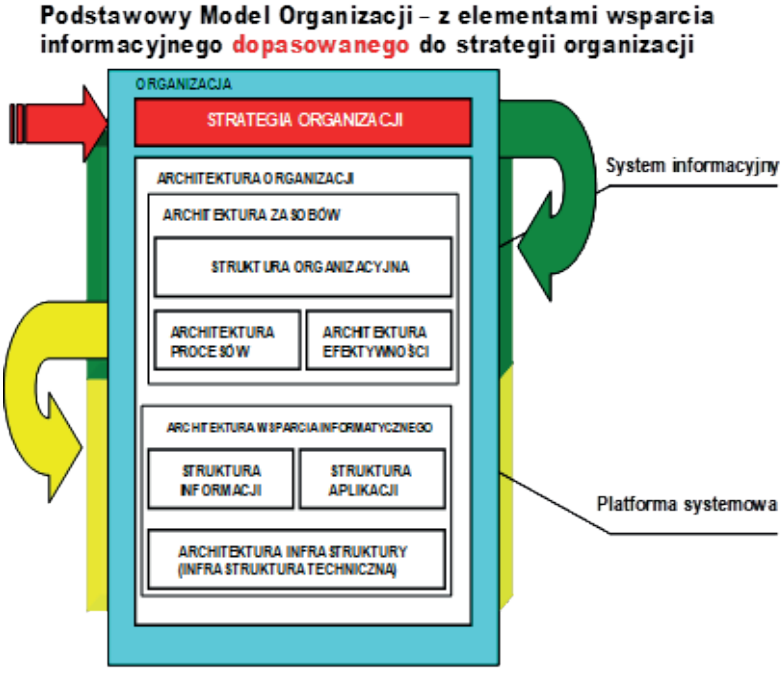
- rola i zakres informacji potrzebnej w wymienionych aspektach oraz struktury danych będących nośnikami tej informacji wraz ze sposobami ich przetwarzania;
- funkcje i usługi systemu informatycznego świadczone przez poszczególne aplikacje (struktura aplikacji);
- infrastruktura techniczna, zapewniająca środowisko działania poszczególnym aplikacjom.

Zakres wdrożeń i korzyści z nowoczesnych rozwiązań informatycznych obejmują:

- **korzyści strategiczne,** do których należy zaliczyć:
  - ✓ **środowisko umożliwiające współpracę,**
  - ✓ umożliwienie prowadzenia transakcji i zmian,
  - ✓ powstaje elastyczna organizacja, która sprawnej adaptuje nowe rozwiązania,
  - ✓ profesjonalna platforma zapewniająca sprawność operacyjną,
  - ✓ tworzenie bazy wiedzy;
- **korzyści wynikające z adaptowalności gotowych rozwiązań,** które gwarantuje:
  - ✓ standaryzacja i optymalizacja procesów gospodarczych, finansowych i kadrowych,
  - ✓ zmniejszenie liczby poprzednio stosowanych systemów i interfejsów,
  - ✓ wykorzystanie dotychczasowych inwestycji w IT dzięki nowoczesnej architekturze,
  - ✓ sprawne planowanie przyszłych potrzeb,
  - ✓ najlepszy zestaw gotowych komponentów;
- **rozwiązania, które poprzez swoją kompleksowość ułatwią pełne wykorzystanie i pozwolą amortyzować całkowity koszt** w obszarach:
  - ✓ funkcjonowania logistyki, finansów i kadr,
  - ✓ podejmowanie trafnych decyzji,
  - ✓ skalowania zdolności do globalnego wykorzystania,
  - ✓ elastyczności organizacyjnej oraz możliwość powołania grup zadaniowych;
- **ograniczenie ryzyka** związanego z:
  - ✓ podejmowaniem trafnych decyzji,
  - ✓ doświadczeniami, zaangażowaniem i partnerstwem profesjonalnych firm IT,

- ✓ wdrożeniami dla wielu użytkowników,
- ✓ dużą aktywną grupą klientów z sektora bezpieczeństwa;
- ✓ korzyściami wynikającymi z inwestycji firm IT w badania i rozwój.

System informatyczny w takim ujęciu jest integralną częścią całej organizacji – nie istnieje bez niej jako samodzielne rozwiązanie. Wymienione aspekty składają się na strategię organizacji, która wyznacza sposób działania i dopasowania poszczególnych organizacyjnych elementów składowych. Inaczej mówiąc: strategia organizacji jest rozumiana tutaj jako specyficzne połączenie **ludzi, środków (zasobów) i metod działania** w celu osiągnięcia celów organizacji w założonym czasie. Dopasowanie działania platformy systemowej do obiegu i wykorzystania informacji w organizacji jest bardzo istotne w czasie jej budowy, jaki w trakcie jej późniejszego funkcjonowania.



Rys. 3. Podstawowy Model Organizacji – z elementami wsparcia informacyjnego dopasowanego do strategii organizacji

Źródło: D. Samól, J., Kuck. *Współczesne metody wsparcia informatycznego dla logistyki, kadr i finansów*, w: *Perspektywy informatyzacji logistyki wojska polskiego*, SG WP, „Logis. Wewn." 2006, nr 4, s. 48.

W płaszczyźnie technicznej systemu powinna być także odwzorowana struktura organizacyjna, uwzględniająca identyfikację i rolę użytkowników, oraz zakres używanej informacji i miejsc zdarzeń. Opracowanie modelów procesów, które w przejrzysty sposób przekładają się na wymagane struktury informacji, obejmuje z reguły: kierowanie, dowodzenie, informowanie, sprawozdawczość, planowanie i dotyczy wielu dziedzin związanych z logistyką, kadrami i finansami. Jest jednocześnie kluczowym elementem powodzenia całego przedsięwzięcia. Dzieje się tak dlatego, że ze struktury potrzebnej informacji wynika struktura zastosowania (aplikacji). Dlatego też niezmiernie ważnym jest, aby oprogramowanie dostarczało gotowych wzorców (modeli) referencyjnych, łączących w sobie sferę systemu informacyjnego z wymaganymi strukturami platformy systemowej. Dopiero przy takim wspomaganiu staje się możliwe stworzenie wsparcia informacyjnego dla złożonych procesów, a wdrożenia technologii IT przebiegają w założonym czasie i budżecie.

Za dobry przykład rozwoju prac analitycznych może służyć Podstawowy Model Organizacji (rys. 3), w którym przedstawiono związek elementów wsparcia informacyjnego wynikający z dopasowania do strategii organizacji. W kolejnym kroku ustalana jest lista celów stawianych rozwiązaniu informatycznemu, jakim jest w tym przypadku system klasy ERP. Rozwiązanie, w zależności od struktur organizacyjnych, może być kształtowane na różnych poziomach i z różnych perspektyw. W organizacjach tych powinny powstać odpowiednie zasoby, a w nich zdolności wyrażone w zgromadzonej wiedzy, wyszkoleniu i gotowości do współdziałania na platformie informatycznej. Dopiero w powiązaniu z nimi istotną rolę odgrywają takie elementy, jak struktura informacji, struktura aplikacji istruktura techniczna. Innymi słowy – rozwiązanie informatyczne składa się w pierwszej kolejności z **odpowiednio przygotowanych ludzi, którzy są zdolni do współpracy w ramach wspólnej organizacji**. Dopiero za nimi postępuje technologia i infrastruktura. Wspomniane obszary tematyczne można również zobaczyć w perspektywie procesów. Uszczegółowienie założeń występuje tu na poziomie wielu rodzajów i kategorii procesów – takich, jak kierowanie i dowodzenie, informowanie, planowanie, prognozowanie i symulacje, ewidencja i sprawozdawczość, opracowanie struktur i normatywów oraz kontrola i ocena. Daje to podstawę do wyznaczenia kształtu rozwiązania informatycznego w przedstawionymi na rysunku – architekturze procesów, architekturze efektywności, architekturze wsparcia informatycznego – w powiązaniu z racjonalnie

przeprowadzanymi zmianami organizacyjnymi. W takich warunkach system informatyczny może okazać swoją pełną przydatność jako integralna część całej organizacji.

Z przedstawionego przykładu wynika, że strategia organizacji jest podstawą formułowania całego rozwiązania informatycznego, które powinno być z nią zharmonizowane. Tym sposobem powstaje całościowy system działający na jednej platformie technologicznej, który wspomaga strukturę organizacyjną, architekturę procesów i architekturę efektywności (architekturę zasobów) zarówno w aspekcie logistycznym, finansowym, jak i kadrowym. Warto zauważyć, że opieramy się tutaj na jednolitej (spójnej) strukturze informacji i zintegrowanej strukturze aplikacji. Podstawą całości jest warstwa infrastruktury, która w takim ujęciu nabiera strategicznego znaczenia dla całej organizacji. Istotne metody zarządzania informacją i przetwarzania danych wynikają również bezpośrednio z analizy modelu sytuacji globalnej. Obecnie technologia informacji dostarcza bogatą paletę możliwości, w tym kooperację w ramach prowadzenia przedsięwzięć o charakterze projektowym i innowacyjnym oraz szkoleniowym.

W dzisiejszych czasach dostępne technologie IT posiadają duży potencjał i są ze sobą zintegrowane warstwowo. Oprócz integracji w warstwie technicznej, dzięki odpowiedniej funkcjonalności, zapewnia się tutaj przede wszystkim integrację na poziomie współpracy pomiędzy użytkownikami. Drugim – nie mniej ważnym zagadnieniem – jest integracja zarządzania procesami biznesowymi. Realizuje się ona poprzez odpowiednio przemyślany dobór i konstrukcję aplikacji (metod przetwarzania informacji i programów komputerowych). Trzecim elementem jest integracja informacji, bez której dwa pierwsze praktycznie nie mogłyby istnieć. W integracji informacji ważna jest spójność i semantyczna jednoznaczność. Prowadzi to do sytuacji, w której procesy są jednolicie wspomagane w całym obszarze organizacji, a informacja (i tworzące ją dane) nie są uwięzione w jednej tylko bazie danych lub aplikacji. W takich warunkach jest możliwe zapewnienie funkcjonalności dla następujących obszarów tematycznych[48]:

- rachunkowość finansowa i rachunek kosztów;
- planowanie, kierowanie i dowodzenie;
- analizy operacyjne i zapewnienie kontynuacji działań;
- nabycie (obsługa procesów zakupowych);

[48] D. Samól, J. Kuck. *Współczesne metody wsparcia informatycznego dla logistyki, kadr i finansów*, w: *Perspektywy informatyzacji logistyki wojska polskiego*, „Logis. Wewn." 2006, nr 4, s. 54.

- wsparcie logistyczne wykonywanych zadań;
- obsługa eksploatacji i bieżących napraw;
- obsługa konserwacji i remontów;
- zarządzanie gospodarką materiałową;
- zarządzanie infrastrukturą;
- zarządzanie kadrami i obsługa administracyjna kadr.

Kombinacja wymienionych obszarów z poszczególnymi aspektami organizacyjnymi pozwala na formułowanie metod stosowanych w rozwiązaniach informatycznych w obszarach logistyki, finansów i zarządzania kapitałem ludzkim. Zastosowana struktura informacji umożliwia tworzenie materiałowej hierarchii planistycznej będącej podstawą do tworzenia planów, symulacji i prognoz na różnych poziomach szczegółowości – do zestawów włącznie.

Architektura procesów i architektura informacji dają podstawy do efektywnego działania. Informacja naprawdę istnieje jednak tylko wtedy, gdy dostrzega ją użytkownik. Role użytkowników są ważne dlatego, że:

- indywidualna rola użytkownika określa jego potrzeby informacyjne;
- rozprzestrzenianie informacji zharmonizowanej z rolami buduje środowisko dla zarządzania wiedzą;
- stanowiska działania użytkowników oparte na rolach pozwalają na łączenie informacji ustrukturalizowanej i nieustrukturalizowanej (dokumentów) z różnych źródeł;
- role odzwierciedlają zasady działania organizacji – zwłaszcza w środowisku międzynarodowym;
- role są używane do określania zasad bezpiecznego dostępu do informacji.

Praktyczną realizację koncepcji ról użytkowników w postaci portalu informacyjnego prezentującego informację pochodzącą z różnych źródeł, kontekstowo dopasowaną do potrzeb użytkownika. Przykładowo użytkownik posługując się mapą numeryczną (cyfrową) widzi sytuację w interesujących go aspektach zgodnych z jego rolą.

Informacja może przynieść efekty dla tego, kto z niej korzysta, wtedy, gdy jest rzetelna (prawdziwa). Nie powinna być półprawdą lub wprowadzać użytkownika w błąd. Rzetelność wynika z dokładności i metody rejestrowania rzeczywistych zdarzeń (prawidłowość metodologiczna). Poziom rzetelności zależy głównie od precyzji narzędzi rejestracyjnych i procesu przetwarzania informacji, stopnia obiektywizmu oraz od błędów metodycznych. Informacja rzetelna

to informacja wiernie odwzorowująca rzeczywistość operacji gospodarczych i przebiegów procesów zachodzących w identyfikowanym środowisku.

1.4. Istota bezpieczeństwa informacyjnego

Bezpieczeństwo może być postrzegane jako brak widocznych zagrożeń i obejmować niemal wszystkie obszary życia człowieka. Termin bezpieczeństwo ma charakter podmiotowy i jest używany do określenia stanu pewności, spokoju czy braku zagrożenia.

Abraham Masłow wyróżnia bezpieczeństwo, po potrzebach fizjologicznych, jako drugie w hierarchii potrzeb człowieka[49]. Brak bezpieczeństwa u człowieka powoduje poczucie zagrożenia, niepokój, często stres. Zarówno bezpieczeństwo, jak i zagrożenie, są ze sobą związane. Gdy zagrożenie nie istnieje mamy poczucie bezpieczeństwa. Zagrożeniem określamy pewien stan psychiki i świadomości, wywołany postrzeganiem zjawisk, które oceniane są jako niekorzystne lub niebezpieczne. Obecnie obserwuje się tendencje do poszerzania się treści pojęcia bezpieczeństwo, zarówno o wartości wewnętrzne podlegające ochronie, jak i siły oraz środki ochrony stosowane do jego utrzymania.

Rys. 4. Hierarchia potrzeb Abrahama Maslowa

Źródło: https://pl.psichiatria.org/wp-content/uploads/2018/09/piramida-maslowa2-300x225 .png [dostęp: 15.06.2020].

[49] A. Masłow, *A theory of Human Motivation,* „Psychogical Review" 1943, lipiec, s. 370-396.

W związku z cyfrową rewolucją przemiany techniczne i organizacyjne powodują nowe zróżnicowanie w społeczeństwie, organizacjach i instytucjach, a nawet państwach. Do nowych wyzwań towarzyszących budowie społeczeństwa informacyjnego zalicza się[50]:

- wzrost powszechności stosowania systemów komunikacji elektronicznej w zastosowaniach administracji publicznej (urząd – urząd, urząd – przedsiębiorca, urząd – obywatel);
- korzystanie z wydzielonych sieci teleinformatycznych dla wybranych systemów oraz sieci publicznych w relacjach urząd – urząd;
- planowany rozwój i wdrażanie systemów e-administracja – korzystanie w szerszym zakresie z sieci Internet, także w komunikacji w relacji urząd – urząd;
- rozwój i wzrost liczby ofert usług sieciowych i dodatkowych, realizowanych przez ich dostawców;
- rozwój technologii dostępowych i sieci radiodostępowych;
- wzrost liczby zagrożeń, m.in. cyberterroryzmem, szpiegostwem, przestępczością i klęskami żywiołowymi;
- obowiązki na rzecz bezpieczeństwa państwa, zapewnienia funkcjonowania usług w sytuacjach szczególnych zagrożeń.

Nowe zagrożenia powodują potrzebę podjęcia skutecznych działań zapobiegawczych. **Bezpieczeństwo informacyjne** jest przez praktyków bardzo często rozumiane jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania. Środki bezpieczeństwa podejmowane są w celu zapewnienia poufności, integralności i dostępności informacji. Głównym celem jest wyeliminowanie zagrożenia informacji[51].

Bezpieczeństwo informacyjne stanowi zbiór działań, metod, procedur podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych

[50] J. Jańczak, A. Nowak, *Bezpieczeństwo Informacyjne Wybrane problemy*, AON, Warszawa 2013, s. 13.

[51] Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*. Wyd. Adam Marszałek, Toruń 2006.

zasobów informacyjnych poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją lub zniszczeniem[52].

W innym ujęciu bezpieczeństwo informacyjne dotyczy zagwarantowania sobie przez dany podmiot (np. państwo) integralności, kompletności oraz wiarygodności posiadanych zasobów informacyjnych w każdej formie, nie tylko elektronicznej. Odnosi się więc zarówno do wszelkiego rodzaju wysiłków służących ochronie posiadanych informacji, istotnych w kontekście bezpieczeństwa (a więc mających wpływ na sprawne funkcjonowanie struktur państwowych i społeczeństwa), jak i zapewnieniu przewagi informacyjnej przez zdobywanie nowych lub bardziej aktualnych danych oraz akcje dezinformacyjne wobec ewentualnych przeciwników (państw lub innych podmiotów)[53]. Z kolei bezpieczeństwo informatyczne (teleinformatyczne) odnosi się do faktu szybkiego upowszechniania określonych metod gromadzenia, przetwarzania, przesyłania informacji oraz wiążących się z tym konsekwencji w sferze bezpieczeństwa, nie zaś zwiększenia rangi informacji we współczesnym świecie[54]. Postęp w teleinformatyce doprowadził do sytuacji, w której konfrontacja objęła cyberprzestrzeń, co prowadzi do rozwoju podmiotów państwowych (pozapaństwowych) czy jednostek, które mogą stać się również źródłem poważnych zagrożeń dla ich bezpieczeństwa. Bezpieczeństwo informacyjne łączy ze sobą sferę nie tylko militarną, ale także pozamilitarną. Występuje sposób oficjalny i niejawny zarówno w czasie pokoju, jak i w czasie kryzysu oraz wojny, co jest jej cechą charakterystyczną.

Generalną zasadą bezpieczeństwa informacji oraz systemów i sieci IT służących do ich przetwarzania i przesyłania jest ochrona informacji przed nieuprawnionym dostępem, ujawnieniem (losowym, zamierzonym) lub nieuprawnionym zniszczeniem lub modyfikacją, a także przed opóźnieniem lub nieuzasadnioną odmową jej dostarczenia. W systemach i sieciach IT powinny zostać wprowadzone środki i metody zapewniające atrybuty bezpieczeństwa informacji[55]. Są one powiązane z kryteriami jakie ma spełniać dostarczona informacja:

---

[52] Potejko P., *Bezpieczeństwo informacyjne, w: Bezpieczeństwo państwa*, red. K. A. Wojtaszczyk, A. Materska-Sosnowska, Oficyna Wydawnicza ASPRA-JR, Warszawa 2009, s. 194.

[53] A. Żebrowski, Bezpieczeństwo informacyjne Polski a walka informacyjna, „ Roczniki Kolegium Analiz Ekonomicznych" 2013, nr 29, online: http://rocznikikae.sgh.waw.pl/p/roczniki_kae_z29_30.pdf [dostęp: 04.03.2024].

[54] M. Madej, *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwapaństw i systemu międzynarodowego, w: Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Wydawnictwo PISM, Warszawa 2009, s. 18-19.

[55] S. Nabrdalik, *Bezpieczeństwo systemów i sieci teleinformatycznych w świetle ustawy o ochronie informacji niejawnych*, w: J. Kuck (red.), *Współczesne zagrożenia w zarządzaniu*

- **poufność** – dostęp do informacji musi być ograniczony do kręgu użytkowników uprawnionych/autoryzowanych;
- **integralność**[56] – informacja musi być zachowana w swojej postaci oryginalnej, za wyjątkiem przypadków, gdy jest ona legalnie aktualizowana lub usuwana przez podmioty do tego uprawnione;
- **integralność systemów** – zapewnienie, że system realizuje swoje funkcje w sposób nienaruszony, wolny od nieautoryzowanej manipulacji, przypadkowej lub zamierzonej;
- **dostępność** – właściwość, że zasób systemu teleinformatycznego musi być możliwy do wykorzystania na żądanie, w określonym czasie przez podmiot uprawniony do pracy w systemie;
- **autentyczność** – zapewnienie, że tożsamość podmiotu lub zasobu systemu jest taka jak deklarowana – dotyczy użytkowników, procesów, systemów lub nawet instytucji;
- **rozliczalność** – dostęp do informacji może być przypisany w sposób jednoznaczny tylko określonemu podmiotowi;
- **niezawodność** – zachowanie i skutki działania, np. aplikacji lub urządzeń systemu są takie, jak zamierzone.

Chcąc mówić o bezpieczeństwie informacji w systemach i sieciach teleinformatycznych, musimy odpowiedzieć sobie na pytanie, co to jest system teleinformatyczny oraz co rozumiemy pod pojęciem bezpieczeństwa teleinformatycznego. Odpowiedzi na pierwsze pytanie udziela ustawa o świadczeniu usług drogą elektroniczną. Według przepisów tej ustawy, **system teleinformatyczny** to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniających przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego[57]. Bezpieczeństwo teleinformatyczne doczekało się w literaturze bardzo wielu definicji. Możemy go rozumieć jako:

i bezpieczeństwie, tom I, Wyd. UKiP J&D Gębka, Katowice 2014, s. 541-542.

[56] W literaturze przedmiotu spotyka się podział na integralność informacji i integralność systemów rozumianych tak jak w podanych definicjach. Często jednak stosuje się tylko pojęcie integralności, rozumiejąc pod tym pojęciem zarówno zachowanie informacji w postaci oryginalnej jak i zapewnienie, że system wykonuje swoje funkcje w sposób nienaruszony, wolny od nieautoryzowanych ingerencji.

[57] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczna (Dz. U. 2002, nr 144, poz. 1204) art. 2 pkt 3.

- całokształt przedsięwzięć zmierzających do zapewnienia bezpieczeństwa systemów i sieci teleinformatycznych oraz ochrony danych wytwarzanych, przetwarzanych, przechowywanych lub przekazywanych w tych systemach i sieciach przed przypadkowym lub celowym ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem ich przetwarzania poprzez zastosowanie w sposób kompleksowy technicznych, programowych, kryptograficznych oraz organizacyjnych środków i metod[58];
- poziom uzasadnionego zaufania i pewności, że potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego) ujawnienia, modyfikacji zniszczenia lub uniemożliwienia przetwarzania danych przechowywanych przesyłanych za pomocą systemów teleinformatycznych, nie zostaną poniesione[59].

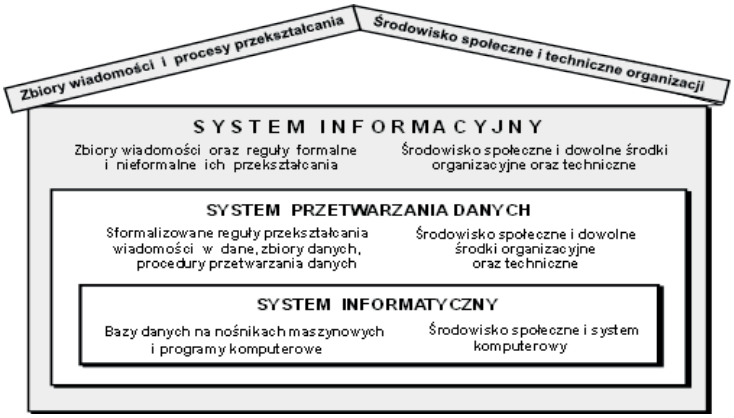
1.5. Rosnąca rola bezpieczeństwa informacyjnego w państwie i podmiotach gospodarczych oraz wśród obywateli

W obecnych czasach transformowanie przez użytkowników określonych informacji wejścia na oczekiwane informacje wyjścia odbywa się najczęściej w systemie informacyjnym. Taki system stanowi wielopoziomową strukturę i działa za pomocą odpowiednich procedur i modeli. Aby system informacyjny mógł sprawnie funkcjonować i być bezpieczny, powinien mieć odpowiednio zorganizowany układ kanałów informacyjnych, którymi przekazywane są informacje do konkretnych użytkowników[60].

[58] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne – wybrane problemy*, Wydawnictwo AON, Warszawa 2013, s. 44.

[59] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008, s. 13.

[60] Powiązania komunikacyjne pomiędzy menadżerami a ich podwładnymi tworzone w celu zwiększenia zdolności organizacji do przetwarzania informacji – zob. R. W. Griffin, *Podstawy zarządzania organizacjami*, PWN, Warszawa 2001, s. 385.



Rys. 5. Ogólny model relacji zachodzących między systemem informacyjnym, systemem przetwarzania danych i systemem informatycznym

Źródło: Z. J. Klonowski, *Systemy informatyczne zarządzania przedsiębiorstwem. Modele rozwoju, właściwości funkcjonalne*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2004, s. 181.

Występujący w systemie informacyjnym system informatyczny (jako część składowa) obejmuje oprogramowanie, konfigurację sprzętu, sieci komputerowe, procedury wspomagające wyprowadzenie informacji z baz danych w celu wsparcia procesu decyzyjnego oraz osiągnięcie określonych celów w trakcie zarządzania czy dowodzenia.

W skład systemu informacyjnego jako całości wchodzi **system informatyczny,** który jest wyodrębnioną jego częścią. Umożliwia działania na informacji poprzez **komputery, oprogramowanie i sieci do przetwarzania, gromadzenia i przesyłania danych**. Systemy informatyczne w organizacjach, instytucjach i przedsiębiorstwach wykorzystywane są w procesie zarządzania (dowodzenia), przez co wspierają realizację poszczególnych funkcji związanych z planowaniem, organizowaniem, motywowaniem i kontrolowaniem.

W dużych organizacjach i instytucjach projektowane i wdrażane są zintegrowane systemy informatyczne. Są one najbardziej zaawansowaną formą rozwiązań informatycznych, wspomagających procesy zarządzania. Mają strukturę modułową co oznacza, że są budowane (składane) z wcześniej zaprojektowanych uniwersalnych „cegiełek" programowych (software'owych), nazywanych modułami[61]. **Zintegrowany system informatyczny charakteryzuje się:**

[61] J. Długosz, *Nowoczesne technologie w logistyce*, Wyd. PWE, Warszawa 2009, s. 55-56.

- **kompleksowością funkcjonalną,** która obejmuje wszystkie sfery działalności organizacji, instytucji, przedsiębiorstwa;
- **integracją danych i procesów** wewnątrz organizacji oraz jej otoczenia realizowanej w ramach struktury informacyjnej;
- **elastycznością strukturalną,** zapewniającą maksymalne dostosowanie rozwiązań sprzętowo-programowych do potrzeb organizacji;
- **otwartością**, która gwarantuje zdolność rozszerzania systemu o nowe moduły, skalowalną architekturę;
- **zaawansowaniem merytorycznym**, zapewniającym pełne informatyczne wsparcie procesów informacyjno-decyzyjnych z wykorzystaniem mechanizmów ekstrakcji i agregacji danych, wariantowania, optymalizacji i programowania;
- **zaawansowaniem technologicznym** gwarantującym zgodność z aktualnymi standardami sprzętowo-programowymi, możliwością przenoszenia na nowe platformy sprzętowe systemów operacyjnych oraz mediów i protokołów komunikacyjnych;
- **zgodnością z aktualnie obowiązującymi przepisami** normującymi działalność informatyzowanej organizacji[62].

Zintegrowany system informatyczny klasy ERP obejmuje w procesie produkcji określone moduły i podsystemy. Do zasadniczych z nich należy zaliczyć te służące do wspomagania:

- planowania i sterowania zdolnościami oraz procesami produkcyjnymi;
- zarządzania środkami trwałymi;
- zarządzania produkcją;
- finansów i księgowości;
- zarządzania jakością;
- zarzadzania zasobami ludzkimi;
- zarządzania kontaktami z klientami;
- nadzoru i kontroli[63].

Narzędzia ERP w obszarze prowadzenia analiz, obsług raportów wymagają jeszcze dalszego doskonalenia. Trudności pojawiają się wtedy, gdy wykorzystujemy standardowe, dostarczone wraz z systemami predefiniowane raporty

[62] Studium Realizowalności Zintegrowanego Systemu Informatycznego Resortu Obrony Narodowej (ZSI RON), t. 1. *Model ogólny systemu* (STD-01), SG WP, Warszawa 2005, s. 135-136.

[63] J. Kuck, *Nowoczesne technologie w logistyce*, AON, Warszawa 2013, s. 18.

uwzględniające częściowo specyfikę poszczególnych organizacji, instytucji czy przedsiębiorstw. Brakuje w nich podstawowych elementów, potrzebnych do analizy i prezentacji danych związanych z:

- graficzną wizualizacją wyników;
- rozwiązaniami do wykonania symulacji i śledzenia wyników;
- ustandaryzowanych danych, pozwalających na analizy porównawcze wyników związanych z procesami produkcyjnymi.

Te niedogodności można usunąć przez rozwiązanie należące do systemów wspomagania decyzji[64]. Systemy Wspomagania Decyzji (SWD, ang. DSS,*Decision Support Systems*) to uniwersalne narzędzia (informatyczne), które dostarczają na wszystkich szczeblach organizacji rzetelną informację, skorelowaną z bieżącą sytuacją danej organizacji i wspomagającą proces podejmowania decyzji. Rozwój, ewolucja systemów DSS w kierunku inteligentnego wspierania podejmowania decyzji DSS dała początek narodzin nowej koncepcji systemów, którą nazwano *Business Intelligence*[65] (BI), czyli systemy dostarczające kompleksowych informacji, wspierające podejmowanie decyzji na wszystkich szczeblach zarządzania organizacją, instytucją czy przedsiębiorstwem.

Do typowych zastosowań systemu BI w organizacji instytucji i przedsiębiorstw możemy zaliczyć:

- **finanse** (analizy ryzyka, prognozy rentowności inwestycji, analiza efektywności, zarządzania kosztami, planowanie budżetu, kontrola i wykrywanie nadużyć);
- **sprzedaż i marketing** (analiza rynku, zarządzanie relacjami z klientem, planowanie i analiza wyników sprzedaży, identyfikacja segmentów rynkowych

[64] Systemy wspomagające decyzje ewoluowały w ciągu ostatnich kilkunastu lat, początkowo od systemów informowania kierownictwa EIS (*Executive Information Systems*), poprzez systemy wspomagania podejmowania decyzji DSS (*Decision Support System*) i systemy wspomagające najwyższe kierownictwo ESS (*Executive Sypport Systems*), aż po systemy analityki biznesowej BI (*Business Intelligence*).

[65] Twórcą systemu *Business Intelligence* jest Hans Luhn. Po pierwszej wojnie światowej wyemigrował do USA, gdzie związał się z firmą IBM. Termin *Business Inteligence* – BI, został wprowadzony przez firmę Gartner Group w 1989 r. jako „zestaw koncepcji metodyk mających na celu usprawnienie podejmowania decyzji biznesowych przez użycie systemów opartych na faktach" J. Janczak Narzędzia analityki biznesowej w zastosowaniach militarnych, Zeszyty Naukowe AON nr 2(91) 2013.
Gartner Group jest amerykańską firmą doradczo-opiniującą o wysokiej renomie w zakresie technologii informacyjnych. Klienci, subskrybując jeden z kilkudziesięciu oferowanych serwisów informacyjnych IT, nabywają także prawo do konsultacji za pośrednictwem telefonu, faksu czy Internetu.

i nowych rynków zbytu, rentowność klientów, segmentacja klientów, analiza promocji i efektywności kampanii, analiza produktów);
- **produkcja i logistyka** (optymalizacja procesów produkcyjnych), zarządzanie jakością, planowanie według strategii dokładnie na czas JIT (*Just-in-Time*);
- **zarządzani łańcuchem dostaw** (wydajność i optymalizacja dystrybucji, planowanie popytu, kontrola stanów magazynowych);
- **zarządzanie zasobami ludzkimi** (planowanie i optymalizacja czasu pracy, planowanie i analiza płac, analiza rotacji kadr);
- **zbilansowanie karty wyników** *(Balanced Ccorecard)*[66].

Obszary funkcjonalne systemu BI mogą obejmować wiele dziedzin życia. Dobre efekty osiągamy szczególnie w logistyce, finansach i działalności kadrowej. W finansach możemy monitorować kondycję finansową przedsiębiorstwa, dokonywać wielowariantowych analiz biznesowych. W logistyce szerokie wykorzystanie dotyczy planowania strategicznego i operacyjnego.

W roku 1999 z inicjatywy federacji europejskiej stowarzyszeń informatycznych **CEPIS**[67] powstał projekt Karty Praw Obywateli Społeczeństwa Informacyjnego. W projekcie tym jest mowa o wejściu w erę, w której informacja staje się dobrem użyteczności publicznej, będziemy od niej tak samo zależni, jak od wody, żywności czy elektryczność. W tych nowych czasach obywatele będą chcieli gwarancji dostępu do zasobów informacji w Internecie. Aby zapewnić obywatelom dostęp do informacji należy kierować się następującymi zasadami:
- dostęp do zasobów informacyjnych oraz Internetu powinien być powszechny;
- informacja powinna być wiarygodna, nie może wprowadzać w błąd;
- obywatele powinni mieć możliwość działania w społeczeństwie informacyjnym bez obaw, że dane ich dotyczące mogą być kiedyś wykorzystane przeciwko nim;
- każdy musi być pewien, że dostępne środki są zadośćuczynieniem w przypadku naruszenia autentyczności oraz prywatności informacji;
- obywatele muszą uzyskać pomoc w stosowaniu tych środków, jeśli zajdzie potrzeba, zasady odpowiedzialności muszą być jasne i nie zdeformowane interesami silniejszych uczestników życia społecznego;

[66] J. Jańczak, *Systemy analityki biznesowej narzędziem wspomagającym procesy decyzyjne w logistyce wojskowe*j, AON, Warszawa 2012, s. 258.

[67] **CEPIS** – Europejska Rada Stowarzyszeń Zawodowych Informatyków; organizacja dążąca do promowania wysokiej jakości standardów w zawodzie informatyka.

- społeczności mają obowiązek umożliwienia obywatelom zdobycia umiejętności potrzebnych do uczestnictwa w społeczeństwie informacyjnym, a zwłaszcza korzystania z możliwości i stawiania czoła wyzwaniom wynikającym z szerokiego wykorzystania Internetu.

Rządy państw oraz organizacje międzynarodowe są odpowiedzialne za zagwarantowanie realizacji powyższych zasad. Kluczowymi strefami są takie, w których istnieje zagrożenie ze strony działalności władz, np.:

- ochrona przed łamaniem zabezpieczeń kryptograficznych;
- ochrona przed pozyskiwaniem informacji przez rządy innych państw w sytuacji, gdy obywatele są nieświadomi tego, że ich dane są dostępne dla innych państw lub tego, że inne państwa mogą zbierać taką informację[68].

1.6. Zasady bezpieczeństwa informacyjnego

Informacja zawsze stanowiła element podlegający szczególnej ochronie. Do podstawowych aktów prawnych regulujących problematykę bezpieczeństwa informacji w Rzeczypospolitej Polskiej należą Konstytucja RP, ustawy, ratyfikowane umowy międzynarodowe, rozporządzenia. Stosowanie aktów normatywno-prawnych w społeczeństwie informacyjnym ma znaczący wpływ na funkcjonowanie organizacji, instytucji, firm czy całej gospodarki narodowej. Utrata integralności oraz poufności informacji może spowodować straty finansowe, konsekwencje prawne, a tym samym wpłynąć na wizerunek organizacji i przesądzić o jej funkcjonowaniu i istnieniu na rynku. Można zdefiniować wiele metod ustalenia wymagań związanych z bezpieczeństwem informacyjnym. Do najważniejszych zalicza się:

- znajomość uregulowań prawnych dotyczących wymaganych działań, zapewniających bezpieczeństwo informacji;
- oszacowanie poziomu ryzyka utraty informacji;
- wypracowanie w organizacji odpowiedniej postawy odnośnie zapewnienia bezpieczeństwa informacji;
- wskazanie obszarów, w których zachodzi konieczność poprawy[69].

[68] *Społeczeństwo informacyjne*, praca zbiorowa pod red. S. J. Nowak, G. Bliźniuk, PTI – Oddział Górnośląski, Katowice 2005, s. 40.

[69] J. Jańczak, A. Nowak, *Bezpieczeństwo Informacyjne Wybrane problemy*, AON, Warszawa 2013, s. 79.

W celu zapewnienia bezpieczeństwa informacji należy zastosować odpowiednią politykę bezpieczeństwa. Można ją podzielić na cztery podstawowe obszary:

- **politykę organizacyjną** – zawierającą procedury organizacyjne, w tym procedury utrzymania ciągłości działania oraz plany awaryjne na wypadek katastrofy, związane z zapasowymi ośrodkami przetwarzania;
- **politykę ochrony technicznej** – związaną z ochroną pomieszczeń, budynków, mienia oraz personelu danej społeczności, czy też organizacji, zawierającą różnego rodzaju instrukcje zabezpieczeń, procedury na wypadek incydentów bezpieczeństwa lub sytuacji zagrożeń;
- **politykę personalną** – związaną z odpowiednim doborem personelu na dane stanowiska, procedurami dotyczącymi zapoznania pracowników z zasadami bezpieczeństwa (BHP, procedury awaryjne, procedury ochrony informacji), ich szkoleniami oraz procedurami działania na wypadek zakłóceń w pracy personelu;
- **politykę bezpieczeństwa informacji –** związaną z zarządzaniem i ochroną informacji stanowiących tajemnicę społeczności i informacji prawnie chronionych, dopuszczeniem osób do informacji oraz systemów przetwarzania informacji do eksploatacji, procedurami kryzysowymi na wypadek incydentów bezpieczeństwa[70].

Cykl funkcjonowania i zasady ochrony systemów teleinformatycznych. Z lektury przepisów zawartych w Rozporządzeniu Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011, nr 159, poz. 948.) można wywnioskować, że w zakresie ochrony systemów i sieci teleinformatycznych mają zastosowanie następujące zasady:

- **zarządzanie ryzykiem** – objęcie systemu teleinformatycznego procesem zarządzania ryzykiem bezpieczeństwa informacji niejawnych przetwarzanych w systemie teleinformatycznym;
- **ograniczenie zaufania** – polega na traktowaniu innych systemów teleinformatycznych jako potencjalnych źródeł zagrożeń oraz wdrożeniu w systemie teleinformatycznym zabezpieczeń kontrolujących wymianę informacji z tymi systemami teleinformatycznym;

[70] Tamże, s. 81.

- **wielopoziomowej ochrony** systemu teleinformatycznego, polegającej na stosowaniu zabezpieczeń na możliwie wielu różnych poziomach organizacji ochrony systemu teleinformatycznego;
- **ograniczenie uprawnień**, polegającej na nadawaniu użytkownikom systemu teleinformatycznego wyłącznie uprawnień niezbędnych do wykonywania pracy;
- **minimalizacja funkcjonalności,** polegającą na instalowaniu, uaktywnianiu i wykorzystywaniu w systemie teleinformatycznym wyłącznie funkcji, protokołów komunikacyjnych i usług niezbędnych do prawidłowej realizacji zadań, do których system teleinformatyczny został przeznaczony;
- **okresowych testów bezpieczeństwa** – przeprowadzanie testów bezpieczeństwa systemu IT.

Szczególne znaczenie na bezpieczeństwo systemów i sieci teleinformatycznych ma przetwarzanie i przesyłanie informacji niejawnych. Według ustawy o ochronie informacji niejawnych, **informacji niejawna** to informacja, niezależnie od formy i sposobu jej wyrażenia, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczpospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne także na etapie jej tworzenia[71].

Duże znaczenie, z punktu widzenia ochrony systemów i sieci teleinformatycznych, ma klasyfikacja informacji niejawnych. Klauzula jaką jest opatrzona informacja niejawna implikuje sposób jej ochrony, a tym samym sposób ochrony i zabezpieczenia systemów i sieci teleinformatycznych.

Ustawa o ochronie informacji niejawnych w art. 5 dokonuje klasyfikacji informacji niejawnych na: **ściśle tajne, tajne, poufne, zastrzeżone**[72], w zależności od szkody, jaką mogłoby wyrządzić jej nieuprawnione ujawnienie dla Rzeczypospolitej albo byłoby z punktu widzenia jej interesów niekorzystne.

Informacjom niejawnym nadawana jest klauzula ściśle tajne, jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że[73]:

- zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;

[71] Ustawa z dnia 10 sierpnia 2010 roku o ochronie informacji niejawnych, art. 1 (Dz. U. 2010, nr 182, poz. 1228).
[72] Tamże, art. 5 (Dz. U. 2010, nr 182, poz. 1228).
[73] Tamże, s. 4.

- zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;
- zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
- osłabi gotowość obronną Rzeczypospolitej Polskiej;
- doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;
- zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze lub osób udzielających im pomocy w tym zakresie;
- zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych albo świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, z późn. zm.) lub osób dla nich najbliższych.

Informacjom niejawnym jest nadawana klauzula **tajne**, jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej przez to, że[74]:

- uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
- pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
- zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej;
- utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione;
- w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
- przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

[74] Tamże, s. 4.

Informacjom niejawnym jest nadawana klauzula **poufne**, jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej przez to, że[75]:

- utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
- utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
- zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;
- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
- zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;
- wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

Oznacza to, że w przypadku informacji niejawnych o klauzulach „ściśle tajne", „tajne" i „poufne" muszą być spełnione łącznie dwie przesłanki:

- nieuprawnione ujawnienie tych informacji musi zagrażać wymienionym (zróżnicowanym adekwatnie do klauzuli) dobrom;
- nieuprawnione ujawnienie tych informacji spowoduje dla Rzeczypospolitej Polskiej – w przypadku „ściśle tajnych" – „szkodę wyjątkowo poważną", „tajnych" – „szkodę poważną", „poufnych" – „szkodę".

Informacjom niejawnym jest natomiast nadawana klauzula **zastrzeżone**, jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej[76].

[75] Tamże, s. 4.
[76] Tamże, s. 5.

1.7. Kształtowanie bezpieczeństwa informacyjnego

Bezpieczeństwo informacyjne **można kształtować wprowadzając politykę bezpieczeństwa informacyjnego, która pozwoli zapewnić ochronę istniejących systemów, zagwarantować państwu i podmiotom, które chroni, posiadanie, przetrwanie i swobodę rozwoju „społeczeństwa informacyjnego".** Takie ujęcie bezpieczeństwa informacyjnego ma charakter pozytywny. Środki polityki bezpieczeństwa informacyjnego budowane w oparciu o ujęcie pozytywne muszą uwzględniać, że[77]:

- informacja stanowi zasób strategiczny państw, organizacji i instytucji;
- informacja i wynikająca z niej wiedza oraz technologie informatyczne staną się podstawowym czynnikiem wytwórczym;
- większość dochodu państwa, organizacji i instytucji zostanie uzyskana z szeroko rozumianego sektora informacyjnego;
- procesy decyzyjne w innych sektorach gospodarki i życia społecznego uzależnione będą od systemów przetwarzania i przesyłania informacji;
- zakłócenie prawidłowości działania systemów informacyjno-sterujących nie wymaga wysokich nakładów materialnych;
- rywalizacja pomiędzy przeciwnikami przeniesie się na płaszczyznę walki informacyjnej.

Organizacja ochrony informacji niejawnych oparta jest na kilku podstawowych zasadach, do których przestrzegania są zobowiązani adresaci ustawy. Najważniejsze zgrupowano w art. 8 ustawy stanowiącym, że informacje niejawne, którym nadano określoną klauzulę tajności:

- mogą być udostępnione wyłącznie osobie uprawnionej, zgodnie z przepisami ustawy dotyczącymi dostępu do określonej klauzuli tajności;
- muszą być przetwarzane w warunkach uniemożliwiających ich nieuprawnione ujawnienie, zgodnie z przepisami określającymi wymagania dotyczące kancelarii tajnych, bezpieczeństwa systemów teleinformatycznych, obiegu materiałów i środków bezpieczeństwa fizycznego, odpowiednich do nadanej klauzuli tajności;

[77] https://ochrona-bezpieczenstwo.pl/ochrona-informacji/prawo/846-bezpieczenstwo- informacyjne-panstwa-pozyskiwanie-informacji-i-kontroling-w-systemie-zarzadzania-kryzysowego-w-panstwie [dostęp: 27.03.2024].

- muszą być chronione, odpowiednio do nadanej klauzuli tajności, z zastosowaniem środków bezpieczeństwa określonych w ustawie i przepisach wykonawczych wydanych na jej podstawie.

Za realizację ochrony informacji niejawnych zgodnie z ustawą odpowiada kierownik jednostki organizacyjnej, a powołany przez niego **pełnomocnik ochrony** jest obowiązany do bieżącego nadzoru nad stosowaniem środków ochrony fizycznej. Przetwarzanie informacji niejawnych w jednostce organizacyjnej wiąże się ze spełnieniem wielu wymogów, jakie stawia ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Większość ciężaru tych wymogów spoczywa na Pełnomocniku ds. Ochrony Informacji Niejawnych. Jednym z tych wymogów jest opracowanie odpowiedniej dokumentacji.

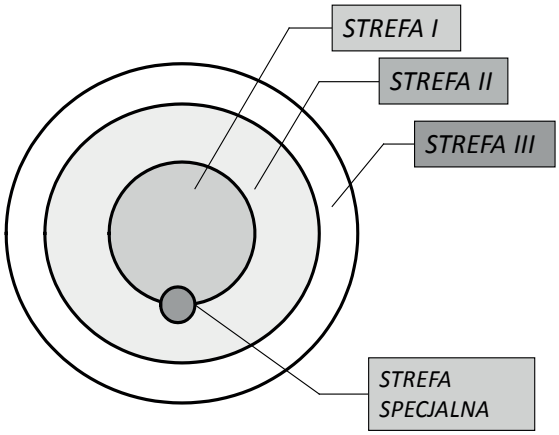
W zależności od klauzuli, Pełnomocnik ds. Ochrony Informacji Niejawnych zobowiązany jest do opracowania następującej dokumentacji:

1. **W przypadku przetwarzania informacji niejawnych oznaczonych klauzulą: poufne, tajne oraz ściśle tajne:**
   - plan ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego;
   - dokumentacja określająca poziom zagrożeń związanych z nieuprawnionym dostępem do informacji niejawnych lub ich utratą;
   - instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli poufne w podległych komórkach organizacyjnych;
   - instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli zastrzeżone w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony;
   - wykaz osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto;
   - dokumentacja bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne, tj. Szczególne Wymagania Bezpieczeństwa (SWB) oraz Procedury Bezpiecznej Eksploatacji (PBE) – jeśli występuje system teleinformatyczny.

2. **W przypadku przetwarzania informacji niejawnych oznaczonych klauzulą zastrzeżone:**
   - plan ochrony informacji niejawnych w jednostce organizacyjnej, w tym w razie wprowadzenia stanu nadzwyczajnego;
   - instrukcja dotycząca sposobu i trybu przetwarzania informacji niejawnych o klauzuli zastrzeżone w podległych komórkach organizacyjnych oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony;
   - wykaz osób zatrudnionych lub pełniących służbę w jednostce organizacyjnej albo wykonujących czynności zlecone, które posiadają uprawnienia do dostępu do informacji niejawnych, oraz osób, którym odmówiono wydania poświadczenia bezpieczeństwa lub je cofnięto;
   - dokumentacja bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne, tj. Szczególne Wymagania Bezpieczeństwa (SWB) oraz Procedury Bezpiecznej Eksploatacji (PBE) – jeśli występuje potrzeba posiadania systemu teleinformatycznego.

1.8. Zarządzanie bezpieczeństwem informacyjnym

Celem wyeliminowania lub zminimalizowania zagrożeń należy wydzielić w obiekcie obszary, które poddane będą szczególnej kontroli wejść i wyjść oraz kontroli przebywania, które zwane są strefami bezpieczeństwa. W celu bezpiecznego przetwarzania informacji niejawnych tworzy się następujące strefy ochronne (rys. 6):



Rys. 6. Strefy ochronne

Źródło: opracowanie na podstawie Rozporządzenia Rady Ministrów z dnia 20 maja 2012 r. w sprawie bezpieczeństwa fizycznego informacji niejawnych, Dz. U. z 2012 r., poz. 683.

StrefA ochronna I – obejmująca pomieszczenie lub obszar, w których informacje niejawne o klauzuli **poufne** lub wyższej są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru umożliwia uzyskanie bezpośredniego dostępu do tych informacji. Pomieszczenie lub obszar spełniają następujące wymagania:

- wyraźnie wskazana w planie ochrony najwyższa klauzula tajności przetwarzanych informacji niejawnych;
- wyraźnie określone i zabezpieczone granice;
- wprowadzony system kontroli dostępu zezwalający na wstęp osób, które posiadają odpowiednie uprawnienie do dostępu do informacji niejawnych w zakresie niezbędnym do wykonywania pracy lub pełnienia służby albo wykonywania czynności zleconych;
- wstęp możliwy jest wyłącznie ze strefy ochronnej.

Strefa ochronna II – obejmująca pomieszczenie lub obszar, w którym informacje niejawne o klauzuli **poufne lub wyższej** są przetwarzane w taki sposób, że wstęp do tego pomieszczenia lub obszaru nie umożliwia uzyskania bezpośredniego dostępu do tych informacji; pomieszczenie lub obszar spełniają następujące wymagania:

- wyraźnie określone i zabezpieczone granice;
- wprowadzony system kontroli dostępu zezwalający na wstęp osób, które posiadają odpowiednie uprawnienie do dostępu do informacji niejawnych

w zakresie niezbędnym do wykonywania pracy lub pełnienia służby albo wykonywania czynności zleconych;
- w przypadku konieczności wstępu osób innych niż te, o których mowa w poprzednim punkcie, zapewnia się nadzór osoby uprawnionej lub równoważne mechanizmy kontrolne;
- wstęp możliwy jest wyłącznie ze strefy ochronnej.

Strefa ochronna III – obejmująca pomieszczenie lub obszar wymagający wyraźnego określenia granic, w obrębie których jest możliwe kontrolowanie osób i pojazdów;
Specjalna strefa ochronna – umiejscowiona w obrębie strefy ochronnej I lub strefy ochronnej II, chroniona przed podsłuchem, spełniająca dodatkowo następujące wymagania:
- strefę wyposaża się w system sygnalizacji włamania i napadu;
- strefa pozostaje zamknięta, gdy nikogo w niej nie ma;
- w przypadku posiedzenia niejawnego strefa jest chroniona przed wstępem osób nieupoważnionych do udziału w tym posiedzeniu;
- strefa podlega regularnym inspekcjom przeprowadzanym według zaleceń Agencji Bezpieczeństwa Wewnętrznego albo Służby Kontrwywiadu Wojskowego, nie rzadziej niż raz w roku oraz po każdym nieuprawnionym wejściu do strefy lub podejrzeniu, że takie wejście mogło mieć miejsce;
- w strefie nie mogą znajdować się linie komunikacyjne, telefony, inne urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny, których umieszczenie nie zostało zaakceptowane w sposób określony w procedurach bezpieczeństwa.

Pomieszczenie lub obszar w każdej strefie ochronnej, w których praca nie odbywa się w systemie całodobowym, sprawdza się bezpośrednio po zakończeniu pracy w celu upewnienia się, że informacje niejawne zostały właściwie zabezpieczone.

Na cykl funkcjonowania systemów i sieci teleinformatycznych składa się: **planowanie, projektowanie, wdrażanie, eksploatacja i wycofanie. Planowanie** polega na definiowaniu:
- przeznaczenia systemu teleinformatycznego;
- ustaleniu maksymalnej klauzuli tajności informacji niejawnych, które mają być przetwarzane w systemie;
- trybu bezpieczeństwa pracy systemu teleinformatycznego;

- ustaleniu liczby użytkowników.

Projektowanie polega na:

- wstępnym szacowaniu ryzyka dla bezpieczeństwa informacji niejawnych w celu określenia wymagań dla bezpieczeństwa;
- wyborze zabezpieczeń dla systemu IT w oparciu o wyniki wstępnego szacowania ryzyka;
- uzgodnieniu z podmiotem akredytującym planu akredytacji obejmującym zakres i harmonogram przedsięwzięć wymaganych do uzyskania akredytacji bezpieczeństwa teleinformatycznego;
- uzgodnieniu z podmiotem zaopatrującym w klucze kryptograficzne rodzaj oraz ilość niezbędnych urządzeń lub narzędzi kryptograficznych, a także sposób ich wykorzystania;
- opracowaniu dokumentu szczególnych wymagań bezpieczeństwa.

Wdrażanie polega na:

- pozyskaniu i wdrażaniu urządzeń lub narzędzi realizujących zabezpieczenia w systemie teleinformatycznym;
- przeprowadzaniu testów bezpieczeństwa systemu teleinformatycznego;
- przeprowadzaniu szacowania ryzyka dla bezpieczeństwa informacji niejawnych z uwzględnieniem wprowadzonych zabezpieczeń;
- opracowaniu procedur bezpiecznej eksploatacji;
- system teleinformatyczny poddaje się akredytacji bezpieczeństwa teleinformatycznego[78].

Eksploatacja obejmuje:

- utrzymanie zgodności systemu teleinformatycznego z jego dokumentacją bezpieczeństwa;
- zapewnienie ciągłość procesu zarządzania ryzykiem w systemie teleinformatycznym;
- okresowo, przeprowadzenie testów bezpieczeństwa w celu weryfikacji poprawności;
- sprawdzenie poszczególnych zabezpieczeń oraz usuwanie stwierdzonych nieprawidłowości;

[78] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, §18 (Dz. U. 2011, nr 159, poz. 948).

- w zależności od potrzeb wprowadza się zmiany do systemu teleinformatycznego oraz jeżeli jest to właściwe, wykonuje testy bezpieczeństwa, a także uaktualnia dokumentację bezpieczeństwa systemu teleinformatycznego.

Wycofanie (zakończenie pracy sytemu):

- zaprzestaje się eksploatacji systemu teleinformatycznego;
- powiadamia się pisemnie ABW albo SKW o wycofaniu systemu z eksploatacji;
- zwrot do ABW albo SKW świadectwa akredytacji bezpieczeństwa systemu teleinformatycznego, jeżeli system teleinformatyczny przeznaczony był do przetwarzania informacji niejawnych o klauzuli „poufne" lub wyższej;
- usuwa się informacje niejawne z systemu teleinformatycznego, w szczególności przez przeniesienie ich do innego systemu teleinformatycznego, zarchiwizowanie lub zniszczenie informatycznych nośników danych[79].

Zarządzanie ryzykiem i analiza ryzyka są to podstawowe procesy, które muszą mieć miejsce przed etapem projektowania i budowy systemów i sieci teleinformatycznych służących do przetwarzania i przesyłania informacji niejawnych. **Zarządzanie ryzykiem** jest całkowitym procesem identyfikacji, kontrolowania i eliminacji lub ograniczenia prawdopodobieństwa zaistnienia ewentualnych zdarzeń, które mogą mieć wpływ na zasoby systemu informatycznego. Posiada kluczowe znaczenie w aspekcie bezpieczeństwa informacji i bezpieczeństwa teleinformatycznego. Pozwala za pomocą analizy ryzyka, zidentyfikować ryzyka na jakie narażone są informacje przetwarzane w systemie informatycznym, a następnie, za pomocą doboru odpowiednich zabezpieczeń, osiągnąć efektywną ochronę przed zidentyfikowanymi zagrożeniami poprzez kontrolowanie, unikanie lub minimalizowanie skutków zamierzonych lub przypadkowych ataków na system i jego zasoby. Zarządzanie ryzykiem jest procesem ciągłym, wprowadzonym już na etapie projektowania systemu i kontynuowanym podczas całego okresu życia systemu, gdzie pozwala kontrolować i minimalizować ryzyka, reagując na zmiany środowiska.

Dla zapewnienia prawidłowego funkcjonowania systemów informacyjnych należy rozpatrzyć działanie sytemu z uwzględnieniem **bezpieczeństwa elektromagnetycznego**. Ma ono na celu niedopuszczenia do utraty poufności informacji niejawnych na skutek wykorzystania elektromagnetycznej emisji ujawniającej,

[79] Tamże.

która pochodzi z elementów systemu. W systemie teleinformatycznym przetwarzającym informacje niejawne o klauzuli „poufne" lub wyższej stosuje się środki ochrony elektromagnetycznej dobierane na podstawie wyników szacowania ryzyka dla bezpieczeństwa informacji niejawnych, z uwzględnieniem zaleceń[80]. **Elektromagnetyczna emisja ujawniająca** jest to emisja, której odbiór, rejestracja a następnie analiza daje możliwość odtworzenia fragmentu przetwarzanej informacji niejawnej. Dzieli się na **elektromagnetyczną emisję promieniowania** i **przewodzącą**.

Do ochrony elektromagnetycznej systemów i sieci teleinformatycznych zastosowany może być sprzęt teleinformatyczny przystosowany do swoich zadań wg. normy TEMPEST. **Norma TEMPEST** (*temporary emanation and spurious transmission*) została nadana programowi ochrony przed niekontrolowaną emisją ujawniającą, który powstał w latach 50. w USA na zlecenie Pentagonu. Na przestrzeni lat standard ten był wielokrotnie rewidowany i publikowany pod różnymi nazwami NAG1A, FS222, NACSIM 5100, NSCD. Obecnie urządzenia klasy TEMPEST wykonywane są w trzech klasach bezpieczeństwa elektromagnetycznego, które nazywane są również poziomami:
Level I (poziom 1) – wg normy **AMSG 720 B;**
Level II (poziom 2) – wg normy **AMSG 788;**
Level III (poziom 3) – wg normy **AMSG 784**.

Kolejnym rozwiązaniem, które wpływa na ochronę informacji, jest **ochrona kryptograficzna**. Polega na zastosowaniu mechanizmów gwarantujących poufność, integralność oraz uwierzytelnienie informacji, które są przetwarzane w systemach lub sieciach teleinformatycznych. Siła mechanizmów kryptograficznych musi być odpowiednia do klauzuli informacji niejawnych. Kryptografia zostanie szczegółowo opisana w dalszej części monografii.

1.9. Ocena poziomu analizowanego bezpieczeństwa informacyjnego

Rozważając pojęcia bezpieczeństwa informacyjnego, bezpieczeństwa informacji, bezpieczeństwa informacji niejawnych oraz bezpieczeństwa systemów i sieci teleinformatycznych, należy zdawać sobie sprawę ze stosunku tych pojęć do siebie. Czy bezpieczeństwo informacyjne jest pojęciem szerszym niż

[80] Tamże.

bezpieczeństwo informacji? Czy może pojęcia te są równoznaczne? Czy bezpieczeństwo teleinformatyczne zawiera się w bezpieczeństwie informacji, czy może jest od niego niezależne? Czy można mówić o bezpieczeństwie informacji, z pominięciem bezpieczeństwa teleinformatycznego?

Bezpieczeństwo informacji obejmuje ochronę wszelkich form wymiany, przechowywania i przekazywania danych – dokumentów papierowych, plików danych, informacji zawartych w głowach pracowników przekazywanych podczas rozmów, telefonicznie, faksem, itp. W tym określeniu zawiera się także **bezpieczeństwo informacji niejawnych** jako specyficznego rodzaju informacji podlegającej szczególnej ochronie ze względu na zawarte w nich treści określone w ustawie o ochronie informacji niejawnych.

Z kolei **bezpieczeństwo teleinformatyczne** obejmuje formy wymiany, przechowywania i przetwarzania danych w postaci elektronicznej z wykorzystaniem technicznych środków teleinformatycznych oraz sieci teleinformatycznych. Bezpieczeństwo teleinformatyczne – oznacza poziom uzasadnionego zaufania i pewności, że potencjalne straty wynikające z niepożądanego - przypadkowego lub świadomego – ujawnienia modyfikacji, zniszczenia lub uniemożliwienia przetwarzania danych przechowywanych lub przetwarzanych za pomocą systemów teleinformatycznych nie zostaną poniesione.

Bezpieczeństwo to z jednej strony stan, jaki chcemy zapewnić systemom i sieciom, z drugiej strony proces. Osiągnięcie pewnego poziomu bezpieczeństwa systemów i sieci nie oznacza, że będą one już raz na zawsze bezpieczne. Dlatego cykliczne prowadzenie audytów systemów i sieci informatycznych przeprowadzane są w celu stworzenia bezpiecznego, niezawodnego systemu informatycznego w instytucji, organizacji, firmie czy przedsiębiorstwie. Audyt systemów informatycznych polega na zapoznaniu się ze wszystkimi zasobami audytowanych, wskazaniu słabych punktów i popełnianych błędów, a także potencjalnych zagrożeń. Zadaniem audytora jest także zabezpieczenie systemu oraz przygotowanie wskazówek dotyczących skutecznego działania w przypadku wystąpienia zagrożenia. Audyt informatyczny ma dostarczyć wiedzy na temat prawidłowego funkcjonowania systemu informatycznego, jego ochrony, podejmowania działań naprawczych[81].

Określenia jakościowych kryteriów informacyjnych znajduje swój wyraz w najbardziej obecnie rozbudowanym modelu audytu systemów informacyjnych

[81] https://magazynprzedsiebiorcy.pl/audyty-it [dostęp: 15.02.2024].

Ten bardzo szczegółowy, biznesowo i procesowo zorientowany model zarządzania sferą technologii informacyjnych, w pierwszym kroku definiuje następujące, częściowo zachodzące na siebie kryteria, jakie ma spełniać dostarczana informacja: efektywność, wydajność, poufność, integralność, dostępność, zgodność, wiarygodność.

W dobie społeczeństwa informacyjnego każda organizacja musi dbać o zabezpieczenie swoich aktywów, jakimi są m.in. informacje. Szczególnie dotyczy to organizacji, w których systemach przetwarza się informacje niejawne w rozumieniu ustawy o ochronie informacji niejawnych. Bezpieczeństwo informacji jest tematem złożonym, zależy od wielu czynników.

Do najistotniejszych, od których zależy, możemy zaliczyć:

- umiejętne zarządzanie bezpieczeństwem poszczególnych rodzajów informacji;
- odpowiednio dobrane rozwiązania techniczne, dzięki którym można zapewnić bezpieczeństwo systemów i sieci teleinformatycznych;
- zdefiniowanie zasad bezpiecznego przetwarzania informacji;
- szkolenia i poziom świadomości pracowników dopuszczonych do przetwarzania informacji;
- monitorowanie aktualnego stanu bezpieczeństwa (np. próby włamań do systemu – rejestr incydentów).

Zapewnienie bezpieczeństwa informacji nie jest aktem jednorazowym polegającym na wdrożeniu zabezpieczeń. Bezpieczeństwo jest dynamicznym procesem wymagającym stałego nadzoru i przystosowania do zmieniających się warunków otoczenia.

2. ZAPEWNIENIE BEZPIECZEŃSTWA INFORMACYJNEGO

2.1. Sposoby pozyskania informacji - elementy wojny informacyjnej

Znajomość sposobów pozyskania informacji stanowiących element **wojny informacyjnej** powoduje, że możemy ją zarówno sprawnie prowadzić, jak i skutecznie jej zapobiegać.

Wojną informacyjną nazywamy działania, których celem jest zdobycie lub wykorzystanie środków informatycznych. Zasoby te można podzielić, w zależności od ich funkcji, na pięć klas: pojemniki, transpondery, czujniki, rejestratory i procesory.

Infrastrukturę informacyjną stanowią zasoby informacyjne, włącznie z systemami komunikacji, które działają w przemyśle, różnych instytucjach lub którymi posługują się ludzie[82].

Przestrzeń informacyjna to zorganizowane wszystkie zasoby informacyjne dostępne dla danej jednostki. Z reguły będą to pracownicy, drukowane dokumenty, systemy komputerowe i komunikacyjne oraz wszystkie informacje strukturalne zakodowane w fizycznym środowisku danej organizacji, instytucji czy firmy. Cyberprzestrzeń (ang. *cyberspace*) jest to przestrzeń informacji, którą tworzą łącznie wszystkie sieci komputerowe[83].

[82] https://pl.wikipedia.org/wiki/Infrastruktura_informatyczna [dostęp: 27.03.2024].
[83] Tamże, s. 25.

Walka informacyjna jest szczególnym przypadkiem procesu sterowania społecznego, gospodarczego, których celem jest niszczenie przeciwnika za pomocą informacji[84].

Informacja niszcząca, która jest narzędziem walki informacyjnej, spełnia dwojakie funkcje[85]:

- **osłabia strukturę przeciwnika** – przede wszystkim utrudniając przekaz informacji między jego kierownictwem i wykonawcami;
- **inspiruje błędne decyzje kierownictwa i błędne działania wykonawców przeciwnika** – inaczej mówiąc, wprowadza do systemu przeciwnika błędne algorytmy decyzyjne i właściwe algorytmy działania, które go osłabiają, a nawet w pewnych wypadkach mogą doprowadzić go do samozniszczenia.

Manipulacja (łac. *manipulatio* – manewr, fortel, podstęp)[86] jest jedną z podstawowych metod stosowanych w walce informacyjnej, polegającą na wywieraniu wpływu na społeczeństwo i gospodarkę. Stosując manipulacje zmierzamy do osiągnięcia określonych celów. Zazwyczaj osoba lub grupa ludzi poddana manipulacji nie jest świadoma środków, przy użyciu których wywierany jest na nią wpływ. Autor manipulacji dąży do osiągnięcia korzyści osobistych, ekonomicznych lub politycznych kosztem innych osób.

Jednym z głównych narzędzi walki informacyjnej jest **propaganda** (od łac. *propagare* – rozszerzać, rozciągać, krzewić)[87], rozumiana jako planowe oddziaływanie na psychikę ludzi za pomocą rozpowszechnianych w skali masowej bodźców o charakterze informacyjnym, zmierzające do ukształtowania u nich odpowiednich norm społecznych lub spowodowania odpowiednich zachowań. Polega na manipulacji intelektualnej i emocjonalnej (czasem z użyciem jednostronnych, etycznie niewłaściwych lub nawet całkowicie fałszywych, argumentów).

Drugim równie skutecznym narzędziem walki informacyjnej jest **wywiad**[88]**.** W skali państwa wywiad to jeden ze sposobów rozpoznania strategicznego, polegający na zbieraniu najważniejszych wiadomości politycznych, wojskowych i gospodarczych.

Do obrony przed działaniami wywiadowczymi przeciwnika służy **kontrwywiad**. Wywiad i kontrwywiad nazywane bywają łącznie **służbami specjalnymi**.

---

84 http://www.awronka.nazwa.pl/bazya/wojnainfor.htm [dostęp: 15.01.2023].
85 Tamże.
86 http://pl.wikipedia.org/wiki/Manipulacja_(psychologia) [dostęp: 27.03.2024].
87 http://pl.wikipedia.org/wiki/Propaganda [dostęp: 27.03.2024].
88 http://pl.wikipedia.org/wiki/Wywiad_(instytucja) [dostęp: 27.03.2024].

Instytucja wywiadowcza (**wywiad**)[89] – służba specjalna zajmująca się pozyskiwaniem (często niejawnych) informacji oraz ich przetwarzaniem, przechowywaniem, analizą tych informacji i przekazywaniem ich zleceniodawcy. Służba wywiadowcza realizuje poza zadaniami o charakterze informacyjnym także zadania o charakterze sprawczym. Taka instytucja poza granicami państwa wykonuje politykę rządu. Politykę zagraniczną rządu może wykonywać w sposób legalny, nielegalny, a także poprzez dyplomację. Czyni to wpływając (także w sposób brutalny) na osoby mające wpływ na działalność, która jest ważna dla rządu, dla interesu państwa.

W skali państwa wywiad to jeden ze sposobów rozpoznania strategicznego, polegający na zbieraniu najważniejszych wiadomości politycznych, wojskowych i gospodarczych. Współcześnie, dzięki takim zdobyczom techniki jak podsłuch satelitarny, działalność wywiadowczą można również prowadzić nie opuszczając terytorium własnego państwa[90].

Oprócz wywiadu państwowego istnieje też **wywiad gospodarczy**. Wywiad gospodarczy organizowany jest przez przedsiębiorstwa zainteresowane pozyskiwaniem informacji o konkurencyjnych przedsiębiorstwach i skutecznym lobbingiem[91]. Realizowany jest przez wyspecjalizowaną i odpowiednio zorganizowaną służbę (nierzadko przez byłych funkcjonariuszy bądź żołnierzy wywiadu lub kontrwywiadu), której zadaniem jest zbieranie informacji o przeciwniku, przedsiębiorstwach strategicznych i prowadzenie walki informacyjnej.

Można też wyróżnić: **szpiegostwo gospodarcze i szpiegostwo przemysłowe**. **Szpiegostwo gospodarcze** obejmuje rządowe operacje wywiadowcze, których celem jest zdobycie tajemnic gospodarczych danego kraju. Do tajemnic tych należą także informacje o polityce i tajemnice handlowe firm tego kraju[92]. **Szpiegostwo przemysłowe** to operacje prowadzone przez jakąś korporację przeciw innej w celu uzyskania przewagi konkurencyjnej na rynkach krajowych czy zagranicznych[93].

Wywiad możemy podzielić na dwa podstawowe rodzaje:

- wywiad **biały** – który zajmuje się pozyskiwaniem i analizą informacji jawnych;

[89] Tamże.
[90] Tamże.
[91] Tamże.
[92] D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, WNT, Warszawa 2002, s. 154.
[93] Tamże, s. 157.

- wywiad **czarny** – który zajmuje się pozyskiwaniem (nielegalnym) informacji niejawnych (prawnie chronionych).

Z kolei **wywiad państwowy możemy po**dzielić na: **polityczny, ekonomiczny, wojskowy i naukowy**[94]**:**

- **polityczny** – obszary zainteresowania: ukształtowanie partii, organizacji społecznych, administracji samorządowej i rządowej, ich programy, cele, struktura, kierownictwo, mniejszości narodowe, społeczności niezasymilowane, podatność na propagandę, grupy opozycyjne;
- **ekonomiczny** – obszary zainteresowania: potencjał gospodarczy państwa, zasoby surowców, ustalanie i analiza słabych ogniw w ekonomice, analiza możliwości wpływu na tę przestrzeń;
- **wojskowy** – obszary zainteresowania: struktura, kadry sił zbrojnych, ruchy wojsk, stan i proces modernizacji, osiągnięcia naukowe w dziedzinie obronności, morale żołnierzy; zbiera wszelkie informacje dotyczące bezpieczeństwa obronnego danego państwa;
- **naukowy** – analizuje wszystko, co wiąże się z rozwojem naukowo-technicznym.

Ze względu na formy pozyskiwania informacji możemy wyróżnić wywiad:

- **agenturalny** – źródłem informacji są ludzie, czyli sieć agentów, którzy samodzielnie pozyskują informacje, do których mają dostęp;
- **technikami operacyjnymi** – bezpośrednie obserwowanie, śledzenie wybranych osób, wymuszanie zeznań, porwania, szantażowanie itp.;
- **elektroniczny** – prowadzony technikami używania i nasłuchu fal radiowych, pozostałego pasma fal elektromagnetycznych na platformach morskiej, lotniczej, lądowej, kosmicznej obserwacji satelitarnej, z wykorzystaniem specjalistów od telekomunikacji, sieci komputerowych i urządzeń wykorzystujących informatykę.

Kanały sterownicze oddziałujące na strukturę przeciwnika w procesach walki informacyjnej dzielimy na[95]:

- **agenturalne**, które są zobowiązane wykonywać wszystkie polecenia ośrodka kierującego walką informacyjną;

[94] https://pl.wikipedia.org/wiki/Wywiad [dostęp: 12.04.2024].

[95] J. Kosecki, *Elementy wojny informacyjnej*, https://www.bing.com/search?q=Kossecki%2c+Elementy+wojny+informacyjnej&FORM=AWRE [dostęp: 12.04.2024].

- **współpracujące**, które wykonują tylko te decyzje ośrodka kierującego walką informacyjną, które są zgodne z ich własnymi celami;
- **inspiracyjne**, które nieświadomie, lub nie całkiem świadomie, wykonują decyzje ośrodka kierującego walką informacyjną, wprowadzając do systemu przeciwnika algorytmy decyzji i działań sprzecznych z jego interesami.

Niezależnie od podanego wyżej podziału, możemy zastosować nieco inny, dzieląc kanały sterownicze oddziałujące na strukturę przeciwnika w procesach walki informacyjnej na:

- **kanały informacyjne**, których zadaniem jest zbieranie i przekazywanie do centrali kierującej walką odpowiednich informacji (o przeciwniku i jego otoczeniu);
- **kanały sterowniczo-dywersyjne**, których zadaniem jest wywieranie wpływu na system przeciwnika (inspirowanie i blokowanie decyzji i działań).

Obydwa rodzaje wymienionych wyżej kanałów mogą być **tajne** lub **jawne**.

W walce informacyjnej przeciw wszelkim zorganizowanym strukturom, zwłaszcza zaś przeciw państwom, są stosowane następujące metody[96]:

- **wzmacnianie centralizacji decyzji u przeciwnika**, przy równoczesnym osłabianiu powiązań poziomych między elementami jego organizacji;
- **inspirowanie błędnej polityki kadrowej u przeciwnika**, zwłaszcza w obrębie jego centrali (struktur decyzyjnych);
- **penetracja centralnego ośrodka decyzyjnego przeciwnika** i rozbudowa kanałów wpływu na ten ośrodek;
- **inspirowanie nadmiaru decyzji** lub inspirowanie błędnych decyzji podejmowanych przez centralne kierownictwo przeciwnika;
- **wprowadzenie do centralnego ośrodka decyzyjnego mechanizmów umożliwiających:** demoralizację, dezinformację, szerzenie indyferentyzmu ideologicznego, braku poszanowania prawa;
- **blokowanie i dezorganizowanie** systemu przepływu oraz przetwarzania;
- **nasyłanie masowej agentury**, która jest łatwo wykrywana i daje zajęcie jego organom kontrwywiadu, odwracając uwagę tych organów od głównych kanałów wpływu, które oddziałują na centralny ośrodek decyzyjny przeciwnika;

[96] Tamże.

- **przechwytywanie dobrych inicjatyw kierownictwa przeciwnika** przez odpowiednie kanały informacyjne i kanały wpływu oraz wypaczanie ich w taki sposób, by stawały się własną karykaturą, zniechęcającą do niej społeczeństwo.

Poszczególne metody są stosowane w walce informacyjnej między państwami, a także w walce politycznej między partiami i obozami politycznymi, mogą też być stosowane w walce z przestępczością zorganizowaną i **gospodarczą (wojnie handlowo-gospodarczej)**. Wojny handlowo-gospodarcze mogą być częścią totalnej wojny informacyjnej i wykorzystywać całe spektrum możliwości, jakie niesie za sobą nowoczesny system informacyjny. W wojnach informacyjnych obezwładnia się przeciwnika informacją – działaniami wywiadu, agentury, propagandą i manipulacją, a potem bierze się go w poddaństwo[97]. We współczesnej totalnej wojnie informacyjnej celem działań niszczących może być człowiek, gospodarka, struktury społeczne, nauka, kultura i właściwie każda dziedzina życia społecznego.

Wojna psychologiczna jest zastosowaniem przeciwko nieprzyjacielowi propagandy łącznie z takimi środkami natury wojskowej, ekonomicznej czy politycznej, jakie potrzebne są dla jej uzupełnienia[98]. Zadaniem jej jest wywieranie wpływu na psychikę przeciwnika w celu obniżenia jego morale i doprowadzenia go do stanu uniemożliwiającego kontynuowanie walki.

Wojna psychologiczna jest to planowe stosowanie propagandy oraz takich środków jak: dywersja, prowokacja, wywiad, szpiegostwo, mających na celu demoralizację przeciwnika, osłabienie jego woli walki i wiary we własną sprawę, szerzenie paniki, fałszowanie informacji itp.[99], tak, aby pomóc w realizowaniu polityki państwa i jego celów oraz zadań wojskowych.

W rosyjskiej terminologii pod pojęciem **„wojna informacyjna" rozumie się oddziaływanie na masową świadomość w międzypaństwowej rywalizacji systemów cywilizacyjnych w przestrzeni informacyjnej, wykorzystujące szczególne sposoby kontroli nad zasobami informacyjnymi, a używane w charakterze „broni informacyjnej"**. Daje się tutaj zauważyć połączenie porządku militarnego z pozamilitarnym, a technologicznego (**cyberprzestrzeń**)

[97] http://pl.wikipedia.org/wiki/Wojna [dostęp: 10.04.2024].
[98] P.M.A. Linebarger, *Wojna psychologiczna*, Archiwum Przekładów i Opracowań [RSW Prasa] Warszawa 1959, s. 5.
[99] M. Wrzosek, Operacje w cyberprzestrzeni. Założenia teoretyczne i praktyka. Wyd. Bellona 2016; 687 (4): 42-59.

ze społecznym (**przestrzeń informacyjna**)[100]. Pojęcie wojny informacyjnej umieszczane jest najczęściej w dwóch kontekstach wynikających z:

- zadań wynikających z „Doktryny bezpieczeństwa informacyjnego Federacji Rosyjskiej";
- geopolitycznej rywalizacji Rosji z Zachodem (przede wszystkim USA i NATO), mającej w efekcie wymiar polityczny, ideologiczny i kulturowy.

Wymiar technologiczny jest marginalizowany i wypierany z przestrzeni publicznej. Świadczy o tym prowadzona w latach 2012-2013 debata na temat projektu **Strategii cyberbezpieczeństwa,** zgłoszonego przez Rusłana Gattarowa[101]. Strategię tę specjaliści z Rady Bezpieczeństwa i służb specjalnych Rosji ocenili jako nazbyt zawężającą problematykę bezpieczeństwa informacyjnego. Bezpieczeństwo cyberprzestrzeni jest traktowane jako pojęcie cząstkowe, choć podkreśla się, że nowe technologie poszerzyły arsenał środków oddziaływania informacyjnego na opinię publiczną. Słabo obecny w przestrzeni publicznej aspekt technologiczny (cyber-) jest chroniony tajemnicą państwową.

W doktrynie geopolityki informacja stanowi niebezpieczny oręż (jest to zarazem broń o niskich kosztach, broń uniwersalna, o nieograniczonym zasięgu, łatwo dostępna, bez barier w postaci granic państwowych). Walka informacyjna i sieciowa (częściej walka informacyjno-psychologiczna) i skrajne jej formy – wojny informacyjno-psychologiczne i sieciowe – są środkiem do osiągania celów państwa w polityce międzynarodowej, regionalnej i wewnętrznej, a także jego geopolitycznej przewagi[102].

Z kolei profesor Panarin[103] w opracowaniu *Druga światowa wojna informacyjna – wojna przeciwko Rosji (Вторая мировая информационная война – война*

[100] J. Darczewska, *Anatomia rosyjskiej wojny Informacyjnej. Operacja krymska – studium przypadku*, „Punkt Widzenia" 2014, nr 42, OSW, s. 12.

[101] Rusłan Gattarow (ur. 1977) – działacz Młodzieżowej Gwardii partii Jedna Rosja, a następnie przewodniczący czelabińskiego komitetu tej partii. Od 2010 roku senator, przewodniczący komitetu ds. społeczeństwa informacyjnego przy Radzie Federacji oraz przewodniczący Rady ds. Pracy z Blogosferą, którą powołano przy prezydium partii Jedna Rosja. W lutym 2014 roku złożył mandat senatora Rady Federacji, a następnie został mianowany wicegubernatorem obwodu czelabińskiego.

[102] J. Darczewska, *Anatomia rosyjskiej wojny Informacyjnej. Operacja krymska – studium przypadku*, „Punkt Widzenia" 2014, nr 42, OSW, s. 13.

[103] Igor Panarin (ur. 1958) – dr hab. nauk politologicznych, dr psychologii, członek rzeczywisty Akademii Nauk Wojskowych Federacji Rosyjskiej i licznych ciał eksperckich przy Prezydencie i Radzie Federacji. Karierę zawodową rozpoczął w KGB ZSRR w 1976 roku. Po roku 1991 pracował w FAPSI; w latach 1999-2003 był szefem wydziału analitycznego Centralnej Komisji Wyborczej. Obecnie jest profesorem Akademii Dyplomatycznej MSZ FR; wykłada także w MGIMO i Rosyjskiej Akademii Służby Państwowej przy Prezydencie.

против Россиии (2012)) przedstawia podstawowe pojęcia z zakresu technologii wojen informacyjnych, będących w praktyce operacjami wpływu, takimi jak:

- **sterowanie społeczne**, tj. wywieranie wpływu na społeczeństwo;
- **manewrowanie społeczne**, czyli intencjonalne sterowanie społeczeństwem dla osiągnięcia określonych korzyści;
- **manipulacja informacją**, czyli wykorzystywanie prawdziwych informacji w sposób wywołujący fałszywe implikacje;
- **dezinformacja**, czyli rozpowszechnianie zmanipulowanych lub sfabrykowanych informacji bądź ich kombinacji;
- **fabrykowanie informacji**, czyli tworzenie fałszywej informacji;
- **lobbing**, **szantaż** i **wymuszanie pożądanej informacji**.

Z opracowań Panarina wyłania się także **zarys podstawowych narzędzi walki informacyjnej, które dzieli on na tajne i jawne**. Zalicza do nich:

- **propagandę** (czarna, szara i biała);
- **wywiad** (służba zbierająca informacje o przeciwniku);
- **komponent analityczny** (monitoring mediów i bieżąca analiza sytuacyjna);
- **komponent organizacyjny** (kanały koordynacyjne i sterownicze, agentura wpływu w mediach, wykorzystywana do urabiania opinii polityków i środków masowego przekazu w kierunku przychylnym dla państwa prowadzącego wojnę informacyjną;
- **inne kanały sprzężone**, w tym siły operacji specjalnych (operacji dywersji prowadzonych pod obcą banderą).

Organizacyjnymi formami wojen informacyjnych są skomplikowane operacje, zarządzane z jednego centrum, które autor nazywa „informacyjnym KGB". Są one realizowane przez „informacyjne *specnazy*"[104].

W **procesie zarządzania operacjami informacyjnymi** Panarin wyróżnia następujące etapy:

- prognozowanie i planowanie;
- organizacja i stymulowanie;
- sprzężenie zwrotne (informacja zwrotna);
- korygowanie operacji;
- kontrola wykonania.

[104] J. Darczewska, *Anatomia rosyjskiej wojny Informacyjnej. Operacja krymska – studium przypadku*, „Punkt Widzenia" 2014, nr 42, OSW, s. 15-16.

Narodowy system walki informacyjnej, polegający na jawnym i tajnym sterowaniu procesami komunikacyjnymi, musi być adekwatny do współczesnych realiów globalnych. Oparty na najlepszych doświadczeniach ZSRR, winien być wzbogacony o doświadczenia USA i Chin[105].

W wielu miejscach na świecie oprócz walki informacyjnej prowadzona jest również **walka energetyczna**, która polega na niszczeniu przeciwnika za pomocą energomaterii.

Także walka ekonomiczna jest mieszanką walki informacyjnej, wchodzi w zakres działalności wywiadu i kontrwywiadu, obejmuje zdobywanie tajemnic gospodarczych przeciwnika, ochronę własnych tajemnic oraz prowadzenie walki energetycznej, która polega m.in. na używaniu energomaterii skumulowanej i przetwarzanej przez własną gospodarkę do niszczenia struktury przeciwnika. Walka energetyczna i walka informacyjna od dawna uzupełniały i wspomagały się wzajemnie. Od czasu jednak, gdy po II wojnie światowej dwa walczące ze sobą o panowanie nad światem obozy zgromadziły tak wielkie środki niszczenia energetycznego (zarówno klasyczne, jak i nuklearne), że ewentualny konflikt zbrojny mógłby grozić zagładą całej ludzkości, coraz większe znaczenie zyskiwała **totalna wojna informacyjna**, której zasadniczą cechą jest ścisłe sprzężenie działań propagandy, wywiadu i kontrwywiadu z walką ekonomiczną i wyścigiem zbrojeń.

W XX wieku wojnę informacyjną zaczęto szeroko stosować jako autonomiczną metodę walki, która w pewnych warunkach odgrywać może rolę wiodącą, prowadząc do rozstrzygnięć decydujących (przynajmniej na określonym etapie walki), zaś walka energetyczna – zarówno ekonomiczna jak i militarna – mają za zadanie tylko wesprzeć operacje z zakresu walki informacyjnej. W ten sposób powstała **totalna wojna informacyjna**.

Wojnę handlowo-gospodarczą możemy określić jako zespół działań militarnych i niewojskowych (ekonomicznych, administracyjnych, dyplomatycznych), skierowanych na osłabienie bądź też dezorganizację potencjału gospodarczo-obronnego innego państwa (grupy państw), a jej powodem są czynniki polityczne. Jest to środek nacisku, przymusu bądź odwetu. Takie niemilitarne oddziaływanie jest dopuszczone przez prawo międzynarodowe, szeroko stosowane w stosunkach międzynarodowych w świecie. Może też stanowić część

[105] Wojna informacyjna i komunikacje (*Презентация книги Панарина Информационная война и коммуникации*) https://ria.ru/20140303/997906409 .html [dostęp:10.04.2021].

składową ogólnej polityki zagranicznej państwa (koalicji, sojuszu). Aby była skuteczna potrzebny jest zazwyczaj długi przedział czasowy. Tego typu wojna może zapobiegać lub powstrzymać pewne zagrożenie, w sposób mniej kosztowny aniżeli groźba militarnej konfrontacji, czy też prawdopodobieństwo jej wystąpienia.

Sankcje gospodarcze (**sankcje ekonomiczne**) to kary nałożone na gospodarkę jednego lub kilku krajów przez inne państwa. Sankcje mogą obejmować[106]:

- cła (opłaty za przewóz dóbr);
- embarga (zakaz przewozu dóbr);
- kontyngenty wwozowe lub wywozowe (zakaz przewozu dóbr);
- ograniczenia monetarne (blokowanie kont bankowych, zakaz przewozu waluty).

Sankcje gospodarcze są ważnym narzędziem polityki ONZ. Jeżeli jakiś kraj łamie prawo międzynarodowe, Rada Bezpieczeństwa ONZ może wydać rezolucję o nałożeniu na to państwo sankcji ekonomicznych.

2.2. Analiza wybranych mechanizmów wojny informacyjnej, cyberterroryzmu i przestępczości komputerowej

Komunikacja, w tym **informacja**, napędza całą naszą cywilizację i wytycza jej kierunki rozwoju. Jest podstawą funkcjonowania wszystkich organizmów i organizacji. Co więcej, dziś informacja zaczyna żyć swoim życiem, znajdując dla siebie lepsze środowisko niż ludzki mózg – **procesor** i pamięć komputera. W inteligentnych domach, w których komputery gromadzą informacje o naszych nawykach i dostosowują do nich domowe urządzenia, żyje się nam coraz lepiej i przyjemniej, ale czy bezpieczniej? Czy mechanizmy zabezpieczeń (w tym prawne), jakie stosujemy w cyberprzestrzeni, pozwalają z optymizmem patrzyć w przyszłość?

Pierwszym konfliktem toczącym się w sieci była wojna w Kosowie, która – zdaniem specjalistów – zamieniła cyberprzestrzeń w miejsce (strefę) wojny, prowadzonej za pomocą elektronicznych obrazków, grup dyskusyjnych oraz hakerskich ataków; zapoczątkowała nową erę, w której wysoce skomplikowane nowoczesne środki przekazu stały się elementami wojennej propagandy.

[106] http://pl.wikipedia.org/wiki/Sankcje_gospodarcze [dostęp: 10.04.2024].

W praktyce działalność w cyberprzestrzeni najczęściej prowadzą hakerzy. **Haker** (ang. *hacker*) to osoba o dużych, praktycznych umiejętnościach informatycznych (lub elektronicznych), identyfikująca się ze społecznością hackerską. Hakerzy odznaczają się bardzo dobrą orientacją w Internecie, znajomością wielu języków programowania, a także świetną znajomością systemów operacyjnych, w tym zwłaszcza z rodziny **Unix (GNU/Linux, BSD** itp.), oraz świetnie rozwiązują problemy związane z bezpieczeństwem systemów. Szukają dziur w systemach i programach komputerowych, niekoniecznie w celu czerpania z nich zysków.

Znaczenie słowa „**haker**" w masowych mediach jest inne niż stosowane przez społeczność hackerską. Media powszechnie używają go wobec osób łamiących zabezpieczenia systemów komputerowych, co w słownictwie informatycznym określa się mianem „**crackingu**", a osoby łamiące te zabezpieczenia mianem „**crackerów**". Określanie **crackerów** mianem hakerów jest bardzo źle widziane w środowisku, gdyż etyka hackerska sprzeciwia się cyberprzestępczości. **Crackingiem** zajmują się również osoby bez hackerskich umiejętności, używające gotowych programów do łamania zabezpieczeń[107].

Cracking to dziedzina informatyki zajmująca się łamaniem zabezpieczeń oprogramowania. Jest niemal zawsze realizowany z naruszeniem praw autorskich, a tym samym nielegalnie. Zasadniczo wyróżnia się dwa typy crackingu:

- **cracking sieciowy**, czyli łamanie zabezpieczeń komputerów w sieciach komputerowych;
- **cracking oprogramowania**, czyli łamanie zabezpieczeń przed niedozwolonym użytkowaniem programów.

Złośliwe oprogramowanie (z ang. *malicious software*) – wszelkie aplikacje, skrypty itp. mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera. Do złośliwego oprogramowania należą:

- **Wirusy** potrafią zrobić najwięcej spustoszenia i zainfekować oraz unieruchomić pracę tysięcy komputerów. Wirus to samoreprodukujący się kod, który uszkadza dane, programy, a niektóre jego odmiany mogą nawet zniszczyć komputer. Jest on zazwyczaj obcym fragmentem wrogiego wykonalnego kodu dołączanym do programu, który dołącza się, nadpisuje lub zamienia inny program w celu reprodukcji samego siebie bez zgody użytkownika. Jego uruchomienie powoduje dołączenie go do innych „zdrowych"

[107] http://pl.wikipedia.org/wiki/Haker_(slang_komputerowy) [dostęp: 10.04.2024].

programów zainstalowanych na komputerze. Działa on kaskadowo, zarażając kolejne niezainfekowane programy. Obecnie funkcjonuje wiele odmian wirusów, liczonych w setkach tysięcy. Praktycznie codziennie pojawia się jego nowa odmiana.

- Ze względu na różne rodzaje infekcji wirusy dzielą się na[108]:
  - ✓ wirusy gnieżdżące się w sektorze rozruchowym twardego dysku;
  - ✓ wirusy pasożytnicze;
  - ✓ wirusy wieloczęściowe;
  - ✓ wirusy towarzyszące;
  - ✓ Makrowirusy.
- **Robak** to inny rodzaj wirusów**.** Jest to złośliwe oprogramowanie podobne do wirusów, rozmnażające się tylko przez sieć. W przeciwieństwie do wirusów nie potrzebują programu „żywiciela". Robak może zachowywać się jak wirus, koń trojański lub bakteria. Działa on w sieci jak potencjalny hacker, lecz jego atak nie musi być koordynowany przez niego. Wyszukuje on słabe strony w poczcie elektronicznej, stronach internetowych czy popularnych chatach i infekuje się na kolejnych komputerach.
- **Bakteria** jest programem, którego zadaniem jest rozmnażanie się na zaatakowanym komputerze. Typowa bakteria na początku dzieli się na dwie kopie, instalując się w środowisku zasobów danych. Następnie ulega kolejnemu rozmnażaniu, przez co zajmuję pamięć w komputerze i uniemożliwia jego pracę.
- **Bomba logiczna** to rodzaj wirusa komputerowego, który po zainstalowaniu się na danym komputerze może przez dłuższy czas pozostawać nieaktywny. Aktywuje go obecność określonych plików, określona data lub uruchamiana przez użytkownika określona aplikacja.
- **E-mail bombing** polega na zapchaniu danego serwera pocztowego ogromną liczbą wiadomości, wysyłanych z wielu miejsc w tym samym czasie do adresata. Skrzynka ofiary ulega wypełnieniu, przez co nie może on odczytać wiadomości, która faktycznie miała do niego dotrzeć. Cyberprzestępcy programują tak komputery, aby wysyłały one nieustannie ogromne ilości maili na konto pocztowe ofiary.
- **Koń trojański**, częściej nazywany „trojan" lub „trojan horse", jest jednym z najgroźniejszych programów używanych przez cyberprzestepców. Po

[108] http://pl.wikipedia.org/wiki/Z%C5%82o%C5%9Bliwe_oprogramowanie [dostęp: 11.04.2024].

zainfekowaniu systemu dokonuje nieprzewidywalnych działań w komputerze. Może usunąć określone pliki lub wszystkie dane z twardego dysku komputera. Potrafi sam zainicjować procedurę formatowania lub przesłać dane do swojego twórcy. Trojona można dołączyć do każdego oprogramowania. Najprostszym sposobem jego rozpowszechniania jest poczta elektroniczna lub wejście na zainfekowaną stronę internetową. Konie trojańskie służą także do wyłapywania haseł. Sytuacja taka następuje, gdy cyberprzestępca zastępuje standardowy program rejestrujący się na komputerze wersją z trojanem. Użytkownik, nie zdając sobie sprawy z zagrożenia, loguje się do systemu, a w między czasie jego hasło przechwytywane jest przez program z koniem trojańskim. Metoda ta jest często łączona z spoofingiem i stosowana przez cyberprzestępców do przechwytywania haseł dostępu do kont bankowych.

- **Wabbit** – program rezydentny nie powielający się przez sieć. Wynikiem jego działania jest jedna określona operacja, np. powielanie tego samego pliku aż do wyczerpania zasobów pamięci komputera;
- **Trojan** – nie rozmnaża się jak wirus, ale jego działanie jest równie szkodliwe. Ukrywa się pod nazwą lub w części pliku, który użytkownikowi wydaje się pomocny. Oprócz właściwego działania pliku zgodnego z jego nazwą, trojan wykonuje operacje w tle szkodliwe dla użytkownika, np. otwiera port komputera, przez który może być dokonany atak włamywacza (hakera);
- **Phishing** – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.
- **Spoofing** czyli fałszowanie adresów IP, mające na celu udawanie serwera w istniejącym połączeniu sieciowym. Technika ta ma na celu uniknięcie zabezpieczeń, jakie wprowadzają na danym serwerze administratorzy sieci wewnętrznej oraz „podszycie" się pod użytkownika sieci, co umożliwia atakującemu przechwytywanie wszystkich danych, które miały trafić do prawdziwego komputera.
- **Sniffing** to oszustwo polegające na monitorowaniu przepływu informacji w sieci i (opcjonalnie) analizowaniu tych informacji. Atak polega na tym, że nie odgaduje się numerów IP, tylko potencjalny cyberprzestępca uzyskuje dostęp do sieci wymuszając zaakceptowanie swojego adresu IP jako

adresu sieciowego. Polega to na przejęciu kontroli nad komputerem łączącym go z siecią, a następnie odłączeniu go i „oszukaniu" serwera, podając się za użytkownika prawdziwego komputera głównego. Stanowi to większe zagrożenie, ponieważ po udanym ataku mamy większy dostęp do zasobów systemu. Istnieją specjalne programy sniffers, które po zainstalowaniu w sieci, w której nastąpiło włamanie, wyłapują wiadomości przemieszczające się w jej obrębie, a wybrane z nich kopiują na dysk atakującego. Dzięki programom typu sniffers można uzyskać wiele cennych informacji, takich jak dane osobowe, hasła dostępowe oraz wiele innych.

- **Hijacking** jest to metoda polegająca na przechwytywaniu transmisji odbywającej się między dwoma systemami. Metoda ta jest bardzo skuteczna, gdy próbujemy uzyskać dostęp do szczególnie chronionych programów
- **Backdoor** – przejmuje kontrolę nad zainfekowanym komputerem, umożliwiając wykonanie na nim czynności administracyjnych, łącznie z usuwaniem i zapisem danych. Podobnie jak trojan, backdoor podszywa się pod pliki i programy, z których często korzysta użytkownik. Umożliwia intruzom administrowanie systemem operacyjnym poprzez Internet. Wykonuje wtedy zadania wbrew wiedzy i woli ofiary;
- **Programy szpiegujące** – oprogramowanie zbierające informacje o osobie fizycznej lub prawnej bez jej zgody, jak informacje o odwiedzanych witrynach, hasła dostępowe itp. Występuje często jako dodatkowy i ukryty komponent większego programu, odporny na usuwanie i ingerencję użytkownika. Programy szpiegujące mogą wykonywać działania bez wiedzy użytkownika – zmieniać wpisy do rejestru systemu operacyjnego i ustawienia użytkownika. Program szpiegujący może pobierać i uruchamiać pliki pobrane z sieci:
  - ✓ **Scumware** – żargonowe, zbiorcze określenie oprogramowania, które wykonuje w komputerze niepożądane przez użytkownika czynności;
  - ✓ **Stealware** – służące do okradania kont internetowych;
  - ✓ **Adware** – oprogramowanie wyświetlające reklamy;
  - ✓ **Hijacker Browser Helper Object** – dodatki do przeglądarek, wykonujące operacje bez wiedzy użytkownika.
- **Exploit** – kod umożliwiający bezpośrednie włamanie do komputera ofiary, do dokonania zmian lub przejęcia kontroli. Wykorzystuje się lukę w oprogramowaniu zainstalowanym na atakowanym komputerze. Exploity mogą być użyte w atakowaniu stron internetowych, których silniki oparte są na

językach skryptowych (zmiana treści lub przejęcie kontroli administracyjnej), systemów operacyjnych (serwery i końcówki klienckie) lub aplikacji (pakiety biurowe, przeglądarki internetowe lub inne oprogramowanie);

- **Rootkit** – jedno z najniebezpieczniejszych narzędzi hackerskich. Ogólna zasada działania opiera się na maskowaniu obecności pewnych uruchomionych programów lub procesów systemowych (z reguły służących hackerowi do administrowania zaatakowanym systemem). Rootkit zostaje wkompilowany (w wypadku zainfekowanej instalacji) lub wstrzyknięty w istotne procedury systemowe. Z reguły jest trudny do wykrycia, ponieważ nie występuje jako osobna aplikacja. Zainstalowanie rootkita jest najczęściej ostatnim krokiem po włamaniu do systemu, w którym prowadzona będzie ukryta kradzież danych lub infiltracja;
- **Keylogger** – Odczytuje i zapisuje wszystkie naciśnięcia klawiszy użytkownika. Dzięki temu adresy, kody, cenne informacje mogą dostać się w niepowołane ręce. Pierwsze programowe keyloggery były widoczne w środowisku operacyjnym użytkownika. Teraz coraz częściej są procesami niewidocznymi dla administratora. Istnieją też keyloggery występujące w postaci sprzętowej zamiast programowej;
- **Dialery** – programy łączące się z siecią przez inny numer dostępowy niż wybrany przez użytkownika; najczęściej są to numery o początku 0-700 lub numery zagraniczne. Dialery szkodzą tylko posiadaczom modemów telefonicznych analogowych i cyfrowych, występują głównie na stronach o tematyce erotycznej.
- Mniej szkodliwe złośliwe oprogramowanie to:
  - ✓ **fałszywe alarmy** dotyczące rzekomo nowych i groźnych wirusów. Fałszywy alarm to także rzekome wykrycie zainfekowanego pliku, które powodują programy antywirusowe;
  - ✓ ***żarty komputerowe***, robione najczęściej nieświadomym początkującym użytkownikom komputerów.

Cyberprzestrzeń, a wraz z nią nowy typ zagrożenia, określany mianem cyberprzestępczości, narodziła się w momencie powstania politycznej koncepcji autostrad informacyjnych. Rozwiązanie to zakładało, że wszelkie informacje w postaci tekstu, dźwięku i obraz będą mogły być przekazywane na znaczne odległości szybko i bez przeszkód. Globalna sieć coraz bardziej się rozrastała i stawała się coraz bardziej podobna do świata rzeczywistego, obejmując coraz to nowe rejony i dziedziny na świecie. Przestępczość, także terroryzm, szybko

znalazły swoje miejsce w przestrzeni wirtualnej. Informacja stała się towarem, można ją więc było wykraść, sprzedać, zniszczyć, posłużyć się nią w celu uzyskania korzyści materialnych czy też ideologicznych. Dlatego właśnie jej ochrona stała się kwestią strategiczną.

Pierwsze informacje na temat niebezpieczeństwa zamachów terrorystycznych przy użyciu systemów komputerowych pojawiły się już w 1979 roku w raporcie rządu szwedzkiego na temat zagrożeń społecznych związanych z komputeryzacją. Zaś samo słowo „cyberterroryzm" zaczęło być używane już w latach 80. w wypowiedziach amerykańskich specjalistów w dziedzinie wywiadu wojskowego. Od tego czasu o cyberterroryzmie mówiło się coraz częściej. To w 1995 roku cybernetyczny świat obiegła wiadomość (jak się później okazało nieprawdziwa), że rząd meksykański zbombardował miasto, w którym korytarze szpitala w Comitan były pełne trupów, a żołnierze gwałcili kobiety i mordowali dzieci. Podczas operacji **Pustynna Burza** w Zatoce Perskiej hakerzy zdołali złamać zabezpieczenia komputerów należących do Pentagonu. Ich łupem padły wówczas plany strategiczne ataku na Iran. Sprawców nigdy nie złapano. 19 września 1995 roku haker złamał zabezpieczenia komputerów francuskiej marynarki wojennej i wykradł sygnatury akustyczne. Znaczniki te pozwalały rozpoznać każdą pływającą jednostkę francuską. Jeszcze groźniej zrobiło się w roku 2001, gdy haker, łamiąc zabezpieczenie, uzyskał dostęp do sieci amerykańskiej marynarki wojennej. Włamywacz przejął kontrolę nad informacjami dotyczącymi systemu GPS oraz obroną strategiczną USA. Zdobył także tajne kody umożliwiające kierowanie statkami kosmicznymi, satelitami oraz pociskami. Nigdy nie ujęto osoby odpowiedzialnej za to włamanie.

W lutym 2000 roku serwery Yahoo, Amazon, CNN, eBay, itp. zostały zaatakowane za pomocą DoS (*denial of service*), co spowodowało wyłączenie na jakiś czas tych serwisów. Sytuacja ta spowodowała zmiany opinii publicznej, która zaczęła dostrzegać, że cyberterroryzm stał się faktem. Pod koniec października 2002 roku świat obiegła elektryzująca wiadomość podana przez FBI. Zaatakowanych zostało 13 podstawowych serwerów DNS („tłumaczą' one adresy internetowe na numeryczne adresy IP, wykorzystywane przez komputery; ich całkowite zablokowanie mogłoby spowodować zupełny paraliż Internetu). W rzeczywistości było to 13 jednoczesnych zmasowanych ataków DDoS (*distributed denial of service*). W krytycznym momencie działały tylko 4 serwery, a cały atak trwał 6 godzin.

Wirus który zaatakował globalną sieć i niszczył wszystko, co napotykał na swojej drodze, jednocześnie spowodował miliardowe straty na całym świecie. Takim wirusem okazał się słynny „I love you". Nawet Pentagon przyznał, że ofiarą tego wirusa padły cztery komputery klasyfikowane jako całkowicie bezpieczne, stanowiące część Defense Data Network – wydzielonej infrastruktury wojskowej.

Początek wojny w Iraku spowodował falę ataków cyfrowych: objawiało się to niszczeniem witryn firm amerykańskich oraz atakami na rządowe i wojskowe systemy informatyczne. Nie był to jednak pierwszy polityczny konflikt w cyberprzestrzeni. W 2000 roku grupa pakistańskich hakerów zniszczyła około 600 indyjskich stron internetowych oraz przejściowo przejęła kontrolę nad niektórymi indyjskimi sieciami komputerowymi. W lutym 2001 roku chińscy hakerzy dokonali kilkuset cyberataków na największe japońskie firmy w odwecie za zaostrzenie przez Japonię polityki wobec Chin. Zaś od marca 1999 do kwietnia 2000 roku dokonano 89 cyberataków na 60 agencji rządowych w Malezji. Celem ataków były głównie „wrażliwe" resorty, takie jak opieka społeczna, imigracja, skarbInnymi nagłośnionymi publicznie działaniami, nazywanymi powszechnie właśnie cyberterroryzmem, były ataki typu DoS na komputery NATO w czasie wojny w Kosowie w 1999 roku. W stanie wojny, ale wojny elektronicznej, znalazły się Stany Zjednoczone i ChRL w maju 2001 roku, kiedy to amerykańscy hakerzy zaatakowali masowo chińskie strony internetowe. W odpowiedzi Chińczycy włamali się na strony amerykańskiej administracji i wielkiego biznesu. Obyło się bez wielkich strat materialnych, ale efekt pozwolił zdać sobie sprawę z tego, jak mogą wyglądać wojny w przyszłości. Przykłady podobnych działań można oczywiście mnożyć. Jednak większość ekspertów nazywa je nie cyberterroryzmem, a po prostu cyberprzestępczością, a dokładnie hakingiem, hakingiem politycznym, wojną informacyjną, haktywizmem czy po prostu zwykłym wandalizmem.

Atak cybernetyczny na Estonię: zmasowany atak prowadzony przez hakerów przeciwko Estonii od 17 maja 2007. Według niektórych źródeł hakerzy powiązani byli z władzami Federacji Rosyjskiej, nie zostały jednak przedstawione żadne dowody potwierdzające tę tezę. W wyniku ataku zostały zablokowane serwery i strony Zgromadzenia Państwowego, agend rządowych, banków i mediów. Zmasowane cyberataki były odwetem za przeniesienie pomnika Żołnierzy Armii Czerwonej z centrum Tallina na podmiejski cmentarz wojskowy. Gdy w całym kraju wybuchły zamieszki, inspirowane przez mieszkających

w Estonii Rosjan, sieć teleinformatyczna Estonii została zaatakowana i doprowadzona do stanu krytycznego. Zablokowano strony rządowe, kancelarii prezydenta, głównych gazet, padły systemy bankowe oraz wewnętrzna sieć estońskiej policji. Po raz pierwszy w historii, równolegle z prowadzonymi działaniami militarnymi podczas konfliktu Rosji z Gruzją w 2008 r., przeprowadzono zmasowane ataki na gruzińskie strony internetowe. Po rozpoczęciu działań wojennych, zaatakowana została strona prezydenta Gruzji, a następnie wiele innych oficjalnych gruzińskich stron rządowych, policji, agencji prasowych oraz stacji telewizyjnych. Odpowiedzialność za te działania przypisywana jest głównie obywatelom Rosji, w tym cyberprzestępczej organizacji Russian Business Network. Podobnie jak w przypadku Estonii, na rosyjskich stronach internetowych bardzo szybko pojawiły się ogólnodostępne instrukcje i narzędzia ułatwiające przeprowadzanie ataków. Opublikowana została również „lista celów".

W lipcu 2008 r., kilka dni po wprowadzeniu zakazu publicznego prezentowania symboli Związku Radzieckiego, ataku na portale internetowe doświadczyła także Litwa. Zablokowano wówczas około 300 witryn internetowych.

DoS (ang. *Denial of Service*, odmowa usługi) – atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania. Atak polega zwykle na przeciążeniu aplikacji serwującej określone dane czy obsługującej danych klientów (np. wyczerpanie limitu wolnych gniazd dla serwerów FTP czy WWW), zapełnienie całego systemu plików tak, by dogrywanie kolejnych informacji nie było możliwe (w szczególności serwery FTP), czy po prostu wykorzystanie błędu powodującego załamanie się pracy aplikacji. W sieciach komputerowych atak DoS oznacza zwykle zalewanie sieci (ang. *flooding*) nadmiarową ilością danych mających na celu wysycenie dostępnego pasma, którym dysponuje atakowany host. Niemożliwe staje się wtedy osiągnięcie go, mimo że usługi pracujące na nim są gotowe do przyjmowania połączeń.

DRDoS – jedna z nowszych odmian ataku odmowy dostępu DoS. Powstała w wyniku połączenia metody zalewania żądaniami synchronizacji (ang. *SYN flood*) i metod wykorzystywanych przy rozproszonych atakach odmowy dostępu DDoS. Polega na generowaniu specjalnych pakietów SYN, których adres źródłowy jest fałszywy – jest nim adres ofiary. Następnie duża liczba takich pakietów jest wysyłana do sieci. Komputery, do których one docierają, odpowiadają pakietami SYN/ACK kierowanymi na adres pochodzący z fałszywego nagłówka. W wyniku takich działań ofiara jest zalewana olbrzymią ilością pakietów z wielu

hostów. W porównaniu do tradycyjnego ataku typu DDoS utrudnia to wykrycie rzeczywistego źródła ataku.

Z informacji przedstawionych na warsztatach NATO wynika, że estońskie serwisy informacyjne i rządowe stały się celem ataków DDoS. Ataki te polegały na rozproszonej odmowie usługi na system komputerowy lub usługę sieciową. Realizowane były równocześnie na wielu komputerach i doprowadzały do zajęcia wszystkich wolnych zasobów, co skutkowało że nie mogły poprawnie funkcjonować. Atak DDoS jest odmianą ataku DoS polegającą na zaatakowaniu ofiary z wielu miejsc jednocześnie. Do przeprowadzenia ataku służą najczęściej komputery, nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania (różnego rodzaju tzw. boty i trojany). Na dany sygnał komputery zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z usług, jakie oferuje. Dla każdego takiego wywołania atakowany komputer musi przydzielić pewne zasoby (pamięć, czas procesora, pasmo sieciowe), co przy bardzo dużej liczbie żądań prowadzi do wyczerpania dostępnych zasobów, a w efekcie do przerwy w działaniu lub nawet zawieszenia systemu.

Na rosyjskojęzycznych forach publikowane są instrukcje, jak przeprowadzić taki atak. Zjawisko cyberwojny, czyli wykorzystania Internetu jako przestrzeni agresji motywowanej politycznie, nie jest niczym nowym. Prócz Estończyków, przekonali się o tym również Gruzini, gdy rosyjski atak na ich system teleinformatyczny, zsynchronizowany z atakiem militarnym, pozbawił kraj możliwości korzystania z Internetu. Rosyjscy hakerzy złamali wówczas zabezpieczenia Amerykanów, aby w ten sposób zablokować najważniejsze gruzińskie serwery. Na wznowienie 20 stron internetowych gruzińscy informatycy potrzebowali tygodnia. W tym czasie wojska rosyjskie posunęły się w głąb Gruzji, wygrywając nie tylko pod względem militarnym, ale także informacyjnym, gdyż rząd w Tbilisi nie mógł poinformować świat o bieżących wydarzeniach. Gruzinom udało się przejąć kontrolę nad serwerem C&C. Najwyraźniej mając już dosyć działalności nieznanego włamywacza, postanowili podłożyć mu niespodziankę. Na jednym z celowo zainfekowanych komputerów umieścili archiwum ZIP o nazwie wskazującej na materiały leżące w polu zainteresowania włamywacza. Archiwum zawierało jednak jego własnego konia trojańskiego. Plik został przez włamywacza pobrany i uruchomiony. Dzięki dostępowi do panelu sterowania botnetu, Gruzini mogli przeszukać komputer swojego przeciwnika i nagrać film z jego udziałem. Gruzini poznali także jego adres email, adres IP oraz lokalizację na terenie Rosji. Niestety włamywacz szybko się zorientował, że coś jest nie tak

i zerwał połączenie, zanim udało się ustalić jego imię i nazwisko. Nie da się jednak ukryć, ze choć postępowanie gruzińskich służb może wydawać się kontrowersyjne, to odniosło ono wymierny sukces, potwierdzając, że za serią włamań stoją Rosjanie.

Największą kradzieżą danych z instytucji rządowych był atak na **Pentagon, departamenty Stanu, Energii i Handlu, NASA** oraz kilka innych amerykańskich agencji rządowych w 2007 roku. Hakerzy ukradli wówczas co najmniej 10 terabajtów danych. W grudniu 2009 r. hakerzy zaatakowali sieć Google. Wykradziono m.in. informacje dotyczące systemu haseł.

W połowie 2010 roku w elektrowniach atomowych zlokalizowanych w **Buszehr w Iranie** wykryto nikomu jeszcze wtedy nieznanego robaka komputerowego o nazwie **Stuxnet**. Obiektem największego ataku był Iran, gdzie Stuxnet zainstalował się w 16 tysiącach komputerów. Okazało się jednak, że systemy komputerowe zostały zainfekowane już rok wcześniej. Stuxnet – robak komputerowy działający w systemie Windows – został po raz pierwszy wykryty w czerwcu 2010. Jest pierwszym znanym robakiem używanym do szpiegowania i przeprogramowywania instalacji przemysłowych. Zawierał rootkit na system Windows, pierwszy w historii PLC rootkit. Wykorzystywał też wiele luk 0-day. Wirus miał zdolność aktualizacji metodą peer-to-peer. W listopadzie 2010 roku prezydent Iranu ujawnił, że złośliwe oprogramowanie spowodowało problemy w niektórych irańskich wirówkach służących do wzbogacania uranu. Twierdził jednak, że problemy te zostały rozwiązane, a produkcja w elektrowni zostanie przesunięta w czasie. Podstawową formą rozpowszechniania się robaka są zainfekowane podręczne pamięci USB. Po zainstalowaniu się w systemie operacyjnym Windows robak zaczyna poszukiwać określonego modelu sterownika PLC produkcji firmy Siemens (systemy SCADA). Sterowniki PLC są często używane w różnego rodzaju fabrykach, rafineriach czy elektrowniach i robak poszukuje kontrolera Siemens SIMATIC WinCC/Step 7. Jeżeli zarażony robakiem komputer nie jest podłączony do poszukiwanego przez niego kontrolera, robak nie robi nic. Jeżeli kontroler zostanie odnaleziony, robak zmienia niektóre z ustawień kontrolera PLC, robiąc to w sposób sugerujący, że jego twórcy mieli na celu tylko wybrane kontrolery. Podejrzewa się, że wirus o nazwie Stuxnet został opracowany wspólnie przez specjalistów izraelskich i amerykańskich, którzy obawiali się stworzenia broni nuklearnej przez Iran. Dokładna liczba zarażonych komputerów i systemów nie jest znana, według danych z 29 września zarażonych było ok. 100 000 komputerów ze 155 krajów, najwięcej infekcji odkryto w Iranie

– 58% z zarażonych komputerów, Indonezji – 18%, Indiach – 10% i Azerbejdżanie – 3,4% (pozostałe kraje poniżej 2%). Według niepotwierdzonych informacji chińskiego producenta oprogramowania antywirusowego, *Rising International*, robak zaatakował kilka tysięcy zakładów przemysłowych w Chinach.

Współczesne zagrożenia dotyczą najczęściej systemów i sieci teleinformatycznych. Zagrożenie, jak twierdzą specjaliści ds. bezpieczeństwa, dotyczy najczęściej sieci, z których nowe szkodliwe programy próbują wykradać informacje. Czasem jednak złośliwe oprogramowanie jest tak wyrafinowane, że nawet specjaliści są wobec niego bezradni i przez wiele lat nie potrafią go wykryć. Tak właśnie jest ze szkodnikiem o nazwie **Regin**, który, jak się okaza**ło, szpie**guje nas od co najmniej 2008 roku.

Pod koniec listopada, po ataku hakerów na Sony Pictures, który doprowadził do odwołania premiery komedii *The Interview*, o atak oskarżyło **Koreę Północną**. Tematem filmu był zamach na przywódcę Korei Północnej Kim Dzong Una. Pjongjang uznał komedię za obraźliwą. Obecnie na czarnej liście znajdują się tylko Iran, Sudan, Syria i Kuba. Sankcje związane z obecnością na liście ograniczają amerykańską pomoc, eksport broni i niektóre transakcje finansowe – wyjaśnia agencja AP. Do ataku przyznali się hakerzy z grupy o nazwie Strażnicy Pokoju (GOP). Zagrozili oni też atakami porównywalnymi z 11 września 2001 roku, jeśli film wejdzie na ekrany kin. *The Interview* miał mieć premierę w USA w okresie świątecznym. Pjongjang zaprzecza, jakoby stał za tym atakiem i jednocześnie zaproponował Stanom Zjednoczonym przeprowadzenie wspólnego śledztwa w tej sprawie. Biały Dom odrzucił tę propozycję, oświadczając, że jest przekonany, iż za atakiem stoją północnokoreańskie władze.

W obszarze bezpieczeństwa cyberprzestrzeni przed atakami swoje działania realizują nie tylko państwa, ale także organizacje międzynarodowe i sojusze militarne. Sygnałem tego jest choćby szczyt NATO w Lizbonie (19-20 listopada 2010 r.) oraz przyjęta tam nowa Koncepcja Strategiczna. W dokumencie tym, wśród wyzwań dla wspólnego, kooperatywnego bezpieczeństwa, zaraz po proliferacji broni masowego rażenia i terroryzmie, wskazano zagrożenie cyberatakami. Cyberataki stają się coraz częstsze, są dobrze zorganizowane, a przez to coraz bardziej destrukcyjne i kosztowne. Mogą zagrażać infrastrukturze krytycznej państwa, w tym funkcjonowaniu transportu, gospodarki i administracji. Istotnym aspektem tego zagrożenia jest fakt, iż jego sprawcami mogą być obce wojska, służby wywiadowcze, organizacje przestępcze, grupy terrorystyczne i/ lub grupy ekstremistyczne.

W 2014 roku doszło do cyberataku na strony internetowe warszawskiej giełdy oraz prezydenta. Do zablokowania stron przyznał się CyberBerkut. Organizacja zamieściła w Internecie oświadczenie, w którym między innymi pisze: „Rzeczpospolita Polska jest jednym ze sponsorów faszyzmu na Ukrainie. Polscy oficjele, naruszając sprawy innego kraju, poświęcają nie tylko interesy swoich obywateli, ale też ich życie”[109].

Zaatakowane zostało konto Newsweeka na Twitterze. Na stronie opublikowano m.in. groźby pod adresem prezydenta USA Baracka Obamy, jego córek i żony.

Oprócz gróźb pod adresem rodziny prezydenckiej Stanów Zjednoczonych, na koncie Newsweeka podmieniono zdjęcie nagłówkowe oraz profilowe. Nowa grafika przedstawia mężczyznę w chuście i napis „CYBERCALIPHATE”. Oprócz tego, znalazło się również odniesienie do ataku na redakcję francuskiego tygodnika satyrycznego Charlie Hebdo. Po zamachu, internauci, solidaryzując się z ofiarami, umieszczali w sieci tabliczki z napisem „Jestem Charlie”. CyberKalifat wykorzystał to hasło, umieszczając na Twitterze Newsweeka informację „Jestem Państwem Islamskim”[110].

Kuala Lumpur, hakerska grupa powiązana z CyberKalifatem, zaatakowała malezyjskie linie lotnicze. Na oficjalnej stronie przewoźnika hakerzy zamieścili wizerunek jaszczura w cylindrze i smokingu, wokół którego pojawiały się napisy „404 – Samolot Nieodnaleziony”, nawiązujące do komunikatu przeglądarek internetowych „404 – Server Not Found”. Wcześniej na stronie można było przeczytać napis „ISIL zwycięży”.

Sojusz Północnoatlantycki (NATO) od 2016 roku, po lądzie, morzu, przestrzeni powietrznej i kosmosie, uznał oficjalnie cyberprzestrzeń jako piątą domenę operacyjną. Pojęcie cyberwojny nie zostało dotąd zdefiniowane w jednoznaczny sposób. Definicja cyberwojny jest przedmiotem wielu debat. James A. Green uważa, że „cyberwojna stanowi kontynuację polityki poprzez działania inicjowane w cyberprzestrzeni zarówno przez podmioty państwowe, jak i niepaństwowe, stanowiące zagrożenie dla bezpieczeństwa innych podmiotów lub

[109] http://www.bankier.pl/wiadomosc/Strony-GPW-i-prezydenta-zaatakowane-przez-CyberBerkut-7217306.html [dostęp: 20.02.2023].

[110] http://tech.wp.pl/kat,130068,title,Panstwo-Islamskie-zaatakowalo-Newsweeka,wid,17251140,wiadomosc.html?ticaid=114bea [dostęp: 10.02.2023].

działanie odpowiadające na zagrożenie dla bezpieczeństwa państwa (rzeczywiste lub postrzegane)”[111] .

Wojna rosyjsko-ukraińska rozpoczęła się od napadu 24 lutego 2022 roku putinowskiej Rosji na Ukrainę i była poprzedzona cyberatakami. Swym zakresem objęły one serwisy internetowe administracji publicznej (tzw. ataki DDoS – ang. *distributed denial of service*, rozproszona odmowa usługi) oraz rozmieszczaniem złośliwego oprogramowania niszczącego dane (tzw. wiper). Pierwszy atak, do którego doszło 14 stycznia, wymierzony został w oficjalne serwisy administracji publicznej, portal Ministerstwa Oświaty, Ministerstwa Spraw Zagranicznych, Ministerstwa Energetyki, strony rządowe, w tym aplikacji Dija oraz Państwowej Służby ds. Sytuacji Nadzwyczajnych. W wyniku przeprowadzonego ataku, poza prowokacyjnymi komunikatami na głównych stronach atakowanych witryn, nie doszło do ujawienia żadnych informacji.

Do kolejnego rosyjskiego ataku na ukraińskie podmioty działające w kluczowych sektorach, m.in. energetycznym, telekomunikacyjnym i transportowym, doszło w połowie lutego. W jego wyniku zakłóceniu uległy witryny internetowe Ministerstwa Obrony oraz Sił Zbrojnych Ukrainy, zablokowano także usługi mobilne banków państwowych, PrivatBanku, i Sbierbanku. Wstrzymano również wypłaty gotówki z bankomatów[112].

Służby Ukrainy uznały, że największym w historii tego kraju atakiem był ten z 15 lutego. Za inicjatorów cyberataków Ukraina uznała Federację Rosyjską. Atak DDoS, którego celem było przeciążenie i zablokowanie usług online ukraińskich instytucji, nie spowodował zamierzonych, rozległych szkód, co było wynikiem szybkiej reakcji Ukrainy i wsparcia udzielonego przez USA. Kolejny incydent cybernetyczny związany z atakiem DDoS miał miejsce w przeddzień inwazji rosyjskiej, 23 lutego. Rosja zaatakowała ukraińskie portale internetowe, w tym wiele stron państwowych oraz internetowych serwisów ukraińskich instytucji państwowych. Wydarzenia ta bezpośrednio poprzedziły działania militarne[113].

Od 15 lutego Ukraina była celem około 2,8 tysięcy cyberataków. 6 marca odnotowano rekordową liczbę 271 ataków DDoS. Rosjanie wykorzystują szeroki

[111] https://sobieski.org.pl/cybernetyczny-wymiar-wojny-rosyjsko-ukrainskiej/ [dostęp: 10.04.2024].
[112] https://sobieski.org.pl/cybernetyczny-wymiar-wojny-rosyjsko-ukrainskiej/ [dostęp: 10.06.2023].
[113] Tamże.

wachlarz metod, aby sparaliżować funkcjonowanie kluczowych instytucji dla funkcjonowania państwa ukraińskiego, zwłaszcza w obszarze prowadzenia operacji obronnej przez Ukrainę[114].

Gdy pierwsze pociski uderzyły w Ukrainę, cywilni eksperci z ukraińskiej branży cybernetycznej zwrócili się do rządu i zaoferowali pomoc – wyjaśnia Jegor Auszew, współzałożyciel ukraińskiej firmy informatycznej Cyber Unit Technologies. Grupa ekspertów jako ochotnicza armia przekazała że jej motywem jest wyłącznie zakończenie tej wojny" – mówił w rozmowie telefonicznej z DW Auszew, który obecnie przebywa w pobliżu Kijowa. W ciągu kilku dni na apel w mediach społecznościowych o przyłączenie się do projektu odpowiedziały setki ekspertów ds. cyberbezpieczeństwa. Miesiąc po rozpoczęciu wojny ich liczba wzrosła – według szacunków Auszewa – do prawie tysiąca osób[115].

Innym wpływowym ugrupowaniem w ramach armii cybernetycznej jest międzynarodowy kolektyw hakerów Anonymous. Wkrótce po rozpoczęciu przez Rosję inwazji na Ukrainę ruch ogłosił na Twitterze, że „prowadzi cyberwojnę przeciwko rosyjskiemu rządowi". Nad cyberatakami pracują obecnie setki hakerów i wolontariuszy z mniejszą wiedzą informatyczną, którzy zajmują się rozpowszechnianiem wśród Rosjan informacji o wojnie. W tym celu wykorzystują m.in. stronę internetową, która umożliwia użytkownikom wysyłanie wiadomości tekstowych, wiadomości WhatsApp i e-maili do dowolnych osób w Rosji[116]. Strona została zaprogramowana przez Squad 303, kolektyw powiązany z Anonymous. Grupa powstała w Polsce i obecnie liczy ponad 100 członków na całym świecie, w tym również w Japonii, Estonii, Niemczech i Francji. Tylko w pierwszym miesiącu wojny za pośrednictwem członków Squad z ich strony internetowej wysłano do ludzi w Rosji ponad 40 milionów wiadomości[117].

Również Polska nie jest wolna od zagrożeń cybernetycznych. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego, w 2020 roku odnotował ponad 246 tys. zgłoszeń dotyczących potencjalnego wystąpienia incydentu teleinformatycznego, z czego 23 309 okazało się faktycznym incydentem. Obie wskazane ilości są najwyższe w historii działania zespołu i stanowią zauważalny

[114] Tamże.
[115] https://www.dw.com/pl/ukrai%C5%84ska-partyzantka-w-cyberprzestrzeni-jak- hakerzy-atakuj%C4%85-rosj%C4%99/a-61273452 [dostęp: 10.06.2023].
[116] Tamże.
[117] Tamże.

wzrost w stosunku do poprzedniego roku – informuje ABW w *Raporcie o stanie bezpieczeństwa cyberprzestrzeni RP*. Coroczna publikacja raportu służy podnoszeniu świadomości użytkowników w zakresie zagrożeń i podatności, a także skutków ich ewentualnego wystąpienia dla systemów teleinformatycznych znajdujących się w obszarze odpowiedzialności[118].

2.3. Polityka bezpieczeństwa informacji

Bezpieczeństwo informacji – ISO 27001[119]. Informacja stanowi taki sam zasób organizacji jak pracownicy, technologie, środki finansowe. Informacje w postaci know-how, bazy danych, warunków handlowych stanowią wartość bilansową, dlatego kluczowe staje się właściwe zabezpieczenie przetwarzanych w organizacji informacji. Należy zwrócić uwagę, że nie chodzi tylko o wdrożenie rozwiązań w obszarze teleinformatyki, która naturalnie ma istotne znaczenie w przetwarzaniu informacji, lecz również zapewnienie bezpieczeństwa fizycznego, organizacyjnego, osobowego, prawnego czy też ciągłości działania. Kierując się zasadą najsłabszego ogniwa, jedynie rozwiązania kompleksowe mogą skutecznie zabezpieczyć przetwarzane danych w organizacji.

Punktem odniesienia przy budowie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) są **międzynarodowe standardy ISO 27001, ISO 27005** oraz zbiór dobrych praktyk w obszarze analizy ryzyka **(w tym ISO 31000**) oraz bezpieczeństwa. Konsultanci Blue Energy posiadają największe w Polsce doświadczenie w zakresie wdrażania SZBI, uzyskane w trakcie realizacji projektów zarówno w dużych koncernach, jak i małych firmach czy też administracji publicznej. Projekty realizowane są przez ekspertów o bogatej wiedzy popartej międzynarodowymi certyfikatami, jak np. CISA, CISM, CISSP, CompTIA Security+, ISO 27001, BS 25999, PRINCE2 Practitioner itp. Opracowana przez Blue Energy metodyka realizacji prac oparta jest na najlepszych praktykach oraz międzynarodowych normach jak ISO 27001, ISO 27002, ISO 27005, wytyczne COBIT oraz ISACA i inne.

Zapewnienie ciągłości działania organizacji polega na zapewnieniu skutecznej realizacji planów strategicznych organizacji. Poprzez analizę kluczowych procesów i zaangażowanych w nie zasobów poznajemy punkty krytyczne,

[118] Tamże.

[119] https://www.iso.org.pl/uslugi-zarzadzania/wdrazanie-systemow/systemy-bezpieczenstwa-informacji/iso-27001/ [dostęp: 10.04.2024].

najbardziej narażone na zagrożenia zewnętrzne i wewnętrzne. Podstawą metodyczną wdrożenia zarządzania ciągłością działania (BCP, BCMS) jest ISO 22301 oraz dobre praktyki z zakresu zarządzania kryzysowego i budowy planów awaryjnych. Analiza BIA (*Business Impact Analysis*) – analiza krytyczności procesów – jest źródłem informacji na temat tego, co jest krytyczne dla funkcjonowania organizacji, jakie procesy, zasoby są niezbędne do realizacji produktu czy usługi.

Polityka bezpieczeństwa informacji to zbiór reguł i procedur dotyczących bezpieczeństwa informacji. Powinna ona uwzględniać cele, sposoby i środki ochrony informacji, inaczej mówiąc odpowiadać na trzy proste pytania: co chronić, przed czym chronić, jak chronić? Ponadto musi odpowiadać konkretnej firmie. Jest to więc nadrzędne narzędzie, które ma uwzględniać wszelkie aspekty ochrony informacji, zarówno związane z przeciwdziałaniem utraty informacji w wyniku oddziaływania obcych służb, nieprzewidzianym działaniem czynników pozaludzkich (zdarzenia losowe, jak pożar, powódź, itp.), czy też nieumyślnym skasowaniem lub bezpowrotną utratą danych.

Planując politykę bezpieczeństwa informacji należy uwzględnić:

- **wartość posiadanych zasobów informacyjnych** – przeanalizować, co ma być poddane ochronie, jakie będą konsekwencje przełamania ochrony;
- **źródło agresji** – kto mógłby zagrażać naszym zasobom informacji (obce służby wywiadowcze, agendy rządowe, terroryści, sabotażyści, konkurenci, złodzieje, nieuprawnieni pracownicy, ciekawscy; jaka jest wartość naszej informacji dla potencjalnego agresora;
- **poziom możliwości agresora** – jakimi możliwościami technicznymi, intelektualnymi i organizacyjnymi dysponuje potencjalny agresor;
- **jakie nakłady finansowe i rzeczowe** byłby w stanie ponieść, ile czasu poświęcić dla uzyskania lub zniszczenia naszych informacji;
- **poziom ochrony** – jakiej klauzuli dokumenty posiadamy, ich ilość, jakie inne informacje powinny podlegać ochronie;
- **poziom dostępu** i liczbę uprawnionych osób;
- **inne** możliwe zdarzenia powodujące utratę informacji;
- **wskazania służb** ochrony państwa.

Przy opracowaniu szczególnych wymagań bezpieczeństwa należy także uwzględnić charakterystykę i dane o budowie systemu lub sieci teleinformatycznej, określić środki ochrony zapewniające bezpieczeństwo przetwarzanych informacji oraz zadania administratora i osoby odpowiedzialnej za funkcjonowanie

systemu lub sieci. Rozwijając powyższe zagadnienia i wprowadzając je w życie w postaci konkretnych procedur – wdrażanie systemu ochrony informacji – powodujemy zwiększenie bezpieczeństwa w obszarze chronionym, przeciwdziałając negatywnym oddziaływaniom zewnętrznym w maksymalnie możliwym stopniu.

Jako istotny element polityki bezpieczeństwa, a dokładniej mówiąc narzędzie służące do jej realizacji, należy uznać wyżej wspomniany kontrwywiad gospodarczy. W działalności tego typu instytucji, tworzonych zarówno na szczeblu ogólnonarodowym, jak i przez poszczególne podmioty uczestniczące w życiu gospodarczym, występuje wiele ogólnych zasad wywodzących się ze sprawdzonych rozwiązań organizacyjnych i metod działania stosowanych przez służby wywiadowcze.

Aby nie dopuścić do wykorzystania przez wywiad osobowych źródeł informacji, dużą wagę przywiązuje się do ochrony i obserwacji osób, fizycznego zabezpieczenia dokumentów, weryfikacji pracowników, kontroli ich podróży i kontaktów z obywatelami innych krajów, ograniczania dostępu do określonych pomieszczeń, nadawania klauzuli tajności poszczególnym dokumentom, kontroli przechowywania i przekazywania dokumentacji niejawnej według ogólnej zasady polegającej na udostępnianiu w takim zakresie, w którym jest ona potrzebna do służbowego wykorzystania. Niezależnie od tego, w ograniczonym zakresie, mogą być podejmowane działania mylące, mające na celu sprowokowanie określonych przedsięwzięć przez konkurenta. Powodzenie takich działań jest możliwe tylko w przypadku starannie przygotowanych, długofalowych przedsięwzięć[120].

Analiza ryzyka realizowana dla punktów krytycznych daje odpowiedzi, w jaki sposób zabezpieczyć funkcjonowanie organizacji. Celem **analizy ryzyka** jest określenie i oszacowanie prawdopodobieństwa oraz skutków wystąpienia danego (niepożądanego) zdarzenia. Pozwala ona określić poziom ryzyka w sposób jakościowy i ilościowy, dzięki czemu mogą zostać przeprowadzane działania zapobiegawcze lub działania polegające na jego eliminacji. Analiza ryzyka jest jednym z elementów procesu zarządzania ryzykiem. Wyróżnia się kilka rodzajów podejścia do analizy[121]:

- podejście podstawowego poziomu – zastosowanie standardowych zabezpieczeń;

[120] http://www.wywiad-gospodarczy.pl/2.html [dostęp: 15.01.2023].
[121] http://pl.wikipedia.org/wiki/Analiza_ryzyka [dostęp: 05.04.2024].

- podejście nieformalne – oparte na wiedzy i doświadczeniu ekspertów;
- szczegółowa analiza ryzyka – z wykorzystaniem technik analizy ryzyka;
- podejście mieszane.

Analiza ryzyka jest narzędziem wykorzystywanym m.in. do:

- przygotowania polityki bezpieczeństwa;
- planowania i organizacji systemami zarządzania bezpieczeństwem;
- zarządzania projektami informatycznymi;
- zarządzania organizacją, instytucją czy przedsiębiorstwem;
- różnego rodzaju analiz gospodarczo-biznesowych.

Odpowiedzi na pytania co i kto zagraża naszym procesom, zasobom, realizowanym działaniom, łańcuchowi dostaw czy współpracownikom umożliwiają wdrożenie działań prewencyjnych, podnoszących odporność naszego systemu informacyjnego na sytuacje krytyczne. Oczywiście zabezpieczenie się przed wszystkimi możliwymi zagrożeniami jest ze względów organizacyjnych i kosztowych niemożliwe. Zarządzanie ciągłością działania zapewnia nam narzędzia reagowania w sytuacji kryzysowej, w postaci minimalnej akceptowalnej konfiguracji oraz planów ciągłości działania/planów odtworzeniowych. Minimalna akceptowalna konfiguracja to poziom dostępności zasobów informacyjnych niezbędny do realizowania procesu na minimalnym akceptowalnym poziomie.

Plany ciągłości działania oraz plany odtworzeniowe to zbiór działań podejmowanych w sytuacjach kryzysowych niezbędnych do zabezpieczenia zasobów organizacji i umożliwiających jak najsprawniejsze odtworzenie działalności po awarii.

Zgodnie z dobrymi praktykami wszelkie plany i mechanizmy powinny zostać poddane testom, które wykażą adekwatność i realność ich realizacji w sytuacji kryzysowej. **Testy penetracyjne**[122] polegają na przeprowadzeniu kontrolowanego ataku na system teleinformatyczny, mający na celu praktyczną ocenę bieżącego stanu bezpieczeństwa tego systemu, w szczególności podatności i odporności na próby przełamania zabezpieczeń. Polega na analizie systemu pod kątem występowania potencjalnych błędów bezpieczeństwa spowodowanych niewłaściwą konfiguracją, lukami w oprogramowaniu lub sprzęcie, słabościami w technicznych lub proceduralnych środkach zabezpieczeń, a nawet niewystarczającą świadomością użytkowników.

[122] http://pl.wikipedia.org/wiki/Test_penetracyjny [dostęp: 10.04.2024].

Jest to ocena bezpieczeństwa systemów operacyjnych, sieciowych, serwerów usługowych pod względem zarządzania i monitorowania, jak również weryfikacja konfiguracji pod kątem zapewnienia wymaganego poziomu poufności i integralności danych. **Testy penetracyjne** swoim zakresem obejmować mogą:

- sieć teleinformatyczną, w tym urządzenia sieciowe;
- systemy wystawione na zewnątrz sieci;
- systemy informatyczne wewnętrzne;
- systemy automatyki przemysłowej.

Testy penetracyjne symulują działania rzeczywistego napastnika. Polegają one na testowaniu i stosowaniu techniki oraz narzędzi, które dobierane są w zależności od potrzeb.

Świadomość pracowników w zakresie regulacji wewnętrznych, bezpieczeństwa informacji, funkcjonowania organizacji jest podstawowym czynnikiem sukcesu (zapewnienie odpowiedniego poziomu bezpieczeństwa). Liczenie na samodoskonalenie może być złudne, a szkolenia teoretyczne nie zawsze dają oczekiwane efekty. Dlatego należy wykonać audyt socjotechniczny wraz z dedykowanym szkoleniem opartym na spostrzeżeniach audytowych. Audyt socjotechniczny polega na:

- badaniu postaw;
- ocenie zachowań;
- przeprowadzeniu prowokacji;
- realizacji ataku pozorowanego;
- opracowaniu i prezentacji raportu z rekomendacjami.

Po przeprowadzonym ataku socjotechnicznym opracowujemy dedykowane szkolenie z zakresu bezpiecznej komunikacji i higieny bezpiecznych zachowań. Szkolenie takie powinno zawierać:

- analizę procesu komunikacji;
- charakterystykę atakujących;
- typy ataków;
- metody obrony;
- podstawy bezpiecznych zachowań.

Opracowanie planów obrony dotyczących infrastruktury krytycznej znajduje podstawę w ustawie z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym wraz z jej nowelizacją z 19 września 2009 oraz Rozporządzeniu Rady Ministrów z dnia 30 kwietnia 2010 roku. Opracowanie systemu zarządzania

kryzysowego to zakres znacznie szerszy od opracowania planów obrony infrastruktury krytycznej, gdyż wymaga stworzenia mechanizmów organizacyjnych oraz ich utrwalenia. Ze względu na charakterystykę zagadnień zarządzania kryzysowego możemy zidentyfikować następujące obszary: Ze względu na charakterystykę zagadnień zarządzania kryzysowego możemy zidentyfikować następujące obszary:

- komunikacji wewnętrznej i zewnętrznej;
- bezpieczeństwa fizycznego;
- bezpieczeństwa osobowego;
- bezpieczeństwa prawnego;
- bezpieczeństwa teleinformatycznego;
- bezpieczeństwa informacji (poufność, dostępność, integralność).

Za skuteczne zabezpieczenie sieci informatycznej i za bezpieczeństwo informacji w organizacji odpowiada jej dyrektor, komendant, szef, kierownik itp. Zaniedbania w tym zakresie mogą skutkować problemami natury prawnej. Także wyciek danych czy włamanie nadwyręża reputację urzędu i powoduje utratę zaufania społecznego. Wszelkie awarie lub niepożądane ingerencje mogą doprowadzić do utraty kluczowych danych oraz przestoju funkcjonowania organizacji, instytucji czy przedsiębiorstwa.

2.4. Jak kształtować bezpieczeństwo informacyjne

W dzisiejszym świecie granice między umiarem i przesadą, informacją i dezinformacją, korzyścią i stratą są płynniejsze niż dawniej lub w ogóle się zacierają. Informacja jest orężem, jednak dziś bardziej obosiecznym niż kiedykolwiek wcześniej. Każde państwo, które zwiększa swój udział w międzynarodowym podziale pracy, handlu i kooperacji, z jednej strony staje się coraz większym rynkiem zbytu towarów, alokacji kapitałowej, inwestycji obcych, a z drugiej poszukuje dla siebie nowych rynków zagranicznych, stając się konkurentem na globalnym runku gospodarczym. Czynniki te powodują, iż nasz kraj, polskie firmy, coraz intensywniej budzą zainteresowanie obcych służb wywiadowczych i stają się celem ataków zmierzających do pozyskania w nich lub o nich informacji, zarówno o znaczeniu strategicznym, jak i typowych informacji zbieranych przez wywiadownie gospodarcze i biura konsultingowe. Aby chronić rodzimą gospodarkę przed zagrożeniami wynikającymi z oddziaływań

obcych agend wywiadowczych, także nasz kraj realizuje stosowną politykę bezpieczeństwa poprzez zastosowanie niezbędnych instrumentów prawnych i administracyjnych[123].

W ramach rozwiązań prawnych:

- ustawowo zobligowano służby ochrony państwa do: zwalczania, przeciwdziałania szpiegostwu gospodarczemu oraz realizacji i nadzoru przedsięwzięć związanych z ochroną informacji niejawnych (stosowne zapisy znajdują się w ustawie z dnia 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu oraz w ustawie z dnia 09.06.2006 roku o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego);
- zagwarantowano ochronę informacji niejawnych poprzez wprowadzenie w dniu 1 stycznia 2011 r. ustawy o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228);
- zagwarantowano ochronę danych osobowych wprowadzając ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst pierwotny: Dz. U. 1997 r., Nr 133, poz. 883) (tekst jednolity: Dz. U. 2002 r., Nr 101, poz. 926) i tworząc urząd Generalnego Inspektora Ochrony Danych Osobowych;
- ustawodawca dążąc do ochrony rodzimych firm i interesów ekonomicznych wprowadził ustawę o zwalczaniu nieuczciwej konkurencji z 16.04.1993 r., definiując w niej m.in. szpiegostwo gospodarcze (art. 23 ust. 2), tajemnicę przedsiębiorstwa (art. 11 ust. 4) oraz określając sankcje za jej zdradę (art. 23. ust.1);
- ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. 2007 r., Nr 50, poz. 331);
- w 2013 roku rząd przyjął Politykę Ochrony Cyberprzestrzeni RP, dotyczącą przede wszystkim ochrony cyberprzestrzeni w wymiarze pozamilitarnym. W MON trwają natomiast prace nad budową systemu cyberobrony. Dokonane w 2011 roku zmiany w systemie prawnym wprowadziły pojęcie cyberprzestrzeni i ustanowiły prawne podstawy nadzwyczajnego reagowania na występujące w niej zagrożenia;
- Doktryna cyberbezpieczeństwa RP w której zdefiniowano, że cyberprzestrzeń powinna być otwarta, a zarazem bezpieczna i chroniona; by to zapewnić potrzebne są działania instytucji państwa, sektora prywatnego i obywateli. Na podstawie powyższych regulacji prawnych powołano do życia

[123] http://www.wywiad-gospodarczy.pl/3.html [dostęp: 10.04.2024].

niezbędne instrumenty oraz opracowano wymagane procedury, które mają zapewniać ochronę informacji, w tym ekonomicznych, oraz przeciwdziałać ich utracie, także w wyniku oddziaływania obcych służb wywiadowczych.

W ramach realizowanego na szczeblu narodowym systemu bezpieczeństwa, tworzone są stosowne instrumenty, które kompleksowo przeciwdziałają czynom wymierzonym w interesy ekonomiczne państwa. Są to instrumenty prawne i administracyjne:

- **wyspecjalizowane służby kontrwywiadowcze**, umocowane ustawowo w strukturze państwa – są narzędziem wykonawczym państwa w zakresie polityki bezpieczeństwa;
- **stosowne uregulowania prawne:**
  - ✓ w zakresie ochrony wytwarzania, przetwarzania i przechowywania dokumentacji niejawnej;
  - ✓ w zakresie postępowania z informacjami niejawnymi;
  - ✓ w zakresie ochrony danych osobowych;
  - ✓ o zwalczaniu nieuczciwej konkurencji;
  - ✓ przeciwko szpiegostwu gospodarczemu.
- **zabezpieczenia organizacyjne**;
- **tworzenie procedur dostępu** do informacji niejawnych – certyfikaty bezpieczeństwa osobowego i przemysłowego;
- **realizacja zabezpieczeń systemowych** w zakresie przesyłu informacji, tworzenia odpornych na ataki zewnętrzne elektronicznych sieci wewnętrznych oraz systemów składowania danych.

Zabezpieczenie informacji strategicznych prowadzone jest poprzez ochronę źródeł informacji, zarówno osobowych, jak i nieosobowych (urzędnicy państwowi oraz osoby z kierownictwa instytucji – posiadający bezpośredni dostęp do informacji – które realizują planowanie strategiczne w obszarze gospodarki, instytucje gromadzące istotne informacje ekonomiczne, rządowe bazy danych itp.). W odniesieniu do źródeł osobowych stosowana jest tzw. osłona kontrwywiadowcza, natomiast w odniesieniu do nieosobowych (instytucjonalnych) stosuje się tzw. ochronę obiektową.

W związku z faktem, iż w instytucjach państwowych oraz przedsiębiorstwach o znaczeniu strategicznym, szczególnym dla gospodarki państwa, znajdują się istotne informacje mogące stanowić o bezpieczeństwie, w tym ekonomicznym, danego kraju, są one z jednej strony narażone na szczególnie aktywne

oddziaływanie służb wywiadowczych, z drugiej zaś podlegają szczególnej ochronie przez organy państwa, z wykorzystaniem szeregu metod i środków. Dlatego też nakłada się na nie szczególne obowiązki z zakresu ochrony informacji oraz wspomaga się realizowane przez nie działania w tym obszarze poprzez wyspecjalizowane instytucje rządowe – służby kontrwywiadu[124].

Dla zabezpieczenia strategicznych informacji należy opracować i wdrożyć **kompleksową politykę bezpieczeństwa**, która obejmuje m.in. następujące zagadnienia:

- politykę informacyjną;
- politykę informacji niejawnych;
- zasady ochrony danych osobowych;
- politykę bezpieczeństwa systemu teleinformatycznego;
- zasady ochrony tajemnicy przedsiębiorstwa lub innych tajemnic zawodowych;
- zapobieganie przestępstwom na szkodę firmy, a szczególnie fałszerstwom i oszustwom;
- zasady ochrony fizycznej i technicznej;
- inne polityki związane z bezpieczeństwem.

Takie działania niestety są bardzo kosztowne i zazwyczaj nie ograniczają się do zastosowania prostych zabezpieczeń fizycznych, administracyjnych i elektronicznych w zakresie komputerowych sieci i baz danych. W niektórych państwach jednak podejmowane są różne działania profilaktyczne przez służby państwowe, szczególnie wobec małych firm uczestniczących w produkcji związanej z wysoko rozwiniętą technologią. Realizowane jest to poprzez organizację pogadanek, wydawanie broszur na temat zagrożeń ze strony obcych wywiadów, jak i firm realizujących rozpoznanie konkurencyjne, opracowywanie i przekazywanie kierownictwom tych firm wytycznych do realizacji przedsięwzięć z zakresu bezpieczeństwa, tworzenie organizacji zrzeszających firmy w celu wymiany doświadczeń oraz dla tworzenia przez nie wspólnych systemów bezpieczeństwa, co powoduje, iż następuje obniżenie kosztów takich działań[125].

Na podstawie doświadczeń wynikających z rzeczywistych sytuacji jakie miały miejsce w zakresie prób rozpoznania firm oraz w skutek analizy metod stosowanych przez agendy wywiadowcze (wywiadownie gospodarcze, biura

[124] http://www.wywiad-gospodarczy.pl/2_1.html [dostęp: 10.04.2024].
[125] http://www.wywiad-gospodarczy.pl/2_2.html [dostęp: 10.04.2024].

konsultingowe, ratingowe) sporządzono wytyczne, które mają ułatwić im ochronę zasobów informacyjnych we własnych firmach, nie podlegających ochronie służb państwowych. Zgodnie z powyższym proponuje się następujące działania, które mogą być wprowadzane w każdej firmie bez konieczności dodatkowych nakładów na ten cel i realizowane bez udziału wyspecjalizowanej komórki kontrwywiadowczej[126]:

- **instruować pracowników,** zwłaszcza handlowców, jak powinni reagować na wszelkie próby indagacji;
- **zwracać baczną uwagę** na to, co mówi się dziennikarzom prasy branżowej;
- **rozsądne operowanie informacjami** o firmie (zwłaszcza w internecie);
- **oszczędne upublicznianie szczegółów technicznych** dotyczących budowy, technologii wytwarzania i programów marketingowych danego produktu itp.;
- **powstrzymywanie się od dyskusji** o problematyce technologicznej i objętej tajemnicą handlową w firmie na konferencjach z pracownikami innych firm, osobami obcymi i dziennikarzami;
- **dokładna analiza treści ogłoszeń** własnych zamieszczanych w prasie z ofertą zatrudnienia nowych pracowników – unikanie szczegółowego wymieniania zakresu wymaganych od kandydata umiejętności z zakresu obsługi specjalistycznego sprzętu i programów komputerowych;
- **właściwe obchodzenie się ze zdezaktualizowaną dokumentacją** – poddawanie jej procesowi niszczenia fizycznego;
- **kontrola dostępu pracowników** do kserokopiarek i innych urządzeń kopiujących dane.

Profesjonalnym zaleceniem dla przedsiębiorców, uwzględniającym całokształt zagadnień w obszarze ochrony firmy, jest metoda realizowana przez niemiecki Federalny Urząd Ochrony Konstytucji. W ramach działań prewencyjnych ochrony przed szpiegostwem wskazuje on niemieckim firmom przyjęcie następujących reguł działania, które nazwano „Złote reguły prewencji":

- nie oczekiwać biernie, aż nastąpi przypadek szpiegostwa w firmie;
- aktualne informacje o firmie przekazywać tylko kompetentnym partnerom;
- ochronę informacji uznawać za istotną część filozofii i strategii firmy;
- analizować regularnie standardy bezpieczeństwa,

[126] Tamże.

- realizować i permanentnie przestrzegać całościową koncepcję bezpieczeństwa;
- środki ochrony koncentrować na istotnych dla przyszłości firmy informacjach;
- kontrolować przestrzeganie i rezultaty wprowadzonych przepisów bezpieczeństwa – wszelkie incydenty przeciwko bezpieczeństwu poddawać sankcjom;
- wprowadzić do użycia „system wczesnego ostrzegania" w zakresie sygnalizowania „wycieków" informacji o wysoko rozwiniętych technologiach;
- konsekwentnie śledzić niejednoznaczne zdarzenia oraz konkretne wskazania na działalność przeciwko bezpieczeństwu – zwrócić się o profesjonalną pomoc do stosownych urzędów;
- ochrona informacji jest strategicznym czynnikiem sukcesu[127].

Jako główny element ochrony informacji w Polsce opracowano system ochrony informacji niejawnych, który tworzą:

- służby ochrony państwa (Agencja Bezpieczeństwa Wewnętrznego i Służba Kontrwywiadu Wojskowego);
- kierownicy jednostek organizacyjnych, w których informacje niejawne są wytwarzane, przetwarzane, przekazywane lub przechowywane;
- pełnomocnicy ds. ochrony informacji niejawnych;
- administratorzy systemu lub inspektorzy bezpieczeństwa teleinformatycznego.

Proces ochrony informacji na poszczególnych szczeblach gospodarki określa USTAWA z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych z późniejszymi zmianami, w której art. 1. 1. precyzuje zasady ochrony informacji, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania. Obejmuje:

- klasyfikowanie informacji niejawnych;
- organizowanie ochrony informacji niejawnych;
- przetwarzanie informacji niejawnych;

[127] http://www.wywiad-gospodarczy.pl/2_3.html [dostęp: 10.04.2024].

- postępowanie sprawdzające prowadzone w celu ustalenia, czy osoba nim objęta daje rękojmię zachowania tajemnicy;
- postępowania prowadzonego w celu ustalenia, czy przedsiębiorca nim objęty zapewnia warunki do ochrony informacji niejawnych (postępowanie bezpieczeństwa przemysłowego);
- organizacji kontroli stanu zabezpieczenia informacji niejawnych;
- ochrony informacji niejawnych w systemach teleinformatycznych;
- stosowania środków bezpieczeństwa fizycznego w odniesieniu do informacji niejawnych.

Zgodnie z ustawą odpowiedzialnym za ochronę informacji niejawnych jest kierownik jednostki organizacyjnej, w której informacje niejawne są wytwarzane, przetwarzane, przekazywane lub przechowywane. Dla realizacji powyższego kierownik jednostki organizacyjnej jest zobowiązany powołać pełnomocnika ds. ochrony informacji niejawnych, który tworzy pion ochrony w celu zapewnienia:

- ochrony informacji niejawnych;
- ochrony systemów i sieci teleinformatycznych;
- ochrony fizycznej jednostki organizacyjnej;
- kontroli ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji;
- okresowej kontroli ewidencji, materiałów i obiegu dokumentów;
- opracowania planu ochrony i nadzorowanie jego realizacji;
- szkolenia pracowników w zakresie ochrony informacji niejawnych.

Każda informacja (w tym szczególnie strategiczna) odgrywa w naszych czasach coraz większą rolę i w funkcjonowaniu gospodarki staje się ważniejsza niż dostęp do kapitału. Takie czynniki jak zaostrzająca się konkurencja, dereglamentacja wielu branż przemysłu czy rozwój wywiadu sprawiają, że informacja strategiczna jest coraz bardziej pożądana przez inne państwa czy firmy. Specjaliści od zabezpieczenia rodzimej gospodarki powinni być zatem przygotowani do organizowania skutecznej ochrony informacji strategicznej. Do zniechęcania wywiadów gospodarczych nie wystarczą już klasyczne metody zabezpieczenia informacji. Należy w tym miejscu zauważyć, że w obecnej dobie ochrona informacji nie polega tylko na niedopuszczeniu do jej przenikania do konkurencji, ale również na zapewnieniu sobie dobrej jakości informacji dostarczanych do nas.

Nie ma sposobu na pełną ochronę informacji. Uwzględniając obecne uwarunkowania, ochrona przed szpiegostwem stała się jeszcze trudniejsza, niż miało

to miejsce w przeszłości. Mimo tego walka z zagrożeniami przedstawionymi powyżej nie jest pozbawiona sensu. Stosowanie kompleksowych strategii zabezpieczania własnych danych (informacji) może zwiększyć koszty i ryzyko zbierania informacji przez przeciwnika.

Działania, które służą zabezpieczeniu własnych zasobów informacyjnych i jednocześnie neutralizowaniu działalności obcych służb wywiadowczych, jak i przeciwdziałaniu szpiegostwu i obcej penetracji, znane są powszechnie pod pojęciem kontrwywiadu. Służby realizujące tego typu zadania jeszcze do niedawna kojarzone były z organami państwowymi (kontrwywiad cywilny, wojskowy, policyjny), jednak obecnie coraz częściej spotyka się wyspecjalizowane instytucje prywatne, zajmujące się kompleksową ochroną kontrwywiadowczą firm, które w niektórych sytuacjach, ze względu na wąską specjalizację i niewielki obszar działania, osiągają lepsze rezultaty niż służby państwowe, realizujące ogromną gamę przedsięwzięć i działające w środowisku globalnym.

Z dużą dozą prawdopodobieństwa można postawić tezę, że **kontrwywiad jest równie stary, jak wywiad, gdyż ma tu zastosowanie reguła „akcji i reakcji"**. Jednakże był on zazwyczaj postrzegany jako przedsięwzięcie bardziej ogólne, realizujące cały wachlarz działań ochronnych. Jeżeli chodzi natomiast o wyspecjalizowane działania kontrwywiadowcze w zakresie przemysłu, które były realizowane wyłącznie dla ochrony jednej z firm, to pierwszym ich organizatorem – jak podaje literatura – był Alfred Krupp, przywiązujący duże znaczenie do kształtowania lojalności personelu zatrudnionego w jego zakładach oraz do stosowania technicznych metod ochrony technologii. Dalszy rozwój tych działań, wymuszony czynnikami zewnętrznymi, tj. rozrostem zasobów informacyjnych, które muszą być poddawane ochronie z jednej strony, a z drugiej wzrastającą i przybierającą coraz to nowe metody działalnością wywiadowczą, spowodował ukształtowanie się ogólnych zagadnień w tym obszarze, jakimi są polityka bezpieczeństwa informacji oraz strategia kontrwywiadowcza.

3. CYBERTERRORYZM I PRZESTĘPCZOŚĆ KOMPUTEROWA

3.1. Cyberterroryzm – definicja i zakres

Szybki rozwój technologiczny i związana z nim powszechna dostępność sieci spowodowały ogromne przeobrażenia w wielu dziedzinach życia. Nie ominęło to także gospodarki światowej, wypływając jednocześnie na zmianę form popełniania przestępstw. Nowocześni, cybernetyczni przestępcy, często traktujący łamanie prawa w sieci jak zabawę lub kolejny sprawdzian własnych umiejętności, stali się zmorą organów ścigania. Ilość przestępstw popełnianych przy użyciu komputerów stale rośnie.

Działalność różnych grup terrorystycznych ma na celu zniszczenie zachodniego modelu życia, i takie oddziaływanie, aby stopniowa jego degeneracja stała się nowym, skutecznym sposobem walki terrorystycznej. Zniszczenie lub choćby osłabienie zaufania obywateli do instytucji państwowych, poczucia bezpieczeństwa czy wiarygodności informacji przekazywanych przez media znacznie przybliża terrorystów do destabilizacji społeczeństwa i jego stylu życia. To szybki rozwój technologiczny i związana z nim powszechna dostępność sieci spowodowały ogromne przeobrażenia w gospodarce i społeczeństwie, wypływając jednocześnie na zmianę sposoby prowadzenia walki o swoje cele. Czasami zdarza się, że początkujący cyberterroryści traktują łamanie prawa w sieci jak zabawę lub kolejny sprawdzian własnych umiejętności.

Definicji cyberterroryzmu jest tak wiele, jak wielu jest specjalistów zajmujących się tą problematyką, jednak najprostszy i najtrafniejszy podaje, że przez cyberterroryzm rozumiemy politycznie motywowany atak na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub

wymuszenia na rządzie i ludziach daleko idących politycznych celów, a takie wykorzystanie internetu przez organizacje terrorystyczne do komunikowania się, propagandy i dezinformacji.

Należy przy tym zauważyć, iż cyberterroryzm jest jednocześnie zaawansowaną technologicznie odmianą tradycyjnego terroryzmu, jak i jednakże składowych technik i narzędzi wykorzystywanych do zastraszania ludzi lub wymuszania ustępstw politycznych na danych władzach. Często mamy do czynienia z zacieraniem granic między cyberprzestrzenią i cyberterroryzmem. Osoby dokonujące ataków w cyberprzestrzeni dzielą się na: aktywistów (prowadzących niedestrukcyjną działalność, w ramach której internet służy wsparciu danej kampanii), haktywistów (są połączeniem aktywistów i hakerów, wykorzystujących metody hakerskie przeciwko określonym celom w sieci, by zakłócić funkcjonowanie internetu, nie powodując przy tym poważnych strat), cyberterrorystów (różnią się od aktywistów celem swoich działań. Ich celem jest wyrządzenie możliwie największych strat wśród swoich wrogów, włączając w to ofiary ludzkie). Celowe działania mogą przyjmować formę:

- zakłócenia działania systemów;
- nieupoważnionego wprowadzania lub kopiowania danych;
- łamania zabezpieczeń, co pozwala na przejęcie kontroli nad poszczególnymi elementami infrastruktury (np. na wypadek wojny).

Po tę ostatnią metodę mogą sięgać służby specjalne nieprzyjaźnie nastawionych państw oraz organizacje terrorystyczne. Z kolei grupy przestępczości zorganizowanej mogą być zainteresowane wykradaniem danych lub dokonywaniem nieupoważnionych zmian, np. w systemach i sieciach instytucji finansowych.

Mark Pollit, specjalista FBI, **definiuje cyberterroryzm jako przemyślany, politycznie umotywowany atak, skierowany na informacje, systemy komputerowe, programy i bazy danych, mający za zadanie zniszczenia celów niewojskowych, przeprowadzony przez grupy obce narodowościowo lub przez tajnych agentów.** Z kolei Amerykański Departament Sprawiedliwości za **terroryzm sieciowy uznaje użycie technologii informatycznej do rozpowszechniania programów, ataków na sieci, systemy komputerowe i infrastrukturę telekomunikacyjną w celu wymiany informacji bądź przesłania groźby.** Narodowe Centrum Ochrony Infrastruktury Stanów Zjednoczonych (US National Infrastructure Protection Center) uważa, że **cyberterroryzm to akt przemocy przeprowadzony przy użyciu komputerów i innych technologii informatycznych, w celu zniszczenia lub zakłócenia działania systemów**

informatycznych, wywołujący panikę i zamieszanie, a tym samym poczucie zagrożenia wśród ludności, w celu zmuszenia rządu lub innych organizacji do spełnienia politycznych, społecznych czy też ideologicznych żądań. W książce *Trzecia fala* Alvin Toffler definiuje **cyberterroryzm jako nowy kierunek destruktywnego oddziaływania, którego istotą jest wykorzystywanie informacji jako narzędzi walki**. Zagrożenia, które niesie ze sobą, w równym stopniu dotyczyć mogą państw tzw. trzeciej fali cywilizacyjnej – społeczeństw postindustrialnych.

Cyberterroryzm stanowi nowe, realne zagrożenie bezpieczeństwa państwa i społeczeństwa. Aby skutecznie przeciwdziałać tym zagrożeniom należy je rozpoznać i przygotować niezbędne siły i środki, które pozwolą identyfikować zagrożenia oraz zastosować odpowiednie metody związane z cyberterroryzmem. Tym, co cechuje cyberterrorystów, jest zachowywanie anonimowości. Cyberterroryści sprytnie ukrywają swoją tożsamość, zzęsto podając się za osoby, którymi nie są.

Cyberterroryzm to terroryzm dokonywany, planowany i koordynowany w cyberprzestrzeni, tzn. za pomocą komputerów połączonych do sieci komputerowych. Obecnie prawie każda grupa terrorystyczna utrzymuje więcej niż jedną stronę WWW, często w wielu językach. Na stronach tych umieszczona jest przede wszystkim historia organizacji i jej działalność, opis politycznych i ideologicznych celów, biografie przywódców, krytyka działania wrogów, a także informacje o przeprowadzonych akcjach. Na tych stronach WWW umieszcza się praktycznie wszystko: ogłoszenia, artykuły, komentarze, zdjęcia, filmy, prowadzi kampanie informacyjne czy rekrutacyjne. Najczęściej w ten sposób publikowane są groźby i informacje o przeprowadzonych akcjach, żądania porywaczy, zdjęcia przetrzymywanych zakładników, wreszcie filmy dokumentujące egzekucje. Na stronach internetowych umieszczane są dostępne linki zawierające informacje o rachunkach bankowych, na które można wpłacać pieniądze. Wykorzystywane do gromadzenia funduszy konta bankowe teoretycznie należą do niezwiązanych z terroryzmem fundacji, organizacji humanitarnych czy też finansowych.

Do tej kategorii zaliczamy używanie e-maili do utrzymywania łączności między konspiratorami oraz dzielenia się informacjami służącymi do przygotowania aktów przemocy, a także używanie serwisów WWW do rekrutacji członków grup terrorystycznych. Można do tej grupy zaliczyć także sabotaż systemów komputerowego sterowania ruchem lotniczym w celu doprowadzenia do zderzeń samolotów lub ich rozbicia, infiltrowanie systemów komputerowych

nadzorujących procesy uzdatniania wody pitnej w celu spowodowania jej zatrucia, włamania do szpitalnych baz danych i zmienianie bądź usuwanie danych w celu doprowadzenia do stosowania niewłaściwych procedur medycznych wobec pacjenta lub pacjentów, doprowadzanie do załamań systemów zasilania w energię elektryczną, które może prowadzić do wyłączenia klimatyzacji latem i ogrzewania zimą lub powodować śmierć ludzi podłączonych do respiratorów w prywatnych domach, niewyposażonych w zapasowe źródła energii[128].

3.2. Przestępczość komputerowa

Wraz z rozwojem technologii informatycznych wystąpiły problemy z niewłaściwym wykorzystywaniem elektronicznego przetwarzania danych. Tak ujawnił się nowy obszar przestępczej działalności. Na rozwój przestępczości komputerowej wpływ mają:

- dostępność rozproszonych sieciowych ośrodków obliczeniowych;
- rozległość sieci;
- brak odpowiedzialności (lub możliwości realnego jej przypisania) za działania związane z obsługą komputerów i telekomunikacją.

Za wzrost przestępczości komputerowej odpowiada:

- zgodność i duża przystosowalność coraz większej ilości zdalnych systemów;
- dostępność taniego sprzętu i oprogramowania;
- standaryzowanie sprzętu i oprogramowania.

Wzrost liczby przestępstw w cyberprzestrzeni zależny jest od kompetencji hackerów, dostępu do systemów i ich funkcjonowania oraz ujednolicania narzędzi internetowych.

Samo środowisko pracy ma wpływ na łatwość dokonania przestępstw. Poziom zabezpieczeń sieciowych i integralności, poufności sieci jest w dalszym ciągu bardzo niski. Elektroniczne przechowywane dane o przeprowadzanych transakcjach bankowych, bazy danych kontrahentów, zamówienia internetowe, ważne umowy czy też dokumentacja osobista stają się łakomym kąskiem dla konkurencji. Należy przy tym poruszyć kwestię wiarygodności i poufności transmisji oraz zabezpieczeń osobistych praw użytkowników sieci. Trzeba uwzględnić bezpieczeństwo informacyjne i skupić się na kwestiach legalności dokumentacji

[128] D. L. Shinder, E. Tittel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Helion, Gliwice 2004, s. 37.

elektronicznej oraz operacji dokonywanych w sieci. Warto zadbać o autoryzacje dokonywane za pomocą podpisu elektronicznego, personalizowany dostęp do sieci, system prywatnych i publicznych kluczy kryptograficznych. Przestępczość w sieci skupia się w dużej mierze na funkcjonowaniu państwa w aspekcie prowadzenia nielegalnych operacji finansowych. Większość ważnych informacji jest już przechowywana w postaci elektronicznej. Często do wykonania tego typu zadań są werbowani byli pracownicy firm lub instytucji. Kusi ich magia szybkich i dużych pieniędzy za przeprowadzoną akcję. Nowym „zjawiskiem" są crackerzy, czyli osoby postronne, które bez posiadania uprawnień uzyskują dostęp do systemu celem dokonania w nim zmian, zmiany lub wykasowania istotnych danych. Crackerzy działają dla rozrywki oraz w celu sprawdzenia swojej wiedzy i posiadanych umiejętności. Crackerzy działają w zwartych, międzynarodowych grupach przestępczych. Najbardziej narażone na ataki ze strony cyberterrorystów są systemy informatyczne powiązane z zarządzaniem ruchem powietrznym oraz lądowym; związane z bazami danych firm, instytucji oraz organizacji, w tym służb ratowniczych i jednostek zarządzania kryzysowego oraz należące do grupy sektora przemysłowego, dystrybucyjnego (w tym energia elektryczna, woda, ropa, gaz) i finansowego.

Cechy wspólne wszystkich cyberataków to:

- trudność wykrycia mocodawców ataku spowodowana tym, że zleceniodawca znajduje wykonawców zamachu, często obywateli innego kraju, lub przeprowadza je samodzielnie korzystając z publicznych miejsc z dostępem do sieci Internet (np. kafejki internetowe);
- wciąż bardzo wysoki stopień anonimowości zamachowców;
- ogromna siła oddziaływania społecznego, ataków dokonywanych w cyberprzestrzeni;
- niebywała łatwość przeprowadzenia zamachu w cyberprzestrzeni, przez co niewielkie często państwa, o małym znaczeniu na arenie międzynarodowej, stają się „języczkiem uwagi" całego świata, stanowiąc realne zagrożenie dla światowych elit rządzących, potęg militarnych i herosów ekonomicznych;
- niezbyt wysokie koszty dokonania cyberataku[129].

Objawy typowych infekcji komputerowych to:

[129] Zob. M. Łapczyński, *Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem*, Komentarz Międzynarodowy Pułaskiego, http://www.stosunkimiedzynarodowe.info/artykul,393,Zagrozenie_cyberterroryzmem_a_polska_strategia_obrony_przed_tym_zjawiskiem [dostęp: 11.11.2014].

- spadek prędkości łącza internetowego;
- spowolnienie działania systemu;
- odmowa dostępu do stron podmiotów odpowiedzialnych za bezpieczeństwo użytkownika w sieci, w tym do stron Microsoftu, firm antywirusowych;
- zdalne sterowanie komputera, co świadczy o komunikacji komputera z zewnętrznym serwerem.

Wirtualne przestępstwa finansowe są łakomym kąskiem dla cyberprzestępców. Na ten stan rzeczy wpływa zbyt niska wykrywalność tego typu przestępstw. Poprzez kradzież prywatnych danych cyberzłodziej wystawia loginy i hasła dostępu do kont ofiar w formie ofert na „czarnym rynku". Tak tożsamość ofiar wystawiana jest na sprzedaż. „Podstawienie" fałszywej strony bankowej to jedna z popularniejszych metod uzyskania danych dostępu do internetowych kont bankowych. Cyberprzestępcy w tym wypadku rozsyłają e-maile zawierające link do witryny bankowej z prośbą o zalogowanie się celem dokonania weryfikacji danych. Tak przestępcy gromadzą bazy danych, które następnie wykorzystują, dokonując dla przykładu zakupów obciążając rachunki ofiar. Trzeba zawsze bardzo ostrożnie posługiwać się własnymi danymi. Należy przed wpisaniem informacji sprawdzić stan ochrony strony internetowej. Warto przy tym pamiętać, iż instytucje finansowe nigdy nie wymagają wirtualnego potwierdzenia danych od swoich klientów.

Cybersquatting polega na wykupieniu za wysoką cenę praw do domeny internetowej. Przestępcy rejestrowali na danym rynku określone domeny z nazwą popularnej firmy lub rozpoznawalnego znaku towarowego.

Tipesquatting jest przestępstwem, które polega na nieznacznej zmianie liter (wielkości lub ilości) w nazwie domeny, tak aby łudząco przypominała nazwę oryginalnej domeny i była wraz z nią znajdowana przez wyszukiwarki. Przy tego typu przestępstwach należy wykazać celowość działań przestępcy, a więc to, że kierował się on chęcią zysku, tym, że chciał wymusić zakup domeny przez daną firmę, organizację, instytucję czy osobę.

Cyberprzestępczość stanowi ogromny problem. W firmach zachodzi rewolucja technologiczna, jednak zmiany w systemach ochrony danych nadal są o krok za nimi. Głównym celem ataków jest sektor finansowy. Zagrożone cyberprzestępstwami są sektory: energetyczny, technologiczny, ochrony zdrowia i medyczny. Cyberprzestępcy narażają firmy, instytucje oraz organizacje nie tylko na straty finansowe, ale również na utratę reputacji, przerwy w działalności, kary czy kradzież tajemnicy. Wzrasta zagrożenie działaniami, które mają w efekcie

końcowym doprowadzić do dezorganizacji kluczowych systemów informacyjnych instytucji rządowych oraz sektora prywatnego za pośrednictwem oddziaływania na system bezpieczeństwa państwa, przeszukiwania baz danych, wprowadzania chaosu i budzeniu poczucia zagrożenia wśród obywateli.

3.3. Cyberterroryzm i przestępczość komputerowa jako zagrożenie bezpieczeństwa

Systemy i sieci teleinformatyczne zalicza się do infrastruktury mającej znaczenie strategiczne. Stanowią one w obecnych czasach niezwykle istotne ogniwo zapewnienia bezpieczeństwa i ekonomicznego dobrobytu państwa oraz jego efektywnego funkcjonowania.

Pod pojęciem cyberterrorymu należy rozumieć wszelkie działania o charakterze kryminalnym lub terrorystycznym realizowane w cyberprzestrzeni[130]. W zestawieniu działań o charakterze cyberterrorystycznym spotkać możemy te, które skierowane są do odbiorcy indywidualnego oraz ataki na grupy czy też dane Państwa. Wciąż narastający problem cyberterroryzmu niejako wymusza stosowanie oprogramowania zabezpieczającego przed atakami ze strony internetowych terrorystów. Występujące zagrożenia cyberterrorystyczne powodują zwiększenie działań prewencyjnych w postaci szkoleń, opracowywania i wprowadzania w życie procedur ochronnych.

Klasyczny atak cyberterrorystyczny polega na uderzeniu w oprogramowanie przeciwnika (ang. *software*). Różnorodność możliwych metod działania jest jednak na tyle duża, że trudno jest stworzyć jednolitą listę terminów wyczerpującą wszystkie możliwe sposoby prowadzenia tego typu akcji w cyberprzestrzeni. W literaturze występują więc różnorodne próby ich kategoryzacji. William R. Cheswick i Steven Bellovin proponują listę 7 kategorii:

- ***Stealingpasswords*** – metody polegające na uzyskaniu haseł dostępu do sieci;
- ***Social engineering*** – wykorzystanie niekompetencji osób, które mają dostęp do systemu;
- ***Bugs and backdoors*** – korzystanie z systemu bez specjalnych zezwoleń lub używanie oprogramowania z nielegalnych źródeł;

[130] T. Trejderowski, *Kradzież tożsamości. Terroryzm informatyczny. Cyberprzestępstwa. Internet. Telefon. Facebook, Eneteia*, Wydawnictwo Psychologii i Kultury, Warszawa 2013, s. 165.

- ***Authenticationfailuires*** – zniszczenie mechanizmu używanego do autoryzacji;
- ***Protocolfailures*** – wykorzystanie luk w zbiorze reguł sterujących wymianą informacji pomiędzy dwoma lub wieloma niezależnymi urządzeniami lub procesami;
- ***Information leakage*** – atakujący zdobywa informacje dostępne tylko dla administratora, niezbędne dla poprawnego funkcjonowania sieci;
- ***Denial of Service*** – uniemożliwienie użytkownikom korzystania z ich systemu.

Fred Cohen ze względu na skutek cyberataku wyróżnia kategorie:
- ***Corrupition*** – nieuprawniona zmiana informacji;
- ***Leakage*** – informacja znalazła się tam, gdzie być nie powinna;
- ***Denial*** – kiedy komputer lub sieć nie nadają się do użytkowania.

Peter G. Neumann i Donn Parker proponują kategoryzację opartą na danych empirycznych:
- ***External Information Theft*** – przeglądanie oraz kradzież informacji przez osobę spoza systemu;
- ***ExternalAbuse of Resources*** – zniszczenie twardego dysku;
- ***Masquerading*** – podawanie się za kogoś innego;
- ***Pest Programs*** – zainstalowanie złośliwego programu;
- ***Bypassing Authenticationor Authority*** – złamanie haseł;
- ***Authority Abusc*** – fałszowanie danych;
- ***Abuse Through Inaction*** – umyślne złe zarządzanie;
- ***Indirect Abuse*** – używanie innych systemów do stworzenia złośliwych programów.

Carl E. Landwehr, Alan R. Buli, John P. Mcdermott i William S. Choi proponują stworzenie matrycy pojęciowej opartej na trzech wymiarach:
- ***Genesis*** – wykorzystanie ,,dziur" w zabezpieczeniach (*securityflaw)*;
- ***Time of Introduction*** – czas ,,życia" oprogramowania i sprzętu komputerowego;
- ***Location*** – lokalizacji ,,dziur" w oprogramowaniu i sprzęcie komputerowym.

William Stallings opracował klasyfikację opartą na działaniu:
- ***Interruption*** – zabezpieczenie systemu zostało zniszczone lub jest niemożliwe do zastosowania;
- ***Interception*** – nieuprawniona grupa zdobyła dostęp do zabezpieczeń;

- ***Modification*** – nieuprawniona grupa nie tylko zdobyła dostęp, ale także manipulowała zabezpieczeniem;
- ***Fabrication*** – nieuprawniona grupa wprowadziła sfałszowany obiekt do systemu.

Przy definiowaniu cyberterroryzmu nie sposób nie wspomnieć o wieloskalowości cyberterroryzmu, czyli prowadzonych na dużą skalę, nie rzadko wobec kilku celom jednocześnie, nadzorowanych ataków grup hackerskich oraz wojnach międzypaństwowych prowadzonych za pomocą sieci Internet. Pojęcie „cyberterroryzmu" zestawiane jest zawsze obok pojęcia „terroryzmu" i „cyberprzestrzeni". Cyberterroryzm wykorzystuje bezprzewodowe sieci na dwa sposoby:

- do przeprowadzenia ataku socjotechnicznego na wybrany cel i odsunięcia od siebie podejrzeń policji – użytkownicy sieci stają się podejrzanymi;
- w celu zaatakowania samej sieci, przechwytywania haseł, loginów, danych kart kredytowych, instalacji botów do dalszych ataków – jej użytkownicy stają się ofiarami[131].

Ataki cyberterrorystów mogą zostać skierowane na:

- telekomunikację – sieci komputerowe (komercyjne, akademickie, wojskowe), linie telefoniczne, satelity;
- system energetyczny, w tym na wytwarzanie i dystrybucję energii, przemysł energetyczny, transport i magazynowanie surowców służących produkcji energii;
- przemysł gazowy i rafineryjny, to jest produkcja, magazynowanie i transportowanie gazu ziemnego oraz ropy naftowej;
- system bankowy i finansowy, uderzając w system przepływu kapitałów;
- transport lotniczy, kolejowy, morski, rzeczny oraz drogowy, osobowo-towarowy oraz wsparcie logistyczne tychże systemów;
- zaopatrzenie w wodę, to jest ujęcia wody, zbiorniki wodne, wodociągi, systemy filtracji i uzdatniania wód;
- służby ratownicze;
- funkcjonowanie władzy i służb publicznych;
- działania mające na celu pozyskanie informacji wojskowych, ekonomicznych czy też technologicznych.

[131] T. Trejderowski, *Kradzież tożsamości. Terroryzm informatyczny. Cyberprzestępstwa. Internet. Telefon. Facebook, Eneteia*, Wydawnictwo Psychologii i Kultury, Warszawa 2013, s. 167-168.

Ataki cyberterrorystyczne zagrażają każdemu elementowi wchodzącemu w skład infrastruktury krytycznej państwa.

Ponieważ nie wszystkie organizacje terrorystyczne dysponują możliwościami, środkami finansowymi i umiejętnościami do przeprowadzenia ataku w cyberprzestrzeni, dlatego też często dochodzi do użycia kombinacji starych i nowych metod działania. Naukowcy z Center for the Study of Terrorism and Irregular Warfare w The Naval Postgraduate School w Monterey w Kalifornii zdefiniowali 3 poziomy zagrożenia związanego z cyberterroryzmem:

- **pierwszy poziom zagrożenia Simple-unstructured**. Cyberterroryści dokonują prostych włamań do indywidualnych systemów informacyjnych, stosując „narzędzia internetowe", skonstruowane przez kogoś innego; organizacja terrorystyczna ma niewielką zdolność analizy celów, będących przedmiotem ataku, dowodzenia, kontroli oraz uczenia się nowych metod atakowania w cyberprzestrzeni;
- **drugi poziom zagrożenia Advanced-structured**. Cyberterroryści dokonują bardziej skomplikowanych ataków przeciwko złożonym systemom i sieciom komputerowym; posiadają możliwość modyfikacji lub tworzenia własnych „narzędzi", służących do atakowania w cyberprzestrzeni; mają zdolność analizy celów będących przedmiotem ataku, dowodzenia, kontroli oraz uczenia się nowych metod atakowania;
- **trzeci poziom zagrożenia Complex-coordinated**. Cyberterroryści dokonują skoordynowanych ataków, obliczonych na totalną destrukcję zintegrowanego systemu obronnego; mają możliwość tworzenia skomplikowanych „narzędzi", służących do niszczenia celów w cyberprzestrzeni oraz analizy celów będących przedmiotem ataku, dowodzenia, kontroli oraz samodoskonalenia[132].

Ataki na systemy informatyczne mogą być połączone z innymi rodzajami ataków terrorystycznych. Mogą być one skierowane w żywotnie ważne systemy, takie jak obsługa ruchu lotniczego czy dystrybucja energii elektrycznej. Biorąc pod uwagę rosnącą skalę tego zjawiska i coraz poważniejsze jego skutki, brak podjęcia dobrze zaplanowanego, usystematyzowanego procesu jego zwalczania może mieć bardzo poważne konsekwencje. W naszym kraju już dziś istnieje wiele systemów informatycznych. Zakłócenie ich działalności mogłoby odbić się

[132] R. Białoskórski, *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa 2011, s. 61.

negatywnie na funkcjonowaniu państwa i bezpieczeństwie obywateli (np. systemy bankowo-finansowe, ubezpieczeń społecznych). Jeszcze poważniejsze są potencjalne zagrożenia dla systemów działających w sektorze energetycznym, wodociągowym, gazociągowym czy w służbach ratunkowych .

W celu uzyskania cyberodporności należy zorganizować skuteczne działania oparte na następujących fundamentach (założeniach):

- każda organizacja została lub zostanie zaatakowana przez cyberprzestępców;
- być przygotowanym do skutecznych szybkich reakcji na incydenty – pozwalające organizacji przetrwać nieuchronny atak;
- prowadzić ciągłą edukację, doskonalenie i ćwiczenia – budujących stan gotowości organizacji do zmierzenia się z nadchodzącym atakiem;
- współdziałaniu z partnerami biznesowymi, ułatwiającym pozyskiwanie informacji oraz czerpanie wiedzy z doświadczeń innych organizacji.

4. WSPÓŁCZESNE ZAGROŻENIA CYBERNETYCZNE A TELEINFORMATYCZNE REZERWY (ZASOBY) STRATEGICZNE PAŃSTWA POLSKIEGO

4.1. Potencjał teleinformatyczny

Celem tego rozdziału jest przedstawienie najważniejszych zagadnień związanych z teorią i praktyką zagrożeń cyberprzestępczości i cyberterroryzmu oraz wskazanie w oparciu o jakie mechanizmy (bazy danych) powinno przebiegać kształtowanie się rezerw (zasobów) strategicznych w obszarze teleinformatyki. Ponieważ obszary związane z obronnością i bezpieczeństwem są szczególnie zagrożone, zapobieganie i minimalizowanie zagrożeń jest w tych obszarach szczególnie istotne. W opracowaniu dokonano analizy sieci komputerowych, systemów, sprzętu i oprogramowania z punktu widzenia potencjału infrastruktury krytycznej państwa. Analiza pozwoliła na wskazanie, że współczesnym zagrożeniom przestępczości komputerowej, cyberterroryzmu można się skutecznie przeciwstawić lub je minimalizować. Odpowiedni poziom zabezpieczeń teleinformatycznych Polski możemy osiągnąć ściśle współpracując z systemami bezpieczeństwa teleinformatycznego UE i NATO.

Główną metodą badawczą zastosowaną w opracowaniu jest analiza literatury przedmiotu oraz prowadzone badania z tego zakresu, jakie autor prowadził w trakcie pracy w Departamencie Informatyki i Telekomunikacji oraz Departamencie Transformacji MON. Oprócz analizy zastosowano także metody wnioskowania i syntezy, jak również skorzystano z opinii ekspertów krajowych i zagranicznych. W opracowaniu postawiono hipotezę, która zakłada że planowanie, gromadzenie i racjonalne, skuteczne zastosowanie strategicznych rezerw

(zasobów) teleinformatycznych powinno pozwolić na ich efektywne wykorzystanie w wielu dziedzinach. Wiarygodne centralnie zgromadzone informacje (bazy wiedzy) zawarte w sprawnie i bezpiecznie funkcjonujących systemach teleinformatycznych o rezerwach (zasobach) strategicznych pozwolą na zabezpieczenie funkcjonowania państwa w różnych sytuacjach zagrożeń. Wiadomości ujęte w tym rozdziale powinny stanowić inspirację dla dalszych poszukiwań (badań) prawidłowości funkcjonowania teleinformatycznych rezerw (zasobów) strategicznych i ich efektywnego i skutecznego wykorzystania. Wykorzystanie teleinformatycznych rezerw (zasobów) strategicznych nie jest opisane w dostępnej literaturze. Uwzględniając powyższe uwarunkowania należy zaapelować do naukowców i decydentów, wskazując na potrzebę zajęcia się właśnie tym obszarem tematycznym i podjęcia działań zmierzających do identyfikacji tych zagadnień. Taką próbą jest właśnie ten rozdział.

4.2. Teleinformatyka na potrzeby obronności i bezpieczeństwa

Rezerwy (zasoby) strategiczne w każdym obszarze są istotnym elementem kształtowania obronności i bezpieczeństwa. Bez nich nie można osiągnąć zakładanych celów, reagować na zagrożenia kryzysowe czy wojenne. Są one elementem zabezpieczenia funkcjonowania państwa, a w tym szczególnie ludności i gospodarki. Stąd też powinny skutecznie wspomóc społeczeństwo i gospodarkę w chwili szczególnego zagrożenia. Ich skuteczność zależy od asortymentu oraz uwarunkowań w jakich zostały zastosowane.

Teleinformatyka, **ICT** (akronim do ang. *information and communication technologies*) – pojęcie obejmujące szeroki zakres wszystkich technologii umożliwiających manipulowanie i przesyłanie informacji[133]. Infrastruktura teleinformatyczna państwa to urządzenia i systemy zorganizowane w sieci

[133] https://www.gov.pl/static/mi_arch/media/3510/Slownik_pojec_SRT.pdf *Słownik pojęć strategii rozwoju transportu do 2020 roku*, Ministerstwo Transportu, Budownictwa i Gospodarki Morskiej, s. 26 [dostęp: 12.04.2024].

telekomunikacyjne[134], teleinformatyczne[135]. Są one odpowiednio zabezpieczone i zasilane wraz z miejscami oraz obiektami ich eksploatowania i świadczą usługi na terenie kraju. Sieć telekomunikacyjna to zespół węzłów (central, systemów komutacyjno-sterujących) i linii telekomunikacyjnych rozmieszczonych w określonym obszarze wraz z systemami zarządzającymi i zabezpieczającymi jej funkcjonowanie, świadcząca usługi telekomunikacyjne użytkownikom (abonentom).

Do rezerw (zasobów) strategicznych w obszarze teleinformatyki należy zaliczyć: obiekty, sieci, systemy, sprzęt, wyposażenie i oprogramowanie oraz specjalistów przygotowanych do ich obsługi. Elementy te powinny zostać objęte szczególną troską państwa. W wielu przypadkach łączy się to ściśle z przepisami dotyczącymi ochrony tajemnicy w systemach i sieciach teleinformatycznych oraz ochroną danych osobowych.

Nowe technologie teleinformatyczne wpływają na kształt obronności i bezpieczeństwa. Jak te zagadnienia w dzisiejszych czasach są niezwykle istotne, możemy zaobserwować analizując pojawiające się zagrożenia. Dlatego każde państwo ma obowiązek monitorować te zagrożenia i po ich wykryciu skutecznie im przeciwdziałać. Oczywiście rezerwy (zasoby) strategiczne, potencjał teleinformatyczny może być wykorzystany czy uruchamiany dla zwiększenia

---

[134] **Sieć telekomunikacyjna** – obiekt techniczny będący zbiorem łączy telekomunikacyjnych i innych urządzeń wymaganych do przysyłania informacji pomiędzy dwoma lub więcej węzłami sieci. W ogólności każda sieć telekomunikacyjna składa się z trzech płaszczyzn (lub odrębnych struktur) współpracujących ze sobą:
- płaszczyzna sterowania jest częścią sieci przenoszącą informacje sterujące;
- płaszczyzna użytkowa lub płaszczyzna danych przenosi ruch użytkowników sieci czyli tych, którzy korzystają z jej usług;
- płaszczyzna zarządzania jest częścią sieci realizującą ruch związany z eksploatacją sieci i administrowaniem.

W polskim prawie pojęcie sieć telekomunikacyjna zdefiniowane zostało w ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, gdzie oznacza: „systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju". https://pl.wikipedia.org/wiki/ Sie%C4%87_telekomunikacyjna [dostęp: 12.04.2024].

[135] **Sieć teleinformatyczna** w każdym domu, biurze, czy przedsiębiorstwie jest integralną częścią prawidłowo i niezawodnie działającego systemu informatycznego i telefonicznego. **Podstawową funkcją takiej sieci** jest połączenie wszystkich urządzeń w jeden sprawnie działający system. Nowoczesne okablowanie obiektu musi uwzględniać wszystkie bieżące potrzeby, a także wybiegać w przyszłość. Okablowania dedykowanego (tzn. np. osobno na potrzeby sieci telefonicznej – okablowanie teletechniczne, na potrzeby sieci komputerowej – okablowanie komputerowe) na rzecz okablowania teleinformatycznego, które jest uniwersalne i umożliwia elastyczne wykorzystanie na potrzeby podłączenia jak największej ilości mediów. http://www.instalacje-instalacje.com.pl /teleinformatyczna.php [dostęp: 10.04.2024].

efektywności działania posiadanych sił i środków w różnych okolicznościach, w tym szczególnie w czasie klęsk żywiołowych, kryzysu czy wojny.

Wszystkie działy gospodarki narodowej są szczególnie uzależnione od systemów informatycznych. Stanowią one także kluczowe elementy w procesie podejmowania decyzji w wielu organizacjach odpowiedzialnych za bezpieczeństwo wewnętrzne i zewnętrzne. Ich dotychczasowy rozwój i zakres wdrożeń pozwala prognozować, że obszary zastosowań informatycznych będą obejmować nowe przestrzenie informacyjne. Obecnie stworzono niemalże nieograniczony dostęp do zbiorów jawnych informacji: finansowych, przemysłowych, marketingowych, technologicznych, wojskowych, policyjnych i innych. Każda działalność związana z obronnością i bezpieczeństwem narodowym staje się coraz bardziej zależna od swobodnego przepływu informacji i od prawidłowego funkcjonowania systemów bazujących na tych informacjach.

W przypadku systemów odpowiedzialnych za obronność i bezpieczeństwo będą to głównie administracja państwowa i terenowa, np. Policja, Straż Graniczna, Służby Specjalne, Państwowa Straż Pożarna, Straż Więzienna i prokuratury, Państwowe Ratownictwo Medyczne, służby i jednostki Ministerstwa Obrony Narodowej, służby Ministerstwa Transportu, Ochotnicza Straż Pożarna włączona do krajowego Systemu Ratowniczo-Gaśniczego, służby i inspekcje (sanitarno-epidemiologiczne, weterynaryjne, ochrony środowiska, gospodarki wodnej), organizacje pozarządowe itp.

W celu zapewnienia sprawnego funkcjonowania tych systemów należy wprowadzić odpowiednią politykę bezpieczeństwa informacyjnego, zapewniającą ochronę istniejących sieci, systemów i zbiorów informacji w nich zawartych. Powinna ona gwarantować wszystkim podmiotom – uczestnikom tego procesu pełne bezpieczeństwo informacyjne, równocześnie zapewniając swobodę rozwoju „społeczeństwa informacyjnego”[136].

W dzisiejszych czasach istnieje silne zapotrzebowanie na podjęcie dyskusji jak w nowoczesnym państwie wykorzystać efektywnie potencjał teleinformatyczny dla skutecznego przeciwdziałania zagrożeniom, jakie niesie za sobą XXI wiek w czasie pokoju, kryzysu czy wojny. Ponadto jakie i w jakiej ilości gromadzić rezerwy (zasoby) teleinformatyczne. Jak te rezerwy (zasoby) ewidencjonować i jakie stosować normatywy oraz kto ma ponosić koszty z tym

[136] T. Jemioła, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, WSIZiA, Warszawa 2009, s. 511.

związane. Dyskusji i ustawowych rozwiązań domaga się zarówno świat nauki, dydaktyka, jak również praktycy, którzy widzą w tym potencjale duże możliwości.

W Polsce informacje o zasobach teleinformatycznych gromadzi indywidualnie wiele instytucji, w tym Urząd Komunikacji Elektronicznej, Ministerstwo Infrastruktury oraz Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Obrony Narodowej i inne. Biorąc pod uwagę rosnące zainteresowanie użytkowanym potencjałem na poszczególnych szczeblach organizacyjnych oraz stały rozwój potencjału teleinformatycznego, już na wstępie należy stwierdzić, że baza informacyjna o zasobach teleinformatycznych powinna mieć charakter krajowy.

Organizacje i instytucje na poszczególnych szczeblach organizacyjnych państwa odpowiedzialne za zapewnienie wewnętrznego i zewnętrznego bezpieczeństwa i obronności powinny być szczególnie zainteresowane diagnozą i oceną istniejącego systemu teleinformatycznego oraz wskazaniem kierunków dalszego ich doskonalenia. Dlatego w rozdziale tym podjęto próbę identyfikacji istniejącego potencjału i rozwiązań obejmujących ten obszar wiedzy.

Zgromadzenie określonych teleinformatycznych rezerw strategicznych wymaga wcześniejszego zdefiniowania zagrożeń i możliwości jakimi dysponować powinny organizacje i instytucje odpowiedzialne za obronność i bezpieczeństwo.

Mając to na względzie **przez teleinformatyczne rezerwy strategiczne będziemy rozumieć** celowo wydzielone zasoby będące w dyspozycji państwa lub możliwe do pozyskania z innych źródeł do uruchamiana w określonej sytuacji zagrożenia bezpieczeństwa i obronności państwa, bezpieczeństwa i porządku publicznego, zdrowia publicznego oraz występujących sytuacji kryzysowych czy wojennych, w tym także związanych z wypełnieniem zobowiązań międzynarodowych. Jednak zakres, skala, asortyment oraz wielkość ich zastosowania nie będzie stała i jednorodna, każdorazowo zależeć będzie od oceny sytuacji zagrożeń.

W sumie podjęta problematyka jest złożoną materią, zarówno z punktu widzenia merytorycznego, jak również metodycznego. Dotyczy to identyfikowania rezerw (zasobów) strategicznych, jak również praktycznych ich aspektów (tworzenia, uruchamiania, wymiany, utrzymywania, rozlokowania, finansowania itp.). Samo zjawisko wykorzystania potencjału (rozwiązań) teleinformatycznego jest obecnie mało opisane w krajowej literaturze przedmiotu, a istniejące zasoby bibliograficzne, co do opisu istniejącej infrastruktury telekomunikacyjnej w kraju, zarówno te powszechnie dostępne, jak i wśród operatorów telekomunikacyjnych,

maja charakter ogólny. Opracowania szczegółowe, jakimi dysponują operatorzy telekomunikacyjni, stanowią tajemnice organizacji firmy itp., są chronione przez ich właścicieli i nie są udostępniane.

4.3. Sieci komputerowe, systemy, sprzęt i oprogramowanie jako zasoby IT państwa

Temat budowy sieci komputerowych[137] jest jednym z najważniejszych tematów związanych z gospodarką narodową, w tym obronnością i bezpieczeństwem państwa. Powstające nowe technologie napędzają obecny rynek w coraz szybszym tempie. Wiele firm zajmuje się projektowaniem oraz budową sieci komputerowych, których działanie jest kluczowe dla zapewnienia funkcjonowania całej gospodarki narodowej, w tym zapewnienia odpowiedniego poziomu bezpieczeństwa wewnętrznego i zewnętrznego.

W najprostszej postaci siecią komputerową może być połączenie ze sobą dwóch komputerów poprzez kabel sieciowy (kabel krosowany), co w efekcie umożliwia przesyłanie danych pomiędzy jednym a drugim komputerem. Jednak obecnie sieci komputerowe z reguły są bardziej złożone, a komputery połączone ze sobą poprzez routery, huby, przełączniki, serwery itp. Przeznaczeniem sieci komputerowej – ideą, dla której została stworzona i wciąż jest ulepszana i rozwijana – jest przede wszystkim komunikacja i przesyłanie danych. Składniki sieci komputerowych to:

- **host, czyli komputer sieciowy**, dzięki któremu użytkownicy mają do niej dostęp;
- **serwer stale włączonego komputera** o dużej mocy obliczeniowej, wyposażony w pojemną i wydajną pamięć operacyjną i pamięć masową;

[137] **Sieć komputerowa** – zbiór komputerów i innych urządzeń połączonych ze sobą kanałami komunikacyjnymi oraz oprogramowanie wykorzystywane w tej sieci. Sieć komputerowa umożliwia wzajemne przekazywanie informacji oraz udostępnianie zasobów własnych między podłączonymi do niej urządzeniami, tzw. „punktami sieci". Głównym przeznaczeniem sieci komputerowej – ideą dla której została stworzona i wciąż jest ulepszana i rozwijana – to ułatwienie komunikacji pomiędzy ludźmi, będącymi faktycznymi użytkownikami sieci. Sieć umożliwia łatwy i szybki dostęp do publikowanych danych, jak również otwiera techniczną możliwość tworzenia i korzystania ze wspólnych zasobów informacji i zasobów danych. https://pl.wikipedia.org/wiki/Sie%C4%87_komputerowa [dostęp: 10.04.2024].
Sieć komputerowa, zestaw sprzętu i oprogramowania pozwalający przekazywać informacje między komputerami (zwanymi węzłami sieci komputerowej).

- **medium transmisyjne** nośnik informacji, realizujący funkcję kanału komunikacyjnego. Są to kable: miedziane i światłowodowe i/lub fale radiowe;
- **sprzęt sieciowy** – koncentratory, przełączniki, routery, karty sieciowe, modemy, punkty dostępu;
- **oprogramowanie** – programy komputerowe zainstalowane na hostach, serwerach i innych urządzeniach sieciowych.

Topologia sieci komputerowej to model układu powiązań między komputerami znajdującymi się w sieci. Określenie to może odnosić się do konstrukcji logicznej bądź fizycznej sieci. Topologia fizyczna pokazuje realizację sieci komputerowej, stanowi układu przewodów, transmisyjnych, jest połączeniem fizycznym hostów i ustalonym standardem komunikacji, zapewnia bezbłędną transmisję danych i jest ściśle powiązana z topologią logiczną. Natomiast topologia logiczna przedstawia sposób komunikowania się hostów między sobą przy użyciu urządzeń topologii fizycznej. Podział sieci komputerowych ze względu na układ powiązań (topologię) to:

- **topologia liniowa** – wszystkie elementy (oprócz granicznych) są połączone z sąsiadującymi;
- **topologia magistrali** – wszystkie elementy sieci podłączone do jednej magistrali;
- **topologia pierścienia** – bardzo podobna do liniowej, z tą różnicą, że nie ma elementów granicznych, bo wszystkie połączone są w tzw. pierścień;
- **topologia podwójnego pierścienia** – niczym zwykła topologia pierścienia, z tą różnicą, iż tworzy 2 pierścienie;
- **topologia gwiazdy** – komputery są podłączone do jednego punktu centralnego, koncentratora (koncentrator tworzy fizyczną topologię gwiazdy, ale logiczną magistralę) lub przełącznika;
- **topologia gwiazdy rozszerzonej** – posiada punkt centralny (podobnie do topologii gwiazdy) i punkty poboczne (jedna z częstszych topologii fizycznych Ethernetu);
- **topologia hierarchiczna** – zwana także topologią drzewa, jest kombinacją topologii gwiazdy i magistrali;
- **topologia siatki** – oprócz koniecznych połączeń sieć zawiera połączenia nadmiarowe; rozwiązanie często stosowane w sieciach, w których jest wymagana wysoka bezawaryjność.

Podstawowe rodzaje sieci komputerowych ze względy na zasięg to:

- **LAN (*Local Area Network*) – sieć lokalna**, o najmniejszym zasięgu, zazwyczaj ograniczona do jednego lub kilku pobliskich budynków czy też jednej instytucji. W sieciach tych są stosowane dwie technologie – rozwiązania oparte na kablach miedzianych i światłowodowych (techniki xDSL, FITL) oraz na łączach radiowych (sieci Wi-Fi, Bluetooth). W sieciach lokalnych przewodowych najczęściej używaną technologią jest Ethernet/IEEE 802.3 oraz w mniejszym stopniu Tonek-Ring/IEEE 802.5 i FDDI (*Fiber Distrubuted Data Interface*);
- **MAN (*Metropolian Area Network*) – sieć miejska**, obejmująca swoim zasięgiem miasto, aglomerację miejską. Tego typu sieci używają najczęściej połączeń światłowodowych do komunikacji pomiędzy wchodzącymi w jej skład rozrzuconymi sieciami LAN. W Polsce sieci miejskie są budowane przede wszystkim przez duże organizacje rządowe, edukacyjne lub prywatne, które potrzebują szybkiej i pewnej wymiany danych. Do technologii używanych przy budowaniu takich sieci należą: ATM, FDDI, SMDS oraz ostatnio Gigabit Ethernet. Tam, gdzie niemożliwe jest użycie połączeń światłowodowych, często stosuje się bezprzewodowe połączenia radiowe, laserowe lub podczerwone;
- **WAN (*Wide Area Network*) – sieć rozległa**, sieć o dużym zasięgu, przekraczającym obszar jednego miasta, np. sieć łącząca rozsiane po kraju lub świecie oddziały przedsiębiorstwa. Protokoły stosowane w sieciach rozległych to m.in. X.25, Frame Relay, Point to Point Protocol, ATM;
- **GAN (*Global Area Network*)/ Internet** – sieć o zasięgu globalnym; Internet nazywany jest również siecią sieci.

Do zarządzania zasobami znajdującymi się w sieci służy serwer – komputer, na którym znajduje się systemowe oprogramowanie sieciowe oraz zasoby (pliki, aplikacje, drukarki itp.). Wykonuje on określone zadania dla użytkowników sieci oraz czuwa nad prawidłowym korzystaniem z jego zasobów. Pojęcie serwer dotyczy maszyny, która w sposób kontrolowany przez administratora umożliwia korzystanie z jej zasobów.

Internet jest to globalny system wspólnie połączonych sieci komputerowych, który używa standardowego protokołu internetowego TCP/IP by obsłużyć miliardy użytkowników na całym świecie. Nazywany siecią sieci (*network of networks*), która składa się z milionów: prywatnych, publicznych, akademickich, biznesowych, rządowych sieci, od lokalnego do globalnego zasięgu, które połączone są ze sobą poprzez szeroką gamę elektronicznych, bezprzewodowych oraz

optycznych technologii sieciowych. Internet niesie ze sobą szeroką gamę zasobów informacyjnych i usług.

Media sieciowe, inaczej media transmisyjne, są to nośniki służące do transmisji sygnałów w telekomunikacji. Jest to podstawowy element systemów telekomunikacyjnych. Możliwości transmisji zależą od wybranych mediów transmisyjnych. Wyróżnia się media **bezprzewodowe** oraz **przewodowe**. Bezprzewodowe technologie wykorzystujące media bezprzewodowe:

- WLAN (WIRELESS LAN);
- DSSS (ang. DIRECT SEQUENCE SPOREAD SPECTRUM);
- FHSS (ang. FREQUENCY HOPPING SPREAD SPECTRUM);
- BLUETOOTH.

Do przewodowych technologii wykorzystujących media przewodowe zaliczymy:

- ETHERNET;
- FDDI (ang. FIBER DISTRIBUTED DATA INTERFACE);
- PLC (ang. POWER LINE COMMUNICATION);
- TOKEN RING.

Do przewodowych mediów transmisyjnych należą:

- kabel symetryczny (w tym tzw. skrętka);
- kabel współosiowy (kabel koncentryczny);
- kabel światłowodowy (światłowód – jednomodowy, wielomodowy);
- kable energetyczne.

Do bezprzewodowych mediów transmisyjnych należą:
fale elektromagnetyczne (fale radiowe);
promień lasera.

Media transmisyjne możemy podzielić również ze względu na rodzaj transmisji:

- simpleks – transmisja tylko w jednym kierunku;
- półdupleks – transmisja w obu kierunkach, ale nierównoczesna;
- dupleks – równoczesna transmisja w obu kierunkach.

Urządzenia działające w sieci możemy podzielić na: aktywne oraz pasywne. Urządzenia aktywne potrzebują do działania zasilania i można je konfigurować. Przetwarzają otrzymywane dane, a następnie po przetworzeniu przesyłają je

dalej. Urządzenia pasywne do działania nie potrzebują zasilania oraz nie są w stanie przetwarzać informacji[138].

Na polskim rynku działa kilku kluczowych producentów sprzętu telekomunikacyjnego, który jest eksploatowany w ramach sieci Telekomunikacji Polskiej. Tymi kluczowymi dostawcami są: Alcatel Telecom, Ericsson, Lucent Technologies18, Samsung, Siemens, DGT – jedyny polski dostawca.

Systemy telekomunikacyjne w Polsce charakteryzują się dużą różnorodnością sprzętu pochodzącego od różnych dostawców. Równolegle z dostawą specjalistycznego sprzętu komutacyjnego, transmisyjnego lub końcowego dostawcy sprzęty oferują mniej lub bardziej skomplikowane systemy i podsystemy zarządzania i utrzymania sieci telekomunikacyjnych.

W obecnych czasach jesteśmy uzależnieni od komputerów, które zewsząd nas otaczają i stanowią nieodłączną część naszego każdego dnia w domu, w pracy, w szkole czy podczas zabawy lub nauki. Jak wiadomo komputer to nie tylko monitor i jednostka centralna, klawiatura, mysz, ale to także oprogramowanie, które umożliwia nam pracę z tym całym sprzętem. Oprogramowanie, dzięki któremu jest możliwe wykonywanie rozmaitych czynności, to przede wszystkim system operacyjny. System komputerowy zawiera zasadniczo trzy rodzaje oprogramowania:

- **oprogramowanie systemowe** (podstawowe, bez którego komputer nie będzie wykonywał żadnych operacji na plikach ani działań matematycznych) – kontroluje i koordynuje użycie zasobów sprzętowych poprzez różne programy użytkowe dla różnych użytkowników; jest programem, który działa jako pośrednik między użytkownikiem komputera a sprzętem komputerowym. Zadaniem oprogramowania systemowego jest tworzenie środowiska, w którym użytkownik może wykonywać programy w wygodny i wydajny sposób;
- **oprogramowanie narzędziowe** (usprawnia konfigurację lub naprawia system) – wspomaga zarządzanie zasobami sprzętowymi poprzez dogodne interfejsy użytkowe oraz usprawnia, modyfikuje oprogramowanie systemowe w celu usprawnienia wykonywania programów w bardziej wygodny i wydajny sposób, a przy tym pozbawiony błędów;
- **oprogramowanie użytkowe** (zwane też aplikacyjnym, aplikacjami) – określa sposoby, w jaki zostają użyte zasoby systemowe do rozwiązywania

[138] http://www.sieci.u2.pl/ [dostęp: 14.02.2020].

problemów obliczeniowych zadanych przez użytkownika (kompiler, systemy baz danych, gry, oprogramowanie biurowe); zazwyczaj program, który ma bezpośredni kontakt z użytkownikiem i nie jest częścią większego programu, a z technicznego punktu widzenia jest to oprogramowanie korzystające z usług oprogramowania systemowego[139].

Ogólnie oprogramowanie możemy podzielić także na:

- **oprogramowanie systemowe** – to systemy operacyjne takie jak:
  - ✓ PC/M, DOS, BeOS;
  - ✓ Linux:
    - – Linux Debian, Red Hat Linux, Mandrake Linux, Slackware Linux, PLD Linux, SuSe Linux;
- Windows:
  - – Windows 95/98, 2000, ME, XP, Vista, 7/8/10/11;
  - ✓ MacOS;
  - ✓ Free BSD;
  - ✓ AmigaOS;
  - ✓ Solaris;
  - ✓ OS/2 Warp;
  - ✓ Novell;
- **oprogramowanie użytkowe** – to pojedyncze aplikacje lub pakiety programów takich jak:
  - ✓ edytory tekstu, arkusze kalkulacyjne, edytory graficzne, bazy danych;
  - ✓ **języki programowania;**
  - ✓ programy komunikacyjne;
  - ✓ programy edukacyjne;
  - ✓ programy antywirusowe;
  - ✓ programy narzędziowe.

4.4. Wiedza, specjaliści, firmy jako potencjał infrastruktury krytycznej

W społeczeństwie informacyjnym kluczową rolę odgrywa informacja. **Informacja** (łac. *informatio* – przedstawienie, wizerunek; *informare* – kształtować, przedstawiać) – termin interdyscyplinarny, definiowany różnie w różnych

[139] https://pl.wikipedia.org/wiki/Oprogramowanie [dostęp: 10.04.2024].

dziedzinach nauki; najogólniej – właściwość pewnych obiektów[140], relacja między elementami zbiorów pewnych obiektów, której istotą jest zmniejszanie niepewności (nieokreśloności)[141].

Za **informację** możemy uważać wiedzę przekazywaną przez ludzi. Może być także zdobywana samodzielne przez studiowanie, naukę, poszukiwanie w zasobach bibliotecznych. Zdobywanie, posiadanie i wykorzystywanie informacji następuje zarówno w sposób świadomy, jak i podświadomie. Do podstawowych pojęć w obszarze systemu informacji można zaliczyć: **sygnały, dane, informację, wiedzę i mądrość**[142].

Cechy informacji[143]

- informacja stanowi zasób strategiczny państw i organizacji XXI wieku;
- informacja i wynikająca z niej wiedza oraz technologie informatyczne staną się podstawowym czynnikiem wytwórczym;
- większość dochodu państwa zostanie uzyskana z szeroko rozumianego sektora informacyjnego;
- procesy decyzyjne w innych sektorach gospodarki i życia społecznego uzależnione będą od systemów przetwarzania i przesyłania informacji;
- zakłócenie prawidłowości działania systemów informacyjno-sterujących nie wymaga wysokich nakładów materialnych;
- rywalizacja pomiędzy przeciwnikami przeniesie się na płaszczyznę walki informacyjnej.

W dzisiejszych czasach **informację** i **wiedzę** uważa się za nowy towar na rynku. Informacja może dotyczyć zarówno wiedzy faktycznej, jak i domniemanej, a także reguł, określonych zasad w różnych dziedzinach jej ważności i użyteczności. W tym sensie, informując kogoś o kimś lub czymś, zawiadamiamy go o faktach lub dzielimy się naszą wiedzą albo preferencjami na dany temat[144]. Dotyczy to zarówno osób indywidualnych, organizacji, instytucji, przedsiębiorstw i firm. W ogólnym ujęciu takie podejście możemy postrzegać jako zbiór składników

[140] K. Szaniawski, *Informacja, w: Filozofia a nauka*, wyd. PWE, Warszawa 1987, s. 244.
[141] G. Lissowski, hasło: *Informacja, w: Wielka Encyklopedia Powszechna*, wyd. PWE, Warszawa 2002, s. 126.
[142] M. Wrzosek, *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, AON, Warszawa 2010, s. 24.
[143] T. Jemioła, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe …*, dz. cyt., s. 511.
[144] http://pl.wikipedia.org/wiki/Informacja [dostęp: 10.03.2024].

i procesów. Składniki tego systemu mogą być podsystemami, członkami lub elementami[145] i wpływać także na zapewnienie obronności i bezpieczeństwa.

System możemy definiować również jako zbiór elementów, który odwzorowuje lub kreuje wyodrębniony zbiór obiektów rzeczywistości. Poszczególne elementy są (zwykle) liczbami charakteryzującymi (stanowiącymi odwzorowanie) atrybutów danych (obserwowanych) obiektów rzeczywistości. W zbiorze elementów systemu wyodrębnia się strukturę przez podział na podzbiory elementów: wejścia-wyjścia, stanów, funkcji przejścia, funkcji wyjścia. Zbiór elementów charakteryzujący się pewnymi właściwościami połączonych wzajemnie określonymi relacjami jest modelem systemu i może być przedstawiony metodami matematycznymi, jako zbiór zmiennych i funkcji[146].

W teorii zarządzania **system informacyjny** to zespół środków materialnych, finansowych, algorytmów i ludzi, zapewniający sprawne zarządzanie organizacją, przedsiębiorstwem (firmą). Na gruncie ekonomiki informacji system informacyjny definiowany jest jako kompleks powiązanych ze sobą procesów informacyjnych. Podstawowe zasoby systemu informacyjnego o infrastrukturze teleinformatycznej – telekomunikacyjnej sprowadzają się do klasycznych dwóch grup – zasobów materialnych i osobowych. Systemem informacyjnym jest także specyficzny system społeczno-gospodarczy, który, obok procesów informacyjnych, zawsze współtworzą zasoby oraz informacja.

Z kolei przez **proces informacyjny** rozumiemy proces semiotyczny, ekonomiczny i techniczny, który realizuje co najmniej jedną z następujących funkcji[147]:

- **generowanie** (produkcja) informacji;
- **gromadzenie** (zbieranie) informacji;
- **przechowywanie** (pamiętanie, magazynowanie, archiwowanie) informacji;
- **przekazywanie** (transmisja) informacji;
- **przetwarzanie** (przekształcanie, transformacja, translacja) informacji;
- **udostępnianie** (upowszechnianie) informacji;
- **interpretacja** (translacja na język użytkownika) informacji;
- **wykorzystywanie** (użytkowanie) informacji.

Dla sprawnego funkcjonowania systemu informacyjnego zapewniającego bezpieczeństwo wewnętrzne i zewnętrzne niezbędnym jest posiadanie

[145] P. Cieślar, *Operacje i techniki operacyjne*, AON, Warszawa 2009, s. 26.
[146] http://pldocs.docdat.com/docs/index-117214.html [dostęp: 15.01.2020].
[147] J. Kuck, *Nowoczesność, efektywność i bezpieczeństwo współczesnej logistyki*, AON, Warszawa 2014, s. 31.

w odpowiedniej ilości i jakości specjalistów z dziedzin informatyki i telekomunikacji. Zbudowanie struktur na czas pokoju i zdolność do rozbudowy tego potencjału w przypadku kryzysu czy wojny powinno stanowić priorytet przyszłego działania instytucji państwowych. Za celowe i ważne można określić takie działanie, w którym struktury odpowiedzialne za bezpieczeństwo wewnętrzne i zewnętrzne będą ściśle współpracowały z firmami nowych technologii. Będą też posiadały informacje o możliwościach i potencjale technicznym, programowym i osobowym, który można wykorzystać w przypadku różnych zagrożeń. Minęły już czasy, w których specjalista IT pracował tylko z komputerami. Pracodawcy nie ukrywają, że zależy im na jak najbardziej wszechstronnych pracownikach – specjalistach w wąskim zakresie, ale posiadających jak najszerszą wiedzę z pogranicza biznesu i IT[148].

Krytyczna Infrastruktura Państwa to obiekty i urządzenia, służby odpowiedzialne za obsługę tych obiektów i urządzeń oraz systemy i sieci teleinformatyczne istotne dla bezpieczeństwa i ekonomicznego dobrobytu państwa, jego efektywnego funkcjonowania. Zaliczymy do niej: systemy energetyczne, systemy bankowe, transport, systemy zaopatrzenia w wodę, systemy opieki zdrowotnej, ratownictwo, zarówno publiczne, jak i prywatne. Za krytyczną infrastrukturę teleinformatyczną przyjąć należy systemy i sieci teleinformatyczne niezbędne dla prowadzenia podstawowych działań gospodarczych i funkcjonowania instytucji publicznych państwa. Zarówno infrastruktura otwarta (podłączona do publicznie dostępnych sieci), jak i zamknięta (odseparowana od sieci publicznych) narażona jest na ataki bezpośrednie (m.in. włamania i silne impulsy elektromagnetyczne) i pośrednie, spowodowane na przykład wystąpieniem zakłóceń w zasilaniu, spowodowanych uszkodzeniem systemów energetycznych[149].

Inną definicję infrastruktury krytycznej znajdziemy w Ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym: „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[150]".

[148] https://www.computerworld.pl/news/7-cech-ktore-kazdy-specjalista-IT-posiadac-powinien,348062.html [dostęp: 05.03.2024].

[149] Z. Grzywna, A. Grzywna, *Zarys bezpieczeństwa z uwzględnieniem infrastruktury krytycznej*, wyd. UKiP J&D Gądka, Gliwice 2011, s. 115.

[150] https://www.gov.pl/web/rcb/infrastruktura-krytyczna [dostęp: 05.03.2024].

Regulacja ta ma na celu poprawę stanu bezpieczeństwa powszechnego poprzez zwiększenie efektywności działania organów administracji publicznej w sytuacjach kryzysowych. Obszar bezpieczeństwa powszechnego obejmuje zarówno ochronę życia i zdrowia obywateli, jak również ochronę infrastruktury krytycznej. Zarządzaniem kryzysowym zgodnie z art. 2 omawianej ustawy jest działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz na odtwarzaniu zasobów i infrastruktury krytycznej. Ustawa ta nakłada na organy administracji rządowej obowiązek realizacji zadań z zakresu ochrony infrastruktury krytycznej. Infrastruktura krytyczna w świetle art. 3 ustawy obejmuje systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje następujące systemy: zaopatrzenia w energię i paliwa, łączności i sieci teleinformatycznych, finansowe, zaopatrzenia w żywność i wodę, ochrony zdrowia, transportowe i komunikacyjne, ratownicze oraz zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania, stosowania substancji promieniotwórczych i chemicznych, w tym rurociągi substancji niebezpiecznych. Do zadań organów administracji publicznej związanych z ochroną infrastruktury krytycznej należą między innymi: gromadzenie i przetwarzanie informacji dotyczących zagrożeń infrastruktury krytycznej, opracowywanie i wdrażanie procedur na wypadek wystąpienia zagrożeń infrastruktury krytycznej, odtwarzanie infrastruktury krytycznej oraz współpraca między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej w zakresie jej ochrony. Ustawa nakłada na dyrektora Rządowego Centrum Bezpieczeństwa, będącego państwową jednostką budżetową podległą Prezesowi Rady Ministrów, obowiązek opracowania Narodowego Programu Ochrony Infrastruktury Krytycznej podlegającego aktualizacji co najmniej raz na dwa lata. Program ten ma na celu stworzenie warunków do poprawy bezpieczeństwa infrastruktury krytycznej w zakresie: zapobiegania zakłóceniom funkcjonowania infrastruktury krytycznej, przygotowania na sytuacje kryzysowe mogące niekorzystnie wpłynąć na infrastrukturę krytyczną,

reagowania w sytuacjach zniszczenia lub zakłócenia funkcjonowania infrastruktury krytycznej oraz odtwarzania infrastruktury krytycznej. Omawiany program powinien zawierać wskazanie narodowych priorytetów, celów, wymagań oraz standardów, służących zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej, jak i ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych odpowiedzialnych za systemy zaliczane do infrastruktury krytycznej. Dodatkowo w programie powinny znaleźć się szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, biorąc pod uwagę ich znaczenie dla funkcjonowania państwa i zaspokojenia potrzeb obywateli. Opracowany program powinien zostać przedstawiony Radzie Ministrów, która go przyjmuje w drodze uchwały. Obok obowiązku opracowania programu dyrektor Rządowego Centrum Bezpieczeństwa zobowiązany został do przygotowywania jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy. Niezbędne w tym zakresie informacje powinny być przekazywane organom administracji publicznej przez właściwych wojewodów z zachowaniem przepisów o ochronie informacji niejawnych.

O włączeniu danego obiektu w skład infrastruktury krytycznej informowani są w szczególności jego właściciele oraz posiadacze samoistni i zależni.

Ustawa o zarządzaniu kryzysowym nakłada na właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej obowiązek ich ochrony. W szczególności zobowiązano ich do przygotowywania i wdrażania, stosownie do przewidywanych zagrożeń, planów ochrony infrastruktury krytycznej oraz utrzymywania własnych systemów rezerwowych zapewniających bezpieczeństwo i podtrzymujących funkcjonowanie tej infrastruktury, do czasu jej pełnego odtworzenia. Komunikacja między właścicielami i posiadaczami elementów infrastruktury krytycznej a innymi właściwymi podmiotami powinna odbywać się poprzez dedykowane do tego osoby[151]. W realizację zadań z zakresu ochrony infrastruktury krytycznej zaangażowane, w świetle przepisów ustawy, powinny być także: na szczeblu krajowym – zespoły zarządzania kryzysowego utworzone w ministerstwach i urzędach centralnych odpowiednio przez ministrów kierujących działami administracji rządowej oraz kierowników urzędów centralnych; na szczeblu wojewódzkim – wojewoda, urząd wojewódzki

[151] Z. Grzywna, A. Grzywna, *Zarys bezpieczeństwa z uwzględnieniem infrastruktury krytycznej*, wyd. UKiP J&D Gądka, Gliwice 2011, s. 115.

oraz zespolone służby, inspekcje i straż, a także powoływany przez wojewodę wojewódzki zespół zarządzania kryzysowego; na szczeblu powiatowym – starosta, a na szczeblu gminnym – wójt, burmistrz lub prezydenta miasta. Za koordynację działań w tym zakresie odpowiada Departament Spraw Obronnych w Ministerstwie Infrastruktury, właściwy w sprawach wynikających z ustawy o zarządzaniu kryzysowym. Jednym z kluczowych elementów zapewniających sprawną i całościową ochronę infrastruktury krytycznej jest współpraca sektora publicznego z sektorem prywatnym, jak i współpraca wewnątrz tych sektorów, ze szczególnym uwzględnieniem współpracy przedstawicieli poszczególnych systemów w sektorze prywatnym. Ważnym elementem współpracy jest wypracowanie przejrzystych zasad i procedur między organami i służbami państwa a właścicielami oraz posiadaczami samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej. Wynika to z faktu, iż znaczna część infrastruktury, mającej kluczowe znaczenie dla bezpieczeństwa państwa, znajduje się obecnie w rękach sektora prywatnego[152].

4.5. Współczesne zagrożenia przestępczości komputerowej, cyberterroryzmu, cyberwojny

Mówiąc o zagrożeniu przestępczością i atakami cyberterrorystycznymi należy wskazać, że do istotnych tutaj należy bezpieczeństwo infrastruktury krytycznej państwa definiowane jako „zespół obiektów, urządzeń i instytucji niezbędnych do funkcjonowania gospodarki i państwa. Należy wyraźnie zaznaczyć, iż do infrastruktury mającej znaczenie strategiczne zalicza się także systemy i sieci teleinformatyczne, które w obecnych czasach stały się niezwykle istotne dla bezpieczeństwa i ekonomicznego dobrobytu państwa oraz jego efektywnego funkcjonowania”[153].

Do najczęściej występujących zagrożeń dotyczących systemów informatycznych należy zaliczyć:

- nieuprawniony dostęp do systemu informatycznego;
- nielegalny podsłuch lub inwigilacja przy użyciu środków technicznych;
- naruszenie integralności komputerowego zapisu informacji;

[152] Tamże, s. 131.

[153] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, wyd. Oficyna a Wolters Kluwer business, Warszawa 2010, s. 89.

- sabotaż komputerowy;
- bezprawne wykorzystywanie programów i danych;
- przestępstwa związane z wykorzystaniem komputerów;
- przestępstwa przeciwko wiarygodności dokumentów;
- oszustwo komputerowe.

Ponieważ nie wszystkie organizacje terrorystyczne dysponują możliwościami, środkami finansowymi i umiejętnościami do przeprowadzenia ataku w cyberprzestrzeni, często dochodzi do użycia kombinacji starych i nowych metod działania.

Ataki na systemy informatyczne mogą być połączone z innymi rodzajami ataków terrorystycznych. Mogą być skierowane w ważne systemy, takie jak bankowość, obsługa ruchu lotniczego czy dystrybucja energii elektrycznej itp. Biorąc pod uwagę rosnącą skalę tego zjawiska i coraz poważniejsze jego skutki, niepodjęcie dobrze zaplanowanego, usystematyzowanego procesu jego zwalczania może mieć bardzo poważne konsekwencje. W naszym kraju już dziś istnieje wiele systemów informatycznych. Zakłócenie ich działalności mogłoby odbić się negatywnie na funkcjonowaniu państwa i bezpieczeństwie obywateli (np. systemy bankowo-finansowe, ubezpieczeń społecznych itp.). Jeszcze poważniejsze są potencjalne zagrożenia dla systemów działających w sektorze energetycznym, wodociągowym, gazociągowym czy w służbach ratunkowych[154].

Na przełomie XX i XXI stulecia terroryzm stał się jednym z największych i najszybciej rosnących zagrożeń o charakterze ponadnarodowym. Pogląd ten uzasadnia szereg argumentów.

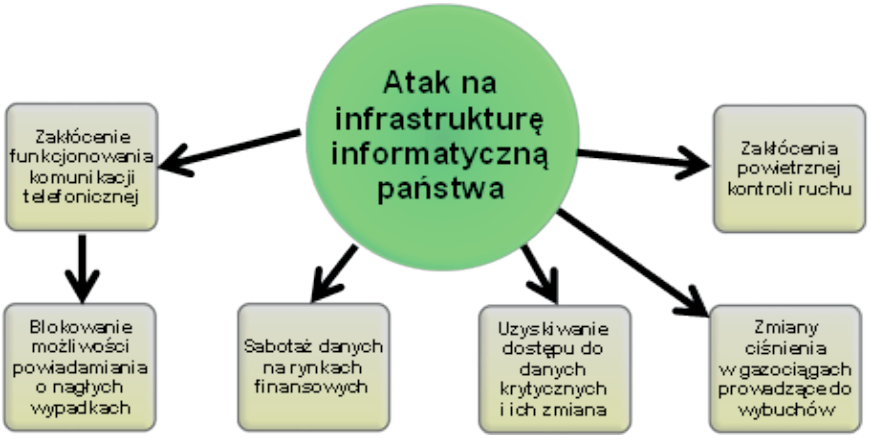
Obecnie liczne organizacje terrorystyczne działają w wielu państwach, na różnych kontynentach, i rekrutują się z obywateli różnych narodowości, wyznających tę samą ideologię. Nowe pokolenie terrorystów znacznie częściej sięga po nowinki techniczne i trafnie identyfikuje punkty newralgiczne, które stopniowo stają się obiektami ataku. Należą do nich z jednej strony obiekty tzw. infrastruktury krytycznej państwa, a z drugiej tzw. cele miękkie. Terroryści, korzystając z ułatwionego dostępu do osiągnięć światowej techniki, coraz szerzej wykorzystują nowoczesne środki walki i łączności. Następuje dążenie terrorystów do prowadzenia działań nowego typu, z wykorzystaniem środków chemicznych, biologicznych, radiologicznych i jądrowych (CBRN) oraz **elementów walki**

[154] Z. Grzywna, *Bezpieczeństwo – Ujęcie kompleksowe*, wyd. UKiP J&D Gądka, Gliwice 2012, s. 111.

informacyjnej. Zwiększa się liczba środowisk skłaniających się ku działalności terrorystycznej. Odnoszone sukcesy w walce z klasycznym terroryzmem mogą sprawić, że terroryści kierować będą swoje zainteresowanie w stronę nowych metod działania, np. cyberterroryzmu. Może on dla terrorystów stać się atrakcyjną formą działania z następujących powodów:

- w porównaniu z klasycznym terroryzmem jest tańszą formą działalności. Do jego przeprowadzenia potrzebny jest jedynie komputer i podłączenie do sieci;
- przedsięwzięcia informatyczne stwarzają możliwość bardziej anonimowej działalności terrorystycznej niż formy tradycyjne. W cyberprzestrzeni nie ma fizycznych barier kontrolnych, granic, staży granicznej, celników, których trzeba przechytrzyć;
- potencjalna liczba celów ataków informatycznych jest znaczna. Terroryści mogą zaatakować komputery, rządowe sieci komputerowe, sieci firm prywatnych czy indywidualnych osób itp.;
- cyberterroryzm cechuje się stacjonarnością, tj. dla wykonania ataku nie ma konieczności podróżowania. Przy przeprowadzaniu ataków w cyberprzestrzeni ryzyko poniesienia śmierci lub obrażeń fizycznych przez terrorystów jest znikome;
- dotychczasowe przykłady przestępstw informatycznych pokazują, jak wielka liczba ludzi może być dotknięta skutkami takiego działania; wynika to z globalnego charakteru informatyzacji[155].

[155] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe" Akademii Marynarki Wojennej 2005, rok XLVI, nr 1 (160), s. 185.



Rys. 7. Skutki przeprowadzenia ataku cyberterrorystycznego na infrastrukturę informatyczną państwa

Źródło: A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, wyd. Oficyna a Wolters Kluwer business, Warszawa 2010.

Najpoważniejszym źródłem zagrożeń dla sieci teleinformatycznych – obok niedoskonałości rozwiązań technicznych – są działania celowe. Mogą przyjmować formę:

- zakłócenia działania systemów;
- nieupoważnionego wprowadzania lub kopiowania danych;
- łamania zabezpieczeń, co pozwala na przejęcie kontroli nad poszczególnymi elementami infrastruktury (np. na wypadek wojny)[156].

Telekomunikacja jest tym sektorem, który wraz z działem energetyki decyduje o działaniu wielu innych sektorów. Dla większości niezwykle ważną kwestią jest dostęp do usług telekomunikacyjnych. Uzależnienie społeczeństwa od prawidłowego funkcjonowania telekomunikacji sprawia, że wielkiego znaczenia nabiera zapewnienie sieciom i usługom telekomunikacyjnym odporności na uszkodzenia, zakłócenia oraz na obecne zagrożenia dla struktury telekomunikacyjnej.

Zdarzające się z różnych przyczyn usterki systemów telekomunikacyjnych oraz informatycznych, a także celowe ataki, mogą w różnym stopniu wpłynąć na

[156] https://ena.lpnu.ua:8443/server/api/core/bitstreams/d4941166-d688-45ba-b999-47074d966d07/content [dostęp: 05.03.2024].

ich bezpieczeństwo. Ataki osób, organizacji, instytucji, w sposób przemyślany lub nie, na sieci telekomunikacyjne można podzielić następująco[157]:

- ataki fizyczne na infrastrukturę telekomunikacyjną;
- ataki elektromagnetyczne na strukturę telekomunikacyjną;
- ataki przy użyciu środków logicznych, skierowane przeciw systemom informacyjnym w systemach sieci telekomunikacyjnych;
- zagrożenia społeczne wobec decydentów w systemach zarządzania i sterowania sieciami telekomunikacyjnymi;
- przeciążenie ruchem sieci telekomunikacyjnej;
- uzależnienie od innych sektorów społeczeństwa.

Walki (zagrożenia) informacyjne mogą być ukierunkowane na kwestionowanie autorytetu określonego państwa na arenie międzynarodowej, czy też negowanie jego zaufania sojuszniczego. W szerokim zakresie może być włączana do tego dyplomacja, handel zagraniczny i media. Na oddziaływanie takie szczególnie jest podatna sfera ekonomiczna, polityczna i społeczna. W działaniach tych mogą być również stosowane incydenty powodujące napięcia społeczne w stosunkach dobrosąsiedzkich. W przypadku państwa czy koalicji liczba elementarnych postaci tajemnic i zapotrzebowań na informacje jest znaczeniowo niezmiernie złożona. Z tego też względu dbałość o bezpieczne warunki egzystencji państwa wiąże się nierozerwalnie z potrzebą ciągłego rozpoznawania otoczenia i bronienia dostępu do własnych tajemnic – co jest wyzwaniem bardzo poważnym, szczególnie w dobie rozwijających się nowych technologii wspierających systemy informacyjne, wśród których poczesne zagrożenie zajmuje cyberterroryzm[158].

4.6. Wykorzystanie potencjału teleinformatycznego organizacji i instytucji odpowiedzialnych za zapewnienie bezpieczeństwa

Głównym celem ochrony informatycznych elementów infrastruktury mającej strategiczne znaczenia dla państwa jest nie tylko zapobieganie potencjalnym atakom, lecz także zredukowanie podatności na ataki, minimalizacja zniszczeń poniesionych na skutek przeprowadzenia ataków oraz skrócenie do minimum

[157] Z. Grzywna, A. Grzywna, *Zarys bezpieczeństwa* ..., dz. cyt., s. 134.
[158] T. Jemioła, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe*..., dz. cyt., s. 513.

czasu niezbędnego do przywrócenia jej pełnej funkcjonalności. Z tego też powodu podejmowane w tym obszarze działania powinny obejmować tworzenie i rozwijanie planów ochrony kluczowych zasobów, zarządzanie kryzysowe w wypadku awarii, wsparcie techniczne dla organizacji dotkniętych atakiem, koordynację w dziedzinie ostrzegania, zabezpieczenia, przeciwdziałania, stosowania nowych rozwiązań zwiększających bezpieczeństwo teleinformatyczne państwa. Ważnym czynnikiem jest zabezpieczenie środków finansowych zarówno na badania naukowe, jak i praktyczne działanie w przypadku identyfikacji zagrożeń w obszarze nowych technologii.

W literaturze można spotkać opisy traktujące na równi z infrastrukturą krytyczną „specyficzne informacje, np. militarne związane z przemysłem zbrojeniowym, nowymi technologiami i rodzajami broni; ekonomiczne dotyczące transakcji, banków, kredytów; czy wreszcie osobiste – takie jak pliki i korespondencja osób prywatnych, dane osobowe, numery identyfikujące”[159].

W Polsce ustawodawca przyjął zasadę uzupełniania istniejących ustaw o kwestie związane z cyberprzestępczością, co sprawiło, że brak jest całościowej systematyki w jednej ustawie. W konsekwencji kompetencje w zakresie walki z cyberprzestępczością zostały dodane jako zadania uzupełniające dla instytucji dbających o bezpieczeństwo narodowe, przestrzeganie prawa i ochronę obywateli (w tym walczących z terroryzmem).

Głównymi instytucjami w Polsce, zaangażowanymi w przeciwdziałanie zagrożeniom terrorystycznym oraz zwalczanie terroryzmu na terenie kraju, są:

- Ministerstwo Administracji i Cyfryzacji;
- Ministerstwo Spraw Wewnętrznych i podległe mu służby: Policja, Straż Graniczna i Biuro Ochrony Rządu;
- Ministerstwo Obrony Narodowej i podległe mu służby: Służba Wywiadu Wojskowego, Służba Kontrwywiadu Wojskowego i Żandarmeria Wojskowa;
- Ministerstwo Spraw Zagranicznych;
- Ministerstwo Finansów (związane z przeciwdziałaniem finansowaniu terroryzmu);
- Agencja Bezpieczeństwa Wewnętrznego – stanowi ona, wraz z kadrowym zapleczem technicznym, Krajowy Punkt Centralny w ramach polityki ochrony cyberprzestrzeni. Podmiotem monitorującym incydenty w sieciach

[159] A. Suchorzewska, *Ochrona prawna systemów...*, dz. cyt., s. 111.

i systemach komputerowych podłączonych do sieci rozległej NATO jest Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputerowe umiejscowione w Wojskowym Biurze Bezpieczeństwa Łączności i Informatyki podlegającym Ministerstwu Obrony Narodowej. Szef ABW i Minister Obrony Narodowej przy współpracy z ministrem właściwym do spraw wewnętrznych są odpowiedzialni za współpracę z NATO Cyber Defence Management Authority – CDMA;

- inne organy administracji rządowej.

Bardzo ważną dla bezpieczeństwa cyberprzestrzeni instytucją jest Agencja Bezpieczeństwa Wewnętrznego. Jej zadania koncentrują się na rozpoznawaniu, zapobieganiu i zwalczaniu zagrożeń, które godzą w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny. Do zadań ABW należy również wykrywanie i zapobieganie terroryzmowi (w tym cyberterroryzmowi) oraz innych czynów godzących w bezpieczeństwo państwa[160]. Do ABW należy rozpoznawanie mechanizmów działania incydentów, które mogą zagrażać infrastrukturze teleinformatycznej państwa, takich jak cyberterroryzm lub podsłuch elektromagnetyczny, a także ich efektywne zwalczanie i przeciwdziałanie powstawaniu podobnych zjawisk.

Computer Emergency Response Team (CERT Polska) – CERT Polska jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet. Jednostka działa od 1996 roku. Do końca roku 2000 funkcjonowała pod nazwą CERT NASK. Od 1997 roku jest członkiem FIRST (Forum of Incidents Response and Security Teams) i w ramach tej organizacji współpracuje z podobnymi zespołami na całym świecie. CERT to instytucja dedykowana wyłącznie do walki z przestępstwami internetowymi i do zwiększenia bezpieczeństwa sieci. Zespół CERT Polska działa w strukturach Naukowej i Akademickiej Sieci Komputerowej, w związku z tym jego działalność jest finansowana przez NASK. NASK jest własnością Skarbu Państwa, przychody uzyskuje głównie ze sprzedaży domen, posiada status jednostki badawczo-rozwojowej. W związku z tym można uznać, iż polska jednostka CERT realizująca zadania zlecone przez ministra w drodze rozporządzenia jest jednostką rządową.

[160] M. Pomykała, *Instytucjonalno-prawne podstawy przeciwdziałania cyberterroryzmowi, w: Cyberterroryzm – nowe wyzwania XXI wieku*, T. Jemioła, J. Kisielnicki, K Rajchel (red.), WSI-ZiA, Warszawa 2009, s. 576.

System Reagowania na Incydenty Komputerowe (SRnIK) – celem systemu jest zapewnienie realizacji i koordynacji procesów zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach i sieciach teleinformatycznych obrony narodowej. Nadzór nad funkcjonowaniem SRnIK sprawuje Dyrektor Departamentu Informatyki i Telekomunikacji. Od lutego 2012 roku Dyrektor Departamentu pełni też rolę Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni. W ramach SRnIK działa zespół MIL–CERT stanowiący Wojskowy Zespół Reagowania na Incydenty Komputerowe SRBN RP.

Do zadań po powstaniu Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL jest zapewnienie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed zagrożeniami płynącymi z cyberprzestrzeni, szczególnie ataków mających na celu zniszczenie lub zakłócenie działania infrastruktury systemów i sieci teleinformatycznych, których uszkodzenie może stanowić zagrożenie dla życia, zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach albo sprawić duże straty materialne, a także zakłócić funkcjonowanie państwa. Do celów CERT.GOV.PL należy:

- kreowanie polityki w zakresie ochrony przed cyberzagrożeniami;
- koordynowanie i przepływ informacji pomiędzy podmiotami w tym zakresie;
- wykrywanie, rozpoznawanie i przeciwdziałanie cyberzagrożeniom;
- współpraca z krajowymi instytucjami, organizacjami oraz podmiotami resortowymi w zakresie ochrony cyberprzestrzeni.

Do zakresu świadczonych przez CERT.GOV.PL usług należy:

- koordynacja reagowania na incydenty;
- publikacja alertów i ostrzeżeń;
- obsługa i analiza incydentów (w tym gromadzenie dowodów realizowane przez zespół biegłych sądowych);
- publikacja powiadomień (biuletynów zabezpieczeń);
- koordynacja reagowania na luki w zabezpieczeniach;
- obsługa zdarzeń w sieciach objętych ochroną przez system ARAKIS-GOV przeprowadzanie testów bezpieczeństwa”[161].

[161] file:///C:/Users/jerzy/Downloads/Raport_CERT_GOV_PL_za_I_kwartal_ 2011.pdf [dostęp: 02.03.2024].

W walkę z incydentami w cyberprzestrzeni jest szczególnie zaangażowana policja. Utworzono w tym celu specjale komórki dedykowane właśnie zagrożeniu w cyberprzestrzeni. Potocznie jednostki nazywane są policją internetową bądź cyberpolicją. Cyberpolicja zwalcza działania osób, które naruszają prawo w cyberprzestrzeni.

Jeśli chodzi o prokuraturę i sądy, to w Polsce nie ma wyspecjalizowanych jednostek prokuratorskich, które są dedykowane przeprowadzaniu postępowań w sprawach przestępstw komputerowych. Niemal wszystkie łamania prawa w cyberprzestrzeni określone kodeksem karnym i ustawach szczególnych są podległe sądom rejonowych. Wyjątkiem jest szpiegostwo komputerowe, które ze względu na dobro i interes oraz bezpieczeństwo kraju podlega sądom okręgowym.

Innymi organami właściw**ymi w sprawach związanych z cyberprzestępczością,** posiadającymi kompetencje w tym obszarze, związanymi z ochroną danych osobowych, informacji niejawnych oraz ochroną rynków telekomunikacyjnych są: Generalny Inspektor Danych Osobowych, Prezes Urzędu Komunikacji Elektronicznej oraz Prezes Urzędu Ochrony Konkurencji i Konsumenta.

W wąskim rozumieniu bezpieczeństwo teleinformatyczne i telekomunikacyjne jest uważane za zbiór zagadnień z dziedziny informatyki, dotyczący oceny i kontroli ryzyka związanego z korzystaniem z komputerów i sieci komputerowych, rozpatrywany z perspektywy poufności, integralności i dostępności danych. Zakładając, iż musimy brać pod uwagę działania z wielu dziedzin, obejmujące zarówno ochronę posiadanych informacji i sposobów ich przekazywania, jak i metody pozyskiwania danych z zewnątrz, złożoność tak opisanego zjawiska najlepiej oddaje tzw. wojna informacyjna. Może ona przybierać zarówno ofensywny, jak i defensywny charakter. W literaturze przedmiotu podaje się, że **wojna informacyjna** to operacje informacyjne prowadzone podczas kryzysu lub konfliktu w celu osiągnięcia lub poparcia konkretnych celów w odniesieniu do konkretnych przeciwników lub przeciwnika. Natomiast operacje informacyjne to działania podjęte w celu wywarcia wpływu na informacje i systemy informacyjne przeciwnika przy jednoczesnej obronie własnych informacji i systemów informacyjnych. Na tak określoną „wojnę" składają się ofensywne i defensywne działania, skierowane przeciw zasobom informacyjnym. Są to działania o charakterze „sukces-porażka". Wojnę prowadzi się dlatego, że te zasoby mają dla ludzi wartość. Działania ofensywne mają na celu zwiększenie wartości dla strony atakującej i zmniejszenie jej dla strony atakowanej. Operacje defensywne zaś prowadzi się po to, by zapobiec potencjalnej utracie tej wartości. Głównym przejawem działań

o charakterze obronnym jest budowanie bezpiecznych systemów ochrony i przekazywania informacji.

Prawdziwie bezpieczny system jest definiowany jako mechanizm wyidealizowany, praktycznie niemożliwy do osiągnięcia, który poprawnie i w całości realizuje tylko i wyłącznie cele zgodne z intencjami osoby nim się posługującej. Zapewnienie bezpieczeństwa sprowadza się w praktyce do zarządzania ryzykiem. Wskazywane są potencjalne zagrożenia, szacowane jest prawdopodobieństwo ich wystąpienia, oceniany potencjał strat, następnie są podejmowane kroki zapobiegawcze w racjonalnym zakresie, biorąc pod uwagę możliwości techniczne i względy ekonomiczne. Zagadnienia bezpieczeństwa teleinformatycznego i telekomunikacyjnego są szczególnie istotne dla tych sektorów polityki bezpieczeństwa państwa, w których istnieje konieczność wykorzystywania przewagi informacyjnej i ochrony treści, do których dostęp powinien być ograniczony. Dotyczy to przede wszystkim obronności i bezpieczeństwa wewnętrznego i zewnętrznego.

Zgodnie z decyzją Ministra Obrony Narodowej za bezpieczeństwo teleinformatyczne uznaje się całokształt przedsięwzięć zmierzających do zapewnienia bezpieczeństwa systemów i sieci teleinformatycznych. Polega na ochronie informacji wytwarzanej, przetwarzanej, przechowywanej lub przekazywanej w systemach i sieciach przed przypadkowym lub celowym ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania poprzez zastosowanie w sposób kompleksowy technicznych, programowych, kryptograficznych oraz organizacyjnych środków i metod. W sektorze bezpieczeństwa militarnego zadania z zakresu ochrony systemów i sieci teleinformatycznych realizują:

- Centrum Bezpieczeństwa Teleinformacyjnego;
- Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki;
- organy bezpieczeństwa systemów łączności i informatyki jednostek organizacyjnych wszystkich szczebli dowodzenia;
- Centrum Zarządzania Systemami Teleinformatycznymi;
- Służba Kontrwywiadu Wojskowego;
- w jednostce (komórce) organizacyjnej:
  - ✓ kierownik jednostki (komórki) organizacyjnej;
  - ✓ pełnomocnik ochrony;
  - ✓ administrator systemu;
  - ✓ inspektor bezpieczeństwa teleinformatycznego.

Niezwykle ważna jest ochrona teleinformatyczna systemów łączności w trakcie pełnienia misji zagranicznych przez polskie kontyngenty wojskowe,

szczególnie na obszarach bezpośrednich działań bojowych. W tym wypadku jej skuteczność może decydować wprost o życiu czy zdrowiu żołnierzy i dlatego coraz większy nacisk kładzie się na odpowiednie przygotowanie i zabezpieczenie pod tym względem operacji z udziałem polskich sił.

Za zagwarantowanie bezpieczeństwa telekomunikacyjnego i teleinformatycznego w działaniach związanych z zapewnieniem bezpieczeństwa wewnętrznego na poziomie państwa jest odpowiedzialna Agencja Bezpieczeństwa Wewnętrznego. Do ustawowych zadań Agencji Bezpieczeństwa Wewnętrznego należy, między innymi, zapewnienie bezpieczeństwa systemów i sieci teleinformatycznych, w których są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne. Zadania ABW w tym zakresie realizuje wyspecjalizowany zespół Departamentu Bezpieczeństwa Teleinformatycznego – Jednostka Certyfikująca przeprowadza certyfikacje systemów i sieci teleinformatycznych oraz środków (wyrobów) w zakresie: ochrony kryptograficznej, ochrony elektromagnetycznej, ochrony akustycznej.

Certyfikacja środków ochrony bezpieczeństwa teleinformatycznego jest prowadzona według polskich i europejskich norm oraz kryteriów oceny. Każdy system lub sieć teleinformatyczna przeznaczona do przetwarzania informacji niejawnych musi uzyskać certyfikat akredytacji bezpieczeństwa teleinformatycznego. Uzależnione jest to od zastosowania certyfikowanych środków ochrony oraz przedstawienia przez użytkownika, zatwierdzonych przez służbę ochrony państwa, szczególnych wymagań bezpieczeństwa systemu lub sieci TI i Procedur bezpiecznej eksploatacji.

Łatwo dostrzec, że zasoby informacyjne i elementy infrastruktury teleinformatycznej Polski podlegają tym samym trendom, co cyberprzestrzeń na poziomie globalnym. Wraz z postępującą informatyzacją państwa, konieczne jest tworzenie skutecznych rozwiązań profilaktycznych, technicznych i organizacyjno-prawnych oraz strategicznych rezerw (zasobów) teleinformatycznych.

4.7. Polska w systemie bezpieczeństwa teleinformatycznego UE i NATO

Cyberbezpieczeństwo to „osiąganie wymaganego poziomu ochrony informacji przetwarzanych w systemach i sieciach teleinformatycznych poprzez

zapewnienie poufności, integralności oraz dostępności”[162]. Cyberterroryzm jest zjawiskiem ponadnarodowym. Obrona przed cyberatakami powinna również być wielonarodowa. Należy „ulepszyć” współpracę międzynarodową:

- wytwarzać, harmonizować i koordynować szeroko adaptowane rozwiązania prawne, pozwalające nie tylko na identyfikowanie i ściganie przestępstw, ale także umożliwiające przeprowadzanie szybkiej, wspólnej reakcji w razie zaistniałego ataku[163];
- opracowywać wspólną terminologię, która umożliwi szybką i sprawną wymianę informacji potrzebną do identyfikacji powstałych zagrożeń i ich zwalczania;
- propagować wiedzę o możliwościach technicznych państw/organizacji partnerskich zaangażowanych w zwalczanie incydentów;
- tworzyć międzynarodowe, wielopodmiotowe porozumienia mające na celu wspólną walkę z cyberprzestępczością;
- budować otwarte międzynarodowe struktury organizacyjne porozumień skierowanych na zwiększenie cyberbezpieczeństwa – dawać podmiotom zaangażowanym szansę na zgłaszanie niepokojących sytuacji i wypowiadanie ich niepokojów;
- spisywać i przestrzegać standardów uniemożliwiających „sytuację, w których pojedyncze podmioty poprzez dostęp do grupowych danych i osiągnięć swoich sojuszników będą działały na szkodę innych”[164]. Są kraje, które utworzyły specjalne ośrodki zajmujące się ochroną systemów krytycznych, a wśród nich: Anglia, Australia, Norwegia, Nowa Zelandia, Stany Zjednoczone. Ich działalność oparta jest na ścisłej, międzynarodowej współpracy.

Cyberprzestępczość i cyberterroryzm są ze sobą ściśle powiązane. Na arenie międzynarodowej nie ma regulacji odnośnie cyberterroryzmu. Są jednak odpowiednie dokumenty pozwalające na skuteczną walkę z cyberprzestępczością, co również zapobiega przerodzeniu się przestępstwa w cyberprzestrzeni w akt terroru.

Przykładem mogą być: „Strategia Komisji Europejskiej nt. Zwalczania cyberprzestępczości” z listopada 2008 roku oraz polski „Rządowy program

[162] file:///C:/Users/jerzy/Downloads/Raport_CERT_GOV_PL_za_I_kwartal_ 2011.pdf [dostęp: 02.03.2024].
[163] A. Suchorzewska, *Ochrona prawna systemów…*, dz. cyt., s. 208.
[164] J. Świątkowska, I. Bunsch, *Cyberterroryzm – nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI...*, dz. cyt., s. 12.

ochrony cyberprzestrzeni na lata 2011-2016" z 2010 roku. W tych dokumentach są zapisy, które mówią o wymogu zorganizowania współpracy organów ścigania z sektorem prywatnym oraz w wymiarze międzynarodowym, co ma na celu skuteczne zwalczanie przestępczości w cyberprzestrzeni.

Natomiast „Konwencja Rady Europy o cyberprzestępczości" zawiera szereg zapisów, które:

- **nakazują:** traktowanie jako przestępstwo umyślnego dostępu do całości lub części systemu informatycznego bez uprawnienia, personalizacje umyślnego i nieuprawnionego przechwytywania transmisji danych;
- **zakazują:** umyślnego i nieuprawnionego uszkadzania, usuwania, niszczenia, zmiany lub blokowania danych informatycznych; uzyskiwania używania, rozpowszechniania, sprzedaży, wytwarzania, sprowadzania lub udostępniania wszelkich środków (w tym programów komputerowych) stworzonych lub przystosowanych do popełniania przestępstw komputerowych;
- **uznają za przestępstwo:** spowodowanie zakłócenia w działaniu systemu informatycznego na skutek wprowadzenia, przesyłania, uszkodzenia, usunięcia, zniszczenia lub zablokowania danych informatycznych bez uprawnienia.

Konwencja ta, oprócz wprowadzenia nakazu ścigania przestępstw przeciwko poufności, integralności i dostępności danych i systemów komputerowych, zobowiązuje państwa członkowskie do wdrożenia środków ustawodawczych i innych, niezbędnych do uznania w prawie krajowym za przestępstwo.

Na poziomie Unii Europejskiej zostały wdrożone inne akty prawne, które odnoszą się do cyberprzestępczości. Niektóre odnoszą się do konkretnego aspektu cyberprzestępczości. Przykładowo decyzja ramowa w sprawie ataków na systemy informatyczne, która nakazuje personalizację zabronionych czynów, m.in. umyślnego, bezprawnego dostępu do całości lub części systemu informatycznego lub naruszenia i przerwania funkcjonowania takiego systemu.

W 2004 roku została utworzona Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA), co spowodowało postęp w uświadomieniu państwom członkowskim i ich obywatelom wyzwania, jakim jest zapewnienie bezpieczeństwa systemów informatycznych, aby było możliwe wdrożenie i opracowanie wspólnych praktyk w zakresie zabezpieczeń tych systemów[165].

[165] J. Kosiński, S. Kmiotek, *Międzynarodowa współpraca w zwalczaniu cyberprzestępczości, w: Cyberterroryzm – nowe wyzwania XXI wieku*, T. Jemioła, J. Kisielnicki, K. Rajchel (red.),

W komunikacie Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 2007 roku o tytule „W kierunku ogólnej strategii zwalczania cyberprzestępczości" jako cyberprzestępstwa zostały wymienione:

- nieuprawniony dostęp do systemów poprzez haching, podsłuch, inżynierię społeczną, wirusy, ataki DoS i DDoS, spam;
- przestępstwa tradycyjne powiązane z komputerami, np. oszustwa, podrabianie towaru, molestowanie dzieci, a także działania terrorystyczne, jak ataki na ludzkie życie przez manipulowanie systemami bezpieczeństwa lub kontrolą ruchu powietrznego;
- przestępstwa „contentowe" dotyczące zawartości. Mowa tu o pornografii dziecięcej, dostarczaniu instrukcji przestępczych, oferty popełniania przestępstw itp.;
- przestępstwa powiązane z naruszeniem praw autorskich i praw pokrewnych[166].

Prezydencja francuska w lipcu 2008 roku przedstawiła „globalny plan w sprawie zwalczania cyberprzestępczości". Ciekawe w tym planie jest to, że ta strategia zaleca podjęcie konkretnych środków operacyjnych, takich jak: cyberpatrole, wspólne zespoły dochodzeniowo-śledcze i wprowadzenie osobnych jednostek badawczych.

Współpraca międzynarodowa w walce z cyberprzestępczością jest kojarzona z dwoma płaszczyznami nieoperacyjnymi – edukacją i szkoleniami oraz współpracą z sektorem prywatnym. W tej pierwszej płaszczyźnie działania te wspierane są głównie przez Interpol i Europol.

Działania Europolu, w ramach projektu AGIS, poskutkowały opracowaniem siedmiu kursów w zakresie bezpieczeństwa informacyjnego na rożnych poziomach, które są wykorzystywane w University College of Dublin do prowadzenia studiów magisterskich dla policjantów. Wśród współpracujących jest kilka uniwersytetów oraz policje niemal ze wszystkich krajów europejskich.

Koncentrując się na cyberterroryzmie trzeba wymienić powstałą w 2008 roku organizację non profit The Internenational Partnership Against Cyber Threats (IMPACT) z siedzibą w Malezji[167]. IMPACT analizuje poważne zagrożenia

WSIZiA, Warszawa 2009, s. 144.

166 Tamże.

167 https://www.bing.com/search?q=The+Internenational+Partnership+Against+Cyber+Threats+%28IMPACT%29+z+siedzib%C4%85+w+Malezji&qs=ds&form=QBRE [dostęp: 20.02.2023].

związane z cyberprzestrzenią, infrastrukturą krytyczną. Dotyczy to czterech obszarów:

- Global Response Center – całodobowe obserwacje stanu cyberprzestrzeni na świecie, publikacja wiadomości na stronie oraz posiadanie zamkniętej sieci dla specjalistów;
- szkolenia – możliwość przeprowadzania szkoleń i koordynacja ich oraz dostarczanie miejsc do tych szkoleń, rozpowszechnianie najlepszych praktyk na poziomie ministrów;
- badania – dostarczanie ekspertyz oraz współpraca z ponad 20 centrami doskonalenia oraz uczelniami;
- centrum współpracy międzynarodowej.

11 stycznia 2013 roku działalność rozpoczęło Europejskie Centrum ds. Walki z Cyberprzestępczością, którego zadaniem jest ochrona obywateli i europejskich przedsiębiorst przed przestępstwami w Internecie. Centrum powstało przy siedzibie Europolu w Hadze. Jest to bardzo ważne wydarzenie, gdyż policja krajowa nie jest w stanie przeprowadzać operacji o tak dużej skali. Spowodowane jest to tym, że dochodzenia w sprawie oszustw internetowych, przemocy wobec dzieci w Internecie i innych cyberprzestępstw dotyczą zazwyczaj setek ofiar, a także podejrzanych w wielu różnych częściach świata. Otwarcie tego centrum oznacza zmianę podejścia Unii Europejskiej do problemu cyberprzestępczości. Teraz działanie będzie w większej mierze opierać się na przewidywaniu i będzie posiadać bardziej wszechstronny charakter. Co bardzo ważne, Centrum będzie gromadzić wiedzę i informację, wspierając wszelkie dochodzenia w sprawach karnych oraz promować takie same rozwiązania we wszystkich państwach Unii Europejskiej.

Centrum skupia się głównie na nielegalnych działaniach grup przestępczych w Internecie, a szczególnie na atakach wymierzonych w bankowość elektroniczną i wszelkie transakcje przeprowadzane w sieci. Duża uwaga będzie również przykładana do przemocy seksualnej wobec dzieci oraz systemów, które dotyczą infrastruktury krytycznej i systemów informatycznych w UE.

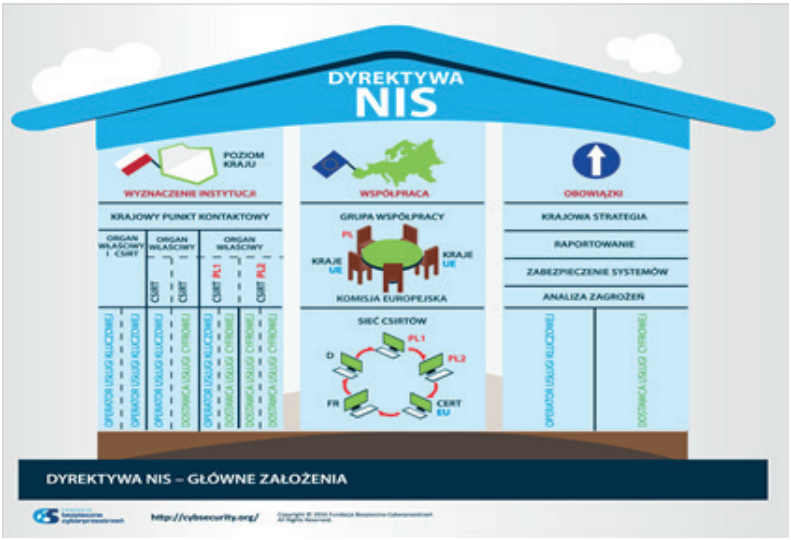
Centrum będzie też wspierać badania, rozwój i działania polepszające pracę organów ścigania i sądownictwa. Będzie ono również przygotowywać oceny zagrożenia, analizę tendencji, prognozę i wczesne ostrzeganie. W tym miejscu będą również gromadzone i przetwarzane dane dotyczące cyberprzestępczości

i zapewniana będzie pomoc techniczna dla organów ściągania państw członkowskich, aby poprawić skuteczność ich działania[168].

Należy zauważyć, że aktywność Polski w międzynarodowej współpracy nie jest duża w zakresie dostarczania wiedzy i doświadczeń i wykorzystywania tej wiedzy. W Polsce jest jednak wielu uzdolnionych ludzi, którzy dbają o bezpieczeństwo informatyczne. Warto zaznaczyć, że zwiększane są kompetencje jednostek i różnych grup w tym zakresie na różnych płaszczyznach państwowych. Zespół CERT cały czas zyskuje większe możliwości, a Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011-2016 wprowadza wiele usprawnień w walce z przestępstwami w cyberprzestrzeni. **CERT– Polska** bierze udział w licznych międzynarodowych inicjatywach: **FISHA**, **NISHA**, **ARAKIS**, **HONEYSPIDER NETWORK**, **WOMBAT, SOPAS**, **N6**.

Pracę nad ujednoliceniem poziomu cyberbezpieczeństwa w Europie rozpoczęli unijni urzędnicy w 2013 r. Trzy lata zajęło Komisji Europejskiej i państwom członkowskim ustalenie sposobu ochrony teleinformatycznej. Końcowym efektem tych prac było przyjęcie tzw. **Dyrektywy NIS, czyli Dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej**. Dyrektywa wiąże każde państwo członkowskie w odniesieniu do rezultatu, jaki powinien zostać osiągnięty w obszarze cyberbezpieczeństwa. Kraje członkowskie mają przy tym swobodę wyboru formy i środków realizacji wynegocjowanych zapisów. Przepisy te w istotny sposób zwiększają poziom bezpieczeństwa państw członkowskich, chociaż nie rozwiązują wszystkich problemów związanych z cyberbezpieczeństwem.

[168] http://europa.eu/rapid/press-release_IP-13-13_pl.htm [dostęp: 24.02.2024].



Rys. 8. Dyrektywa NIS

Źródło: https://www.cybsecurity.org/wp-content/uploads/2016/08/DyrektywaNISodc3.png [dostęp: 12.04.2024].

Zakres Dyrektywy NIS, ogranicza się do dwóch typów podmiotów:

- pierwszy dotyczy tzw. **operatorów usług kluczowych** (przedsiębiorców z sektorów energetyki, transportu, bankowości i infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę pitną, infrastruktury cyfrowej);
- drugi obejmuje **dostawców usług cyfrowych** (internetowych platform handlowych, wyszukiwarek internetowych, usług przetwarzania w chmurze).

W Dyrektywie nie umieszczono bezpośrednio nic o bezpieczeństwie obywateli Unii Europejskiej, jednak samo skierowanie zapisów dyrektywy do dostawców usług cyfrowych stanowi właściwe działanie. Niestety, w ostatecznej wersji Dyrektywy NIS z jej zakresu wykreślono serwisy społecznościowe. Również niezagospodarowanym obszarem pozostaje administracja publiczna[169].

W przypadku operatorów usług kluczowych dyrektywa przewiduje skomplikowany sześciostopniowy sposób identyfikacji (który oczywiście musi być szczegółowo doprecyzowany przez każde państwo członkowskie). Ustalono, że dostawcy usług cyfrowych mają być identyfikowani „z poziomu" Unii

[169] https://www.cybsecurity.org/wp-content/uploads/2016/08/DyrektywaNISodc3. png [dostęp: 15.07.2022].

Europejskiej. Należy zastanowić się, czy państwa członkowskie uważają, że nie będą potrafiły ich wyznaczyć i czy na pewno pozostawienie tego w gestii Komisji Europejskiej doprowadzi do skutecznej identyfikacji tych dostawców i zapewni bezpieczeństwo każdego z państw. Jest to z pewnością jedno z kluczowych wyzwań przy wdrażaniu zapisów dyrektywy. Dla rozwiązania tego zagadnienia Komisja Europejska prawdopodobnie zakłada wynajęcie zewnętrznej firmy konsultingowej, która przeprowadzi ankiety wśród instytucji wiodących państw członkowskich[170].

Wybór operatów usług kluczowych zależy tylko od państwa członkowskiego i będzie dokonany albo razem z implementacją Dyrektywy NIS, albo bezpośrednio po niej. Każdy kraj musi stworzyć listę usług kluczowych dla każdego sektora wymienionego w dyrektywie. Występuje również brak ustaleń, które podmioty będą objęte regulacjami i jakie będą powiązania z istniejącym wykazem infrastruktury krytycznej RP, a to z punktu widzenia spójności dokumentów mówiących o ochronie najważniejszych obiektów jest niezwykle istotne. **Wybrane podmioty będą miały głównie dwa obowiązki**.

- **Pierwszy** nakazuje wprowadzenie środków ochrony (technicznych i organizacyjnych) zależnych od poziomu ryzyka, które być może będzie wyznaczane również przez urzędników.
- **Drugi** to konieczność raportowania incydentów, jednak na razie nie wiadomo komu – czy tzw. organowi właściwemu, czy też właściwemu Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego (Computer Security Inciden Team, CSIRT).

Dyrektywa dotyczy tylko trzech rodzajów dostawców usług cyfrowych: platform handlowych, wyszukiwarek internetowych i usług przetwarzania danych w chmurze. Ponieważ są to operatorzy międzynarodowi zadecydowano, że będą wyznaczeni przez Unię Europejską i, podobnie jak w przypadku operatorów usług kluczowych, będą musieli zapewnić poziom bezpieczeństwa zależnie od zidentyfikowanego ryzyka.

Państwo członkowskie, na którego terytorium nie znajduje się siedziba dostawcy, nie będzie więc bezpośrednio otrzymywało żadnych informacji na temat incydentów dotyczących operatorów usług cyfrowych. Raportowanie nastąpi tylko wtedy, jeśli znana będzie: „liczba użytkowników, których dotyczył incydent, w szczególności: użytkowników zależnych od usługi na potrzeby

[170] Tamże.

świadczenia ich własnych usług, czas trwania incydentu, geograficzny, którego dotyczył incydent, zasięg zakłócenia funkcjonowania usługi, zasięg wpływu na działalność gospodarczą i społeczną[171]". Jeśli dostawca nie ma dostępu do tych informacji, Dyrektywa NIS zwalnia go z obowiązku raportowania.

Dyrektywa NIS określa, że państwo członkowskie musi wyznaczyć tzw. organy właściwe, których zadaniem będzie nadzór nad operatorami usług kluczowych i dostawcami usług cyfrowych. Organy te powinny mieć również możliwość uzyskania od operatorów i dostawców informacji o bezpieczeństwie oraz powinny przeprowadzać audyty bezpieczeństwa. Dyrektywa wskazuje, że takich organów może być wiele. Mowa jest o spektrum od dostawców energii elektrycznej przez instytucje finansowe aż po dostawców usług DNS. **Wyznaczone mają być także Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego**, które zakresem swojego działania objęłyby wszystkich wyznaczonych operatorów usług kluczowych i dostawców usług cyfrowych. Powołanie takich zespołów powinno być obowiązkowe i stanowić jeden z podstawowych punktów implementacji Dyrektywy NIS. Państwo członkowskie będzie zmuszone wyznaczyć także krajowy pojedynczy punkt kontaktowy, którego zadaniem będzie uczestniczenie w Grupie Współpracy i przekazywanie informacji za granicę na życzenie polskich organów właściwych i krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego.

Na poziomie europejskim utworzona zostanie Sieć Zespołów Reagowania Na Incydenty Bezpieczeństwa Komputerowego. Rolę sekretariatu będzie pełnić ENISA, co oznacza, że rola tej agencji w realizacji zadań operacyjnych najprawdopodobniej wzrośnie. Obok zespołów CSIRT wybranych przez władze krajów członkowskich do „sieci CSIRT" należeć będzie także CERT-EU.

Strategiczną rolę Dyrektywa NIS przypisuje kolejnemu międzynarodowemu zespołowi, który nazywany będzie **Grupą Współpracy**. Jej zadania w skrócie można sprowadzić do haseł: współpraca, dyskusja, wymiana dobrych praktyk, zbieranie cyklicznych raportów. Oprócz Komisji Europejskiej i przedstawicieli państw uczestniczyć w niej będzie też Zespół reagowania na sytuacje kryzysowe dla instytucji, organów i agencji (CERT-EU) oraz Agencja Unii Europejskiej dla Cyberbezpieczeństwa (ENISA) jako obserwator.

[171] https://www.cybsecurity.org/pl/9-faktow-o-dyrektywie-nis-ktore-powinienes-znac/ [dostęp: 10.04.2024].

Zespół reagowania na sytuacje kryzysowe dla instytucji, organów i agencji UE (CERT-EU) składa się z ekspertów w dziedzinie bezpieczeństwa informatycznego z głównych instytucji UE. CERT-UE współpracuje z innymi CERT w państwach członkowskich oraz ze specjalistycznymi firmami zajmującymi się bezpieczeństwem informatycznymi w celu reagowania na incydenty związane z bezpieczeństwem informacji i zagrożeniami cybernetycznymi.

Europejska Agencja Bezpieczeństwa Sieci i Informacji (**ENISA**, ang. *European Union Network and Information Security Agency*) – agencja Unii Europejskiej odpowiedzialna za zapewnienie wysokiego i efektywnego poziomu bezpieczeństwa w sieciach i systemach informatycznych w Unii Europejskiej. **Dyrektywa zobowiązuje państwa członkowskie do przyjęcia strategii bezpieczeństwa sieci i systemów teleinformatycznych**.

Jak do tej pory w Polsce funkcjonują:

- ✓ Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022;
- ✓ Ustawa o krajowym systemie cyberbezpieczeństwa;
- ✓ Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024;
- ✓ Narodowe standardy cyberbezpieczeństwa
- ✓ Standardy cyberbezpieczeństwa chmur obliczeniowych.

Z punktu widzenia ochrony najważniejszych w Rzeczpospolitej Polskiej obiektów funkcjonuje już kilka aktów prawnych. Jest ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej wyznaczająca obiekty szczególnie ważne dla bezpieczeństwa RP („czas wojny") i ustawa o ochronie osób i mienia.

Między innymi dlatego w ramach utworzonego systemu ochrony infrastruktury krytycznej (ustawa o zarządzaniu kryzysowym, Narodowy Program Ochrony Infrastruktury Krytycznej) jednym z sześciu bezpośrednio wskazywanych obszarów bezpieczeństwa jest właśnie ochrona teleinformatyczna.

Inaczej też obiekty infrastruktury krytycznej są wyznaczane – funkcjonują obiektywne, szczegółowe kryteria sektorowe (dla każdego z 11 sektorów infrastruktury krytycznej) i przekrojowe (wspólne dla wszystkich sektorów).

Nie sposób nie odnieść wrażenia, że w zdecydowanej większości przypadków obiekt infrastruktury krytycznej, wykorzystujący systemy teleinformatyczne i funkcjonujący w jednym z sektorów wymienianych przez Dyrektywę NIS, powinien być tożsamy z operatorem usługi kluczowej. Zatem z punktu widzenia spójności różnych wymagań niezwykle ważne jest, by kryteria wyznaczania

operatorów usług kluczowych miały jasne odniesienie do kryteriów identyfikacji infrastruktury krytycznej lub po prostu były wspólne.

Osobnym zbiorem obiektów istotnych dla bezpieczeństwa europejskiego jest tzw. europejska infrastruktura krytyczna, czyli taka, której zaprzestanie funkcjonowania może mieć wpływ na co najmniej dwa państwa członkowskie.

Dyrektywa zobowiązuje wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu krajowych zdolności w dziedzinie bezpieczeństwa teleinformatycznego. Jej przepisy umożliwiają stworzenie zarówno scentralizowanego systemu na poziomie krajowym, jak i podzielenie kompetencji między różne podmioty.

Dyrektywa NIS nie dotyczy bezpośrednio usług administracji publicznej, o ile nie są to usługi kluczowe wymienione w dyrektywie. Dokument stanowi jednak harmonizację minimalną, a zatem wyznacza pewne minimalne warunki, które należy spełniać. Nie ogranicza przy tym możliwości państw członkowskich do regulowania problematyki cyberbezpieczeństwa administracji publicznej.

Każde państwo członkowskie zostało zobligowane do ustanowienia **organów właściwych ds. bezpieczeństwa sieci i informacji** (*National Competent Authorities*). Funkcję tę mogą pełnić instytucje już istniejące. Zadaniem organu właściwego jest monitorowanie wdrożenia przepisów dyrektywy na poziomie krajowym we wszystkich sektorach objętych regulacją. Państwa mogą wyznaczyć jeden lub kilka organów. Jest to istotne zwłaszcza, jeśli istnieją regulatorzy sektorowi, mogący odpowiadać za wdrożenie dyrektywy we właściwych sobie sektorach.

Organy właściwe ds. bezpieczeństwa sieci i informacji będą miały uprawnienia do:

- badania przypadków niewypełniania przez operatorów usług kluczowych zobowiązań z zakresu bezpieczeństwa sieci i informacji;
- oceny wyników audytów bezpieczeństwa teleinformatycznego;
- wydawania wytycznych w zakresie bezpieczeństwa teleinformatycznego;
- wprowadzenia sankcji za nieprzestrzeganie przepisów.

Ponadto każde państwo członkowskie musi ustanowić **Pojedynczy Punkt Kontaktowy** (PPK, *Single Point of Contact*). Jego zadaniem jest wzmacnianie współpracy między państwami członkowskimi. Będzie również gromadził informacje o incydentach w skali kraju, a także wymieniał się informacjami o znaczących, międzynarodowych incydentach ze swoimi odpowiednikami z zagranicy.

Rola PPK może być także przypisana do już istniejącej instytucji. Kiedy państwo powoła tylko jeden organ właściwy, będzie on jednocześnie pełnił rolę PPK.

- Ostatnią instytucją w dyrektywie jest **CSIRT**, czyli **Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego**. Kraje członkowskie mogą wyznaczyć jeden CSIRT narodowy dla całego kraju, bądź zbudować sieć CSIRT-ów sektorowych, obejmujących sektory rynkowe. Państwa ze słabiej rozwiniętymi zdolnościami cyberbezpieczeństwa mogły zwrócić się o pomoc w rozwoju CSIRT do Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA).

Dyrektywa NIS wprowadza mechanizmy współpracy na dwóch poziomach:

- **technicznym** – ma być zapewniona poprzez europejską sieć **CISRT** (*CSIRT network*) oraz stworzenie mechanizmów wymiany informacji o incydentach transgranicznych pomiędzy CSIRT-ami wyznaczonymi dla operatorów usług kluczowych oraz dostawcami usług cyfrowych;
- **polityczno-strategicznym** – ma być realizowana poprzez utworzenie **Grupy Współpracy** (*Cooperation Group*), która zajmie się wypracowaniem wspólnych koncepcji strategicznych oraz będzie przyjmowała m.in. roczne raporty od właściwych organów.

Dyrektywa nie ustaliła dokładnych mechanizmów działania obu forów. Zarówno Sieć CSIRT, jak i Grupa Współpracy mają określić je same.

Zobowiązania w zakresie bezpieczeństwa sieci i informacji są różne w zależności od aneksu. **Operatorzy usług kluczowych** (aneks II) są zobowiązani do oceny ryzyka cyberzagrożeń oraz do przyjęcia odpowiednich środków zapewniających bezpieczeństwo sieci i informacji.

Dostawcy usług cyfrowych (aneks III) są objęci regulacją *light touch approach*. Polega ona na kontroli *ex post*, tzn. po zaistnieniu incydentu i tylko przez państwo, na terenie którego dostawca usługi ma swoją siedzibę.

Dyrektywa nakłada także na państwa członkowskie obowiązek przyjęcia **narodowej strategii bezpieczeństwa sieci i informacji**, w której określone zostaną m.in. narodowe cele i priorytety cyberbezpieczeństwa, role i obowiązki organów administracji publicznej, zasady współpracy sektora publicznego i prywatnego, krajowa analiza ryzyka oraz zadania w zakresie edukacji.

Dyrektywa NIS daje organom publicznym konkretne narzędzia do przeciwdziała i reakcji na incydenty w cyberprzestrzeni. Są to m.in. obowiązkowe raportowanie, przygotowanie krajowej strategii NIS, skoordynowanie przepływu informacji czy też zinstytucjonalizowanie współpracy CSIRT-ów.

Muszą też zgłaszać właściwym organom wszelkie incydenty poważnie zagrażające ich sieciom i systemom informatycznym. Obowiązkowemu raportowaniu podlegają incydenty o „znaczącym wpływie na ciągłość działania operatorów", co oznacza, że progi raportowania określą państwa członkowskie w procesie implementacji przepisów dyrektywy.

Operatorzy usług kluczowych (aneks II) to podmioty sektora prywatnego lub publicznego, dostarczające kluczowe usługi (*essential services*). Są to usługi zależne od sieci teleinformatycznych, w przypadku których potencjalne incydenty bezpieczeństwa teleinformatycznego mogą mieć istotny wpływ na możliwość świadczenia tych usług. **Regulacje obejmują następujące sektory:**

- energetyczny (m.in. energia elektryczna, ropa naftowa, gaz);
- transportowy (lotniczy, kolejowy, morski);
- bankowy (m.in. instytucje kredytowe);
- finansowy (m.in. giełda);
- zdrowia (m.in. podmioty świadczące opiekę zdrowotną, w tym szpitale);
- zaopatrzenia w wodę;
- infrastruktury cyfrowej (m.in. punkty wymiany ruchu internetowego, dostawcy usług systemu nazw domen oraz rejestry nazw domen najwyższego poziomu).

Proces identyfikacji operatorów przebiega w etapach:

- sprawdzenie, czy operatorzy prowadzą działalność wymienioną w aneksie II (lista sektorów i podsektorów);
- sprawdzenie, czy operatorzy ci zostali objęci *lex specialis*;
- decyzja, czy operator dostarcza usługi kluczowe (*essential services*). W tym celu każde państwo powinno najpierw stworzyć listę kluczowych dla siebie usług;
- określenie, czy dostarczanie usługi zaklasyfikowanej jako kluczowa, jest uzależnione od systemów IT;
- uwzględnienie konkretnych kryteriów:
  - ✓ **najpierw transsektorowe**: liczba użytkowników zależnych od usługi; zależność innych sektorów od usługi; wpływ, jaki incydent może mieć na gospodarkę, działania społeczne oraz bezpieczeństwo publiczne; zasięg geograficzny; jak istotny jest dany operator dla zapewnienia właściwego poziomu świadczenia usługi w skali kraju;
  - ✓ **później sektorowe**: każde państwo określa je samodzielnie, ponieważ dyrektywa podaje tylko przykłady, takie jak ilość produkowanej energii

lub udział tej produkcji w skali kraju (sektor energetyczny) czy liczba pacjentów obsługiwanych w ciągu roku przez dany podmiot (sektor zdrowia).

Organizacja Narodów Zjednoczonych posiada wyspecjalizowaną agencję zajmującą się problemem cyberbezpieczeństwa – International Telecommunications Union (ITU). Należą do niej państwa (w tym Polska), jak i podmioty gospodarcze (z Polski – Polkomtel S.A., NASK oraz Telekomunikacja Polska S.A.). W 2007 roku agencja ogłosiła plan działań – Global Cybersecurity Agenda, który zapoczątkował współpracę międzynarodową tak, aby zwiększyć poziom bezpieczeństwa w środowisku informatycznym, działać na rzecz standaryzowania i wprowadzania skutecznych rozwiązań dla cyberbezpieczeństwa[172]. Raport Biura ONZ do spraw Narkotyków i Przestępczości, powstały przy współpracy z Grupą Zadaniową do spraw Zwalczania Terroryzmu, zatytułowany „Internet jako narzędzie zamierzeń terrorystycznych", określa wykorzystanie Internetu przez terrorystów jako nieoczekiwanie rosnące w siłę zjawisko. Z raportu można się dowiedzieć, że pionierem w rozwiązaniach legislacyjnych mających na celu kontrolę globalnej sieci przed wykorzystaniem jej jako narzędzie terroryzmu jest Wielka Brytania. Twórcy raportu wśród możliwości Internetu wymieniają użycie go do:

- agitacji na rzecz przemocy, ekstremistycznego charakteru wypowiedzi, prowadzenia rekrutacji, podburzania nastrojów społecznych i preferowana poglądów radykalistycznych;
- finansowania terroryzmu;
- szkolenia;
- komunikacji prowadzonej utajnioną drogową internetową;
- przeprowadzania ataków.

Z drugiej strony globalna sieć ułatwia służbom gromadzenie informacji dotyczących podejrzanych o działalność terrorystyczną oraz monitorowanie podejmowanych przez nich działań. Służby muszą przeprowadzać wyżej opisane działania z poszanowaniem powszechnie obowiązujących praw człowieka.

[172] T. Małysa, *Cyberterroryzm i bezpieczeństwo informatycznej infrastruktury krytycznej cz. III, Zapobieganie i przeciwdziałanie zagrożeniom bezpieczeństwa informatycznej infrastruktury krytycznej, w: Infrastruktura krytyczna*, e– terroryzm.pl, Internetowy biuletyn Centrum Studiów nad Terroryzmem i kwartalnika e-Studia nad Bezpieczeństwem i Terroryzmem, http://e- terroryzm.pl/archiwum/, nr 8/2012, s. 38 [dostęp: 14.12.2022].

Polska jest członkiem **Sojuszu Północnoatlantyckiego (NATO)** i z tej racji uczestniczy w polityce ochrony przed atakami w cyberprzestrzeni. Wspomniana polityka ochrony oparta jest na trzech celach głównych swojej działalności, a mianowicie:

- **koordynacji i doradztwie w zakresie cyberobrony** – tym zadaniem zajmuje się jednostka NATO – Cyber Defence Management Authority. W skład tej jednostki wchodzą przedstawiciele elit politycznych, wojskowych i technologicznych z państw sojuszniczych;
- **wspieraniu poszczególnych członków Sojuszu** – NATO może wysyłać Rapid Reinforcement Teams (RRTs), jeżeli państwo – sojusznik wymaga pomocy. Trzeba w tym miejscu podkreślić, iż kraje wchodzące w skład NATO są samodzielnie, indywidualnie odpowiedzialne za sferę własnych systemów komunikacyjnych. Obecnie budują prototypowe cyberarmie mające na celu obronę kraju w czasie cyberwojny;
- **badaniach i szkoleniu** – w 2008 roku w ramach NATO utworzono Cooperative Cyber Defence Centre of Excellence (CCDCOE) w Tallinie. W jego skład wchodzą specjaliści z Estonii, Niemiec, Włoch, Łotwy, Litwy, Słowacji i Hiszpanii.

Międzynarodowe Wzajemne Partnerstwo Przeciwko Cyberterroryzmowi (IMPACT) to instytucja non-profit, powołana w 2008 roku, oparta o zasady działania partnerstwa publiczno-prywatnego (PPP). Instytucja ta zrzesza państwa z całego świata. W swej działalności koncentruje się na: szkoleniach, certyfikatach bezpieczeństwa, badaniach i rozwoju. Przy IMPACT działa również Globalne Centrum Odpowiedzi na sytuacje kryzysowe z dziedziny zagrożeń cybernetycznych, mające oferować pomoc rządom, które znajdą się w niebezpieczeństwie. Problematyka zagrożenia terroryzmem relatywnie długo nie należała do głównego nurtu procesu integracji europejskiej. Współpraca między państwami członkowskimi miała głównie wymiar ekonomiczny. W początkowym jej okresie koncentrowała się na aspektach gospodarczych, liberalizacji handlu czy tworzeniu podstaw dla funkcjonowania wspólnego rynku[173].

Europejska Agencja do Spraw Bezpieczeństwa Sieci i Informacji (ENISA) jest to agencjazapewniająca bezpieczeństwo sieci i informacji

[173] F. Jasiński, M. Narojek, P. Rakowski, Wewnętrzne i zewnętrzne aspekty współpracy antyterrorystycznej w Unii Europejskiej w kontekście Polski jako państwa członkowskiego, Centrum Europejskie – Natolin, Warszawa 2006, s. 10.

w Unii Europejskiej, dbająca o kulturę przekazywanych informacji z dziedziny bezpieczeństwa.

Polska jako członek Unii Europejskiej, dążąc do uściślenia współpracy gospodarczej, kulturalnej, turystycznej z innymi krajami członkowskimi Unii Europejskiej, musi jak najszybciej przystąpić do budowy wspólnej przestrzeni informacyjnej. Przestrzeń informacyjna obejmuje między innymi bazy: danych, wiedzy, modeli, obrazów, dźwięku wraz z odpowiednim oprogramowaniem jej i środki techniczne, które umożliwiają użytkownikom korzystanie z tych zasobów w sposób bezpieczny i zgodny z przeznaczeniem.

Dla osiągnięcia tych celów musimy wydatkować odpowiednie kwoty na technologie informacyjne. Wyrazem odpowiedzialnego odnoszenia się do cybernetycznej strony bezpieczeństwa były połączone europejsko-amerykańskie ćwiczenia Cyber Atlantic 2011, zorganizowane przez ENISA (Europejską Agencję Bezpieczeństwa Sieci i Informacji) i DHS (Departament Bezpieczeństwa Wewnętrznego USA). Były to prekursorskie tego typu ćwiczenia z udziałem Unii Europejskiej i USA.

Z kolei budowana przez **Defense Advanced Research Projects Agency (DARPA)** kopia Internetu zawierać ma:

- wirtualną kopię serwerów;
- wirtualną kopię infrastruktury przesyłowej;
- wirtualną kopię stacji roboczych;
- wierne symulacje prawdziwych codziennych ruchów w sieci.

Projekt DARPA pozwoliłby na testowanie rozlicznych wariantów ataków i tym samym doskonalsze przygotowanie się do praktycznych ataków w rzeczywistej sieci.

4.8. Identyfikacja strategicznych rezerw (zasobów) teleinformatycznych jako potencjału cyberbezpieczeństwa

Odpowiednie zabezpieczenie sieci, systemów i informacji w nich zawartych może uchronić organizacje i instytucje odpowiedzialne za obronność i bezpieczeństwo, jak również przedsiębiorców oraz osoby prywatne przed stratami wywołanymi przez przestępców czy terrorystów. Cyberterroryzm może spowodować skutki, które odczuje całe społeczeństwo. Z tego powodu należy prawnie

uregulować zasady zabezpieczania sieci i systemów informatycznych, szczególnie tych, które sterują pracą infrastruktury krytycznej. Także bezpieczeństwo informacji niejawnych i danych osobowych, które są gromadzone, przetwarzane i przesyłane przez systemy i sieci teleinformatyczne, nabiera obecnie istotnego znaczenia. Aktualnie wciąż wiele systemów i sieci nie jest bezpiecznych, a w przedsiębiorstwach i instytucjach nie są one monitorowane czy oceniane. Czy w przyszłości wykorzystają ten fakt cyberterroryści by przeprowadzić atak, wciąż nie wiadomo.

Rozpowszechnienie Internetu i rozwój nowych technologii również wspiera pośrednio terroryzm. Informacje umieszczane w Internecie o miejscach, rodzajach i wrażliwościach krytycznych systemów o strategicznym znaczeniu dla państwa są wystarczające do przeprowadzenia ataku terrorystycznego.

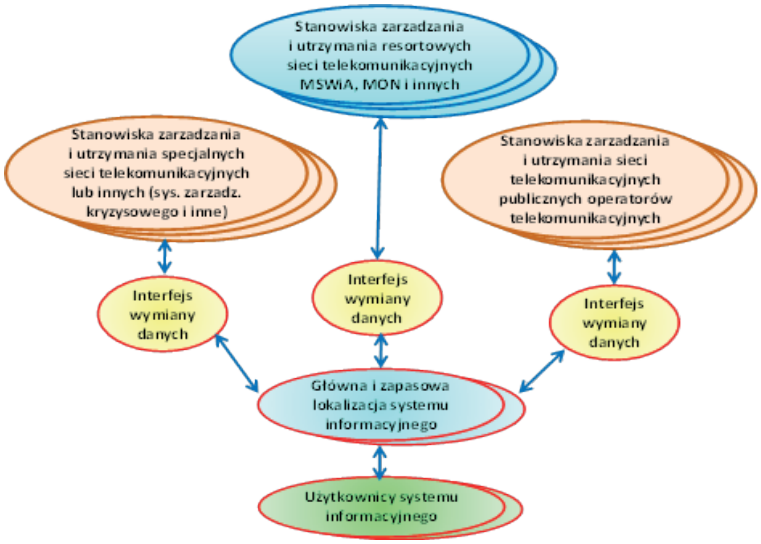
Dla efektywnego przeciwdziałania zjawisku cyberterroryzmu w wymiarze profilaktyki, zwalczania i likwidacji skutków ataków terrorystycznych, niezbędna jest współpraca międzynarodowa i efektywna legislacja w obszarach terroryzmu i przestępczości. Polska, wprowadzając innowacyjne rozwiązania, dostosowując prawo do standardów międzynarodowych, może łatwiej współpracować w ramach Unii Europejskiej i NATO. Skuteczne zapobieganie cyberterroryzmowi wymaga podejmowania różnorodnych działań, w tym posiadania strategicznych rezerw (zasobów) teleinformatycznych. Dlatego konieczne są:

- **uruchomienie programów badawczych** dotyczących bezpieczeństwa teleinformatycznego, które zachęciłyby do wspólnego prowadzenia badań. Podmiotem korygującym w tym zakresie jest Ministerstwo Nauki i Szkolnictwa Wyższego;
- **rozbudowa zespołów reagowania** na incydenty bezpieczeństwa teleinformatycznego w administracji publicznej. Wszystkie te zespoły tworzyłyby krajowy system reagowania na incydenty komputerowe, który odpowiadałyby również za konferencje, szkolenia i ćwiczenia;
- **rozbudowa systemu wczesnego ostrzegania** oraz wdrażanie i utrzymanie rozwiązań prewencyjnych. Departament Bezpieczeństwa Teleinformatycznego ABW wraz z zespołem CERT Polska, działającym w ramach Naukowej i Akademickiej Sieci Komputerowej (NASK), dokonał wdrożenia systemu wczesnego ostrzegania przed zagrożeniami z sieci Internet – ARKIS-GOV;
- **testowanie poziomu zabezpieczeń**. W ramach tego programu dla adresatów są przeprowadzane cykliczne ćwiczenia, które polegają na przeprowadzaniu kontrolowanych ataków symulujących działania cyberterrorystyczne;

- **rozwój zespołów CERT**, które są centrami kompetentnymi, służącymi pomocą merytoryczną (tworzenie właściwych struktur i procedur, rozwiązywanie problemów w jednostkach administracyjnych, przedsiębiorców i innych korzystających z cyberprzestrzeni objętych programem). Ponadto do zadań zespołów należy utrzymywanie strony internetowej, na której znajdują się ważne informacje dla bezpieczeństwa teleinformatycznego, takie jak:
  - ✓ aktualności związane z bezpieczeństwem informatycznym;
  - ✓ informacji o podatnościach i zagrożeniach;
  - ✓ biuletyny bezpieczeństwa;
  - ✓ poradniki i dobre praktyki;
  - ✓ raporty, informacje na temat trendów i statystyk;
  - ✓ forum wymiany informacji i doświadczeń bezpieczeństwa teleinformatycznego.
- **opracowywanie i skoordynowanie planów** ciągłości działania na wypadek zaistnienia sytuacji kryzysowej w obszarze cyberprzestrzeni skutkującej zaprzestaniem realizacji procesu;
- **szkolenia pełnomocników ds. ochrony cyberprzestrzeni**. Szkolenia kończyć się będą certyfikatem, który będzie potwierdzał odbycie szkolenia w zakresie bezpieczeństwa cyberprzestrzeni;
- **racjonalizacja programów kształcenia na uczelniach wyższych.** Bezpieczeństwo cyberprzestrzeni może być zapewnione tylko w przypadku posiadania wysoko wykwalifikowanych kadr w sektorze publicznym i prywatnym;
- **kształcenie kadry urzędniczej** oraz ustanowienie dodatkowych kryteriów obsady stanowisk w administracji publicznej. Konieczna jest edukacja pracowników administracji publicznej, którzy mają dostęp do cyberprzestrzeni RP, w zakresie zagadnień dotyczących bezpieczeństwa sieci;
- **kampania społeczna o charakterze edukacyjno-prewencyjnym**. Wraz z rozwojem Internetu ważne jest, aby szkolić i ostrzegać użytkowników przed zagrożeniami płynącymi z globalnej sieci, aby unikać błędów i zminimalizować zagrożenia cybernetyczne. W ramach kampanii informacje dotyczące bezpieczeństwa są zamieszczane na stronach zespołu CERT.

GOV.PL, Ministerstwa Spraw Wewnętrznych i Ministerstwa Administracji i Cyfryzacji[174].

Budowa systemu informacyjnego o strategicznych rezerwach (zasobach) teleinformatycznych państwa to w obecnych uwarunkowaniach konieczność. Na rysunku 9. przedstawiono schemat blokowy takiego systemu.



Rys. 9 . Schemat blokowy struktury organizacyjnej systemu informacyjnego o strategicznych rezerwach (zasobach) teleinformatycznych państwa (wariant)

Źródło: *Infrastruktura Teleinformatyczna Państwa*, Praca nr: 10300038, Państwowy Instytut Badawczy - Instytut Łączności, Zakład Zastosowań Technik Łączności Elektronicznej (Z–10), Warszawa 2008, s. 115.

Przedmiotowy system informacyjny o strategicznych rezerwach (zasobach) teleinformatycznych powinien zawierać następujące zasadnicze składniki: moduły danych – baza danych; moduł słownikowy; moduł analityczny; moduł dostępu; moduł komunikacyjny; moduł prezentacji; moduł zarzadzania[175].

Moduł danych – baza danych, to zasadniczy element sytemu. Moduł ten realizuje funkcje gromadzenia danych o zasobach teleinformatycznych w kraju oraz

[174] Rządowy program ochrony cyberprzestrzeni Rzeczpospolitej Polskiej na lata 2011-2016.

[175] *Infrastruktura Teleinformatyczna Państwa*, Praca nr: 10300038, Państwowy Instytut Badawczy - Instytut Łączności, Zakład Zastosowań Technik Łączności Elektronicznej (Z–10), Warszawa 2008, s. 115-118.

ich wymianę miedzy modułami za pośrednictwem modułu komunikacji. Do podstawowych funkcji Modułu danych zaliczamy:

- przyjmowanie, przetwarzanie, gromadzenie, aktualizację i dystrybucję danych o teleinformatycznych rezerwach (zasobach) strategicznych w kraju;
- przechowywanie bieżących i historycznych informacji o zmianach danych;
- administrowanie użytkownikami i mechanizmami bezpieczeństwa danych;
- administrowanie procedurami i procesami oraz weryfikacją przepływu informacji (danych);
- zarzadzanie parametrami modułu danych.

Moduł słownikowy – wykorzystywany będzie do ułatwiania i porządkowania pracy z systemem. Do podstawowych funkcji realizowanych przez moduł należy zaliczyć:

- wprowadzanie norm porządkujących prace z systemem;
- definiowanie pojęć używanych przy pracy z poszczególnymi aplikacjami;
- umożliwianie tworzenia przyjaznego w pracy środowiska i łatwego korzystania ze zgromadzonych w systemie informacji.

Moduł analityczny – wykorzystywany będzie do analizy danych pod kątem zjawisk zachodzących w systemie informacyjnym o teleinformatycznych rezerwach (zasobach) strategicznych w kraju, a w szczególności do:

- generowania raportów analitycznych o teleinformatycznych rezerwach (zasobach) strategicznych;
- generowania raportów wydajnościowych dla poszczególnych elementów systemu informacyjnego.

Moduł dostępu – związany jest z dostępem do gromadzonych rezerw (zasobów) strategicznych o infrastrukturze teleinformatycznej w kraju.

Moduł komunikacyjny (w zasadniczej części telekomunikacyjny) – umożliwiać będzie bezpieczne przesyłanie danych o teleinformatycznych rezerwach (zasobach) strategicznych w kraju. Moduł ten realizował będzie następujące funkcje:

- przesyłanie danych z centrów zarzadzania lub utrzymania sieci operatorów telekomunikacyjnych publicznych, prywatnych i specjalnych do bazy danych;
- przesyłanie danych z bazy danych do uprawnionych podmiotów – osób i organizacji w kraju;

- realizacja usług telekomunikacyjnych (w tym dostępu do Internetu) na potrzeby przedmiotowego systemu informacyjnego oraz jego zasobów osobowych.

Moduł prezentacji – umożliwiać będzie prezentacje gromadzonych danych w bazie danych.
Moduł zarzadzania – realizował będzie zadania związane z zarzadzaniem systemami informacyjnymi o teleinformatycznych rezerwach (zasobach) strategicznych w kraju. Dotyczyć to będzie działalności związanej z planowaniem, organizowaniem, sterowaniem, kontrolowaniem teleinformatycznych rezerw (zasobów) strategicznych i jego sieci – systemu telekomunikacyjnego oraz pracy personelu obsługującego. Obejmie optymalne wykorzystanie zasobów systemu i sieci, czyli świadczenie usług możliwie najwyższej jakości, ponosząc przy tym możliwie najniższe koszty. Moduł ten realizował będzie następujące zasadnicze funkcje:

- zarzadzanie modułami systemu informacyjnego;
- zarzadzanie systemem telekomunikacyjnym systemu informacyjnego zgodnie ze standardem ISO 7498-4 (*Management Framework for OSI*), w tym głównie zarzadzanie uszkodzeniami, konfiguracja, rozliczeniami, wydajności bezpieczeństwem;
- zarzadzanie systemem telekomunikacyjnym systemu informacyjnego zgodnie z warstwowym modelem zarzadzania telekomunikacja, w tym głównie zarzadzanie elementami sieci i siecią oraz usługami w skali strategicznej, taktycznej i operacyjnej.

W obecnych czasach potencjał teleinformatyczny powinien być traktowany jako strategiczne rezerwy (zasoby) teleinformatyczne, a tym samym identyfikowany, specjalnie chroniony i planowany do wykorzystania szczególnie w przypadku kryzysu czy wojny.

Głównym celem organizacji systemu informacyjnego o teleinformatycznych rezerwach (zasobach) strategicznych państwa jest:

- budowa krajowego systemu informacyjnego o teleinformatycznych rezerwach (zasobach) strategicznych państwa, umożliwiającego instytucjom i organizacjom odpowiedzialnym za obronność, bezpieczeństwo skuteczne kierowanie państwem na wszystkich szczeblach jego organizacji, od szczebla najniższego po krajowy włącznie;

- dostarczenie instytucjom i organizacjom pełnej i wiarygodnej informacji umożliwiającej realizacje ich zadań statutowych w przedmiotowym zakresie;
- skuteczne monitorowanie zagrożeń teleinformatycznych w państwie;
- współdziałanie organizacji i instytucji w państwie, a w razie zaistniałych nieprzewidzianych i niepożądanych zdarzeń skutecznie im przeciwdziałanie oraz ich likwidacja;
- stworzenie i zbudowanie zautomatyzowanego systemu informacyjnego o strategicznych rezerwach (zasobach) teleinformatycznych państwa, bezpiecznego i niezawodnego w jego funkcjonowaniu.

Realizacja głównych celów organizacji systemu informacyjnego o strategicznych rezerwach (zasobach) teleinformatycznych państwa wymaga realizacji następujących działań:

- gromadzenie rzeczywistych danych o rezerwach strategicznych (zasobach) teleinformatycznych państwa, a dotyczących szeroko rozumianych publicznych systemów łączności elektronicznej, systemów specjalnych i innych, jakie funkcjonują w obszarze naszego państwa;
- przetwarzanie gromadzonych informacji, ich przechowywanie, uaktualnianie oraz prezentowanie przy zastosowaniu map cyfrowych oraz nowoczesnych i dostępnych narzędzi GIS;
- udostępnianie gromadzonych informacji w systemie uprawnionym użytkownikom stosownie do ich kompetencji i realizowanych zadań w zakresie obronności i bezpieczeństwa.

Architekturę tworzą odpowiednio połączone i współpracujące ze sobą trzy zasadnicze elementy. Do tych elementów należy zaliczyć:

- elementy głównego i zapasowego stanowiska (lokalizacji) systemu informacyjnego o zasobach teleinformatycznych w kraju;
- elementy zarządzania, utrzymania sieci publicznych, resortowych, specjalnych i innych operatorów telekomunikacyjnych;
- stanowiska zarzadzania instytucji (organizacji) uprawnionych do przedmiotowego systemu informacyjnego, a odpowiadających za obronność i bezpieczeństwo w kraju – użytkownicy systemu.

„Bezpieczeństwo cybernetyczne stanowi niezwykle ważną gałąź bezpieczeństwa narodowego, a zarazem jedno z ważniejszych wyzwań XXI wieku”[176]. Cyberprzestrzeń Rzeczypospolitej Polskiej obejmuje systemy, sieci i usługi teleinformatyczne istotne dla obronności i bezpieczeństwa (wewnętrznego i zewnętrznego). Są one użytkowane zasadniczo przez instytucje państwowe i samorządowe, system bankowy, w tym także systemy zapewniające funkcjonowanie w kraju transportu, łączności, infrastruktury energetycznej, wodociągowej i gazowej oraz systemy informatyczne, ochrony zdrowia, których zniszczenie lub uszkodzenie może stanowić niebagatelne zagrożenie dla życia lub zdrowia ludzi, dziedzictwa narodowego oraz środowiska albo spowodować poważne straty materialne.

W pełni udało się potwierdzić założenie (hipotezę), że planowanie, gromadzenie i racjonalne, skuteczne zastosowanie strategicznych rezerw (zasobów) teleinformatycznych umożliwia efektywne wykorzystanie ich w wielu dziedzinach. Centralnie zgromadzone informacje (bazy wiedzy) pozwalają sprawnie i bezpiecznie funkcjonować systemom teleinformatycznym. Rezerwy (zasoby) strategiczne mogą zabezpieczyć funkcjonowanie państwa w różnych sytuacjach zagrożeń. Takie działania obecnie podejmuje wiele państw. Także Polska stoi przed takim wezwaniem. Państwowy Instytut Badawczy – Instytut Łączności, Zakład Zastosowań Technik Łączności Elektronicznej – rozpoczął w 2008 roku przytoczone w tym opracowaniu prace badawcze. Jednak w dalszym ciągu odpowiedzialność za bezpieczeństwo i ochronę cyberprzestrzeni Polski jest „rozmyta”. **Nie ma instytucji obejmującej całościowo działania na tym polu**. Niezbędne jest skoordynowanie działań, które umożliwią sprawne i przynoszące efekty reagowanie na ataki na systemy teleinformatyczne i oferowane przez nie usługi.

Opracowanie i wdrożenie w Polsce **systemu informacyjnego o teleinformatycznych rezerwach (zasobach) strategicznych powinien pozwolić rozpocząć proces integracji potencjału sprzętowego, programowego i osobowego do skutecznej walki ze współczesnymi zagrożeniami cybernetycznymi**.

[176] J. Świątkowska, I. Bunsch, *Cyberterroryzm – nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI*, dz. cyt., s. 1.

5. BIOMETRIA W SŁUŻBIE BEZPIECZEŃSTWA INFORMACJI

5.1. Podstawy biometrii

Nowe technologie informacyjne, w tym Internet, mają swoją pozytywną i ciemną stronę. Wirusy, szpiegostwo komputerowe, hakerzy, elektroniczne podsłuchy oraz kradzieże stwarzają przed osobami funkcyjnymi nowe zadania związane z potrzebą zapewnienia bezpieczeństwa informacji. Dla większości organizacji, instytucji, przedsiębiorstw czy firm kwestia ochrony dostępu do przechowywanych danych funkcjonujących z wykorzystaniem systemów i sieci komputerowych jest trudnym, ważnym i odpowiedzialnych zadaniem. Zachowania poufności, integralności i rozliczalności wiadomości oraz skuteczne odpieranie ataków sieciowych staje się obecnie ważnym wyzwaniem. Bezpieczeństwo sieci i systemów informatycznych ma także duże znaczenie dla nas, „zwykłych" użytkowników Internetu, często przetrzymujących na dyskach ważne dokumenty oraz dokonujących za pomocą sieci różnych transakcji finansowych. Powstawanie nowoczesnych rozwiązań, które dają obecnie szerokie możliwości zapewniające bezpieczeństwo sieci i systemów informatycznych, związane jest z biometrią i kryptografią. Należy zatem być świadomym tego, jak je skutecznie zastosować i wykorzystywać w praktyce.

Biometria to nauka zajmująca się badaniem zmienności populacji organizmów. Słowo „biometria" pochodzi od greckiego słowa **„bios" – żywy, życie, procesy życiowe** oraz **„metron" – mierzyć**. Wyniki pomiarów biometrycznych, po opracowaniu metodami statystyki matematycznej, wykorzystywane są w wielu obszarach, między innymi w antropologii, fizjologii, genetyce, hodowli, medycynie, paleontologii, telekomunikacji. **Biometria to jedna z najbardziej**

perspektywicznych technologii informatycznych, polegająca na dokonywania pomiarów istot żywych w celu potwierdzenia tożsamości. W najnowszych zastosowaniach ukierunkowana jest na metody automatycznego rozpoznawania ludzi na podstawie ich cech fizycznych. Rozwiązania oparte na biometrii bardzo szybko zyskują popularność, a na rynku usług biometrycznych rośnie zapotrzebowanie na wykwalifikowanych pracowników.

Najbardziej interesującą i najdłuższą historię ze wszystkich rodzajów biometrii ma identyfikacja osób na podstawie odcisków linii papilarnych palców. Archeolodzy odkryli, że w celu identyfikacji osób już starożytni Babilończycy i Chińczycy wykorzystywali tę metodę. W XIV w. w Persji odkryto, że nie ma dwóch identycznych odcisków palców. Pierwsze naukowe badania na temat odcisków palców pochodzą z późnych lat XVII w., jednakże podstawy współczesnych metod identyfikacji opartych o odciski palców zostały opracowane pod koniec XIX w.

Technologia biometryczna w połączeniu z teleinformatyką została zastosowana po raz pierwszy na terenie Japonii, gdzie na dzień dzisiejszy wchodzi w skład standardowej oferty większości banków. Pierwszy bankomat z funkcją weryfikacji danych biometrycznych pojawił się w 2010 r.

Techniki biometryczne są obecnie jednym z najbardziej dynamicznie rozwijających się działów teleinformatyki. W przyszłości należy przewidywać duży wzrost praktycznych zastosowań biometrii. W Polsce rozwój biometrii obserwujemy w szczególności w obszarze bankowości, gdzie biometria wykorzystywana jest w procesach autoryzacji użytkowników w systemach bankowych[177].

Biometria, w szerokim znaczeniu, jest techniką pomiarów istot żywych. **W wąskim,** najczęściej używanym obszarze IT, jest to technologia automatycznego rozpoznawania człowieka w oparciu o analizę jego unikalnych, niepowtarzalnych cech. Dotyczy to zarówno cech fizycznych, takich jak: układ linii papilarnych, wygląd twarzy i tęczówki, jak też cech jego zachowania, związanych ze sposobem podpisywania się czy mówienia. Lista unikalnych cech każdego człowieka jest jednak o wiele dłuższa. W opracowaniu podjęto próbę ich zidentyfikowania, opisania oraz wskazania, w jakich obszarach mogą zostać efektywnie wykorzystane.

[177] Redakcja PRNews.pl, *Siła tkwi w biometrii*, PRNews.pl, 17 września 2020 [dostęp: 13.03.2021]. Raport. *Biometria w bankowości – kluczowe aspekty*. Redakcja T. Woszczyński, Warszawa, wrzesień 2015.

5.2. Identyfikacja biometryczna człowieka – podział i przykłady

Każdy człowiek posiada niepowtarzalne cechy biometryczne. Cechy te pozwalają odróżnić i jednocześnie zidentyfikować poszczególne osoby. Pierwszym kryterium podziału biometrii mogą być cechy fizjologiczne i odzwierciedlające zachowanie:

- cechy fizjologiczne, do których zalicza się: odcisk lini papilarnych, ciało ludzkie, twarz, odcisk dłoni, DNA, kształt ucha, układ lini krwionośnych, rogówka oka, siatkówka oka, ślady zębów;
- cechy odzwierciedlające zachowanie, do których zalicza się: temperaturę ciała, głos, podpis odręczny, tempo pisania itp.

Systemy biometryczne możemy też podzielić ze względu na:

- **cechy fizyczne:** tęczówka oka, siatkówka, linie papilarne, układ naczyń krwionośnych na dłoni lub przegubie ręki, kształt dłoni, kształt linii zgięcia wnętrza dłoni, kształt ucha, twarz, rozkład temperatur na twarzy, kształt i rozmieszczenie zębów, zapach, DNA itp.;
- **cechy behawioralne** związane z zachowaniem: sposób chodzenia, podpis odręczny, sposób pisania na klawiaturze komputera, głos, a nawet reakcje mózgu. Fala P300 jest reakcją mózgu charakterystyczną dla każdego człowieka.

Biometryczne techniki w praktycznych zastosowaniach zajmują się przede wszystkim weryfikacją osób (porównują uzyskane cechy z zapisaną wcześniej próbką, czyli dokonuje się wyboru jednego z wielu i weryfikuje), a w mniejszym stopniu ich identyfikacją, kiedy to uzyskane z pomiaru cechy należy porównać z każdą zapisaną w bazie próbką.

Obecnie najpopularniejsze techniki biometryczne można podzielić na następujące grupy:

- systemy rozpoznające na podstawie układu linii papilarnych;
- systemy rozpoznające na podstawie geometrii dłoni;
- systemy rozpoznające na podstawie brzmienia głosu;
- systemy rozpoznające na podstawie obrazu tęczówki oka;
- systemy rozpoznające na podstawie unikalnego układu naczyń krwionośnych dłoni;
- systemy rozpoznające na podstawie geometrii twarzy;

- rozpoznanie na podstawie niepowtarzalnego dla każdego człowieka kodu DNA[178].

Rozpoznanie i identyfikacja **osoby na podstawie odcisku palca** odbywa się na zasadzie porównania skanowanego palca z matrycą w bazie poprzez znajdowanie punktów identycznych na obydwu matrycach, a nie dopasowaniu matryc w całości identycznych. Takie rozwiązanie określane jest mianem daktyloskopii metody identyfikacji człowieka na podstawie śladów linii papilarnych opuszek palców rąk (źródło: Leksykon Policyjny). Linie papilarne to charakterystyczne układy (rysunki) listewek skórnych (wybrzuszeń naskórka), rozdzielonych równolegle biegnącymi bruzdami (rowkami)[179].

Linie papilarne opisuje się za pomocą tzw. **minucji** – charakterystycznych cech, takich jak: początki, zakończenia, rozwidlenia, haczyki itp. Wzajemny układ minucji jednoznacznie identyfikuje daną osobę. Do uznania dwóch śladów linii papilarnych za tożsame wystarczy od kilku do kilkunastu cech wspólnych (ta sama minucja występująca w tym samym miejscu). Przyjmuje się, że 12 cech wspólnych wystarcza do pewnego określenia tożsamości, choć niektóre minucje występujące rzadziej lub specyficzne dla danej populacji zmniejszają tę liczbę. W Polsce przyjmuje się, że wystarczające jest 12 zgodnych minucji, w przypadku minucji rzadziej występujących (np. oczka bądź haczyki) wystarczy ich mniej[180].

[178] https://pl.wikipedia.org/wiki/Zabezpieczenie_biometryczne [dostęp: 10.01.2023].
[179] https://www.bing.com/search?q=linie+papilarne+identyfikacja&form=ANSPH1&refig=3b0a4e2dbf2a4fda92a71e6e13a9a8de&pc=U531 [dostęp: 15.10.2022].
[180] https://pl.wikipedia.org/wiki/Linie_papilarne [dostęp: 15.10.2022].

Rys. 10. Podstawowe rodzaje minucji: 1 – początek, 2 – zakończenie, 3 – złączenie, 4 – rozwidlenie, 5 – styk czołowy, 6 – styk boczny, 7 – oczko, 8 – zespół oczek, 9 – kropka, 10 – odcinek, 11 – haczyk, 12 – mostek, 13 – skrzyżowanie, 14 – złączenie podwójne, 15 – rozwidlenie podwójne.
Źródło: https://ksiegarnia.difin.pl/upl/zalacznik-ilustracje.pdf [dostęp: 10.01.2023].

Punkty identyczne wyszukujemy poprzez analizę charakterystyk lokalnych oraz punktów szczególnych w obrazie linii papilarnych, a także ich wzajemnego ułożenia i nachylenia. Dla przykładu w odróżnieniu od wizerunku twarzy, odcisk palca charakteryzuje się trzema cechami:

- **linie papilarne nie zmieniają się w funkcji czasu** (odporne na proces starzenia się);
- **linie papilarne są statyczne i wyraźne** (tylko 3% populacji ma słabe odwzorowania odcisków palców);
- **odciski palców są niepowtarzalne** (powstają we wczesnym stadium płodowym i są różne nawet u bliźniąt jednojajowych).

Trzy prawa sformułowane przez Francisa Galtona[181] głoszą:

- **niezmienność** – linie papilarne nie zmieniają się przez całe życie. Zmienia się tylko ich rozmiar wraz ze wzrostem;

[181] Francis Galton – brytyjski podróżnik, przyrodnik, antropolog, eugenik, wynalazca, meteorolog, pisarz, lekarz, psychometra i statystyk, prekursor badań nad inteligencją.

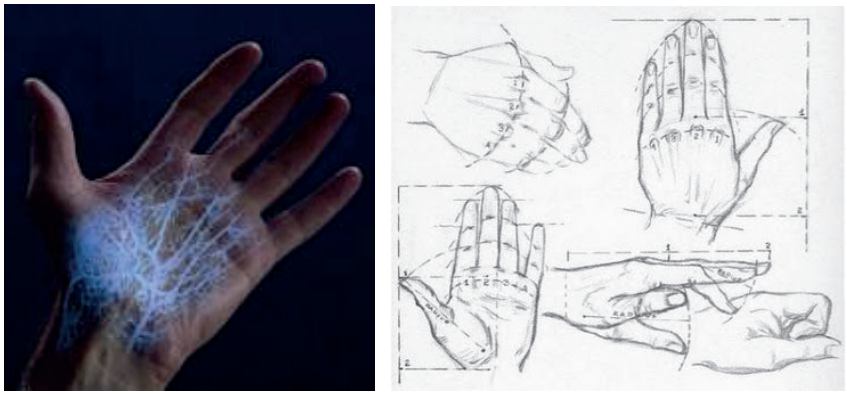
- **nieusuwalność** – linie papilarne nie ulegają zniszczeniu i zanikowi – aby taka sytuacja miała miejsce, należałoby uszkodzić skórę właściwą z listewkami skórnymi. Sytuacje takie jak skaleczenia czy oparzenia nie mają wpływu na ślad daktyloskopijny, ponieważ „rysunki" na palcach powracają po ustąpieniu obrażeń i regeneracji naskórka;
- **niepowtarzalność** – linie papilarne są charakterystyczne dla każdego człowieka. Jest praktycznie niemożliwe, aby dwie osoby miały identyczne ślady daktyloskopijne.

Oznacza to, że osoba porównująca ślad dowodowy z materiałem porównawczym może ze 100% pewnością potwierdzić, że dany ślad pochodzi od jednej, konkretnej osoby[182].

Linie papilarne palca są skanowane przez specjalny czujnik, wmontowany w system zabezpieczający. Następnie jego zapis zostaje przetworzony w cyfrowy kod, na podstawie którego weryfikuje się daną osobę. Rozwiązanie to jest bezpieczne, ponieważ **nie obraz palca (odcisk),** ale wyznaczany za pomocą algorytmu rozpoznania matematyczny odpowiednik tegoż obrazu jest porównywany z matrycą. Ma to kluczowe znaczenie w bezpieczeństwie przechowywania matryc porównawczych wszystkich pracowników. Dla przykładu systemy biometryczne oferowane przez **BioSys** nie przechowują obrazów linii papilarnych, a jedynie ich cyfrowy zapis.

Następną popularną techniką biometryczną są systemy rozpoznające na podstawie **geometrii dłoni**. Technologia ta oparta jest na trójwymiarowym obrazie ludzkiej dłoni wykonanym za pomocą kamery filmującej w podczerwieni. Przez odpowiednie urządzenie w procesie rejestracji wykonywany jest szereg zdjęć, po czym budowany jest wektorowy obraz dłoni. Kilka tysięcy charakterystycznych punktów jest branych pod uwagę w procesie rejestracji. Dodatkowo określane są takie cechy ludzkiej dłoni, jak: długość, szerokość, krzywizny, relatywne zależności odległości i kształtów, które wyróżniają indywidualne cechy każdej dłoni. Tylko sylwetka dłoni jest zapisywana. Wykonywane są między innymi dwa główne zdjęcia, z góry i z boku dłoni. Dużą zaletą tej technologii jest jej nieinwazyjność. Wynika to z faktu całkowitego braku kontaktu dłoni z sensorem rejestrującym jej kształt.

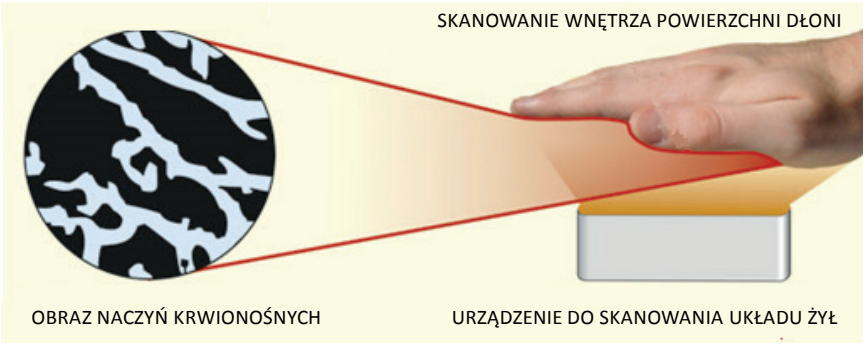
[182] Zasada 3N Francisa Galtona - Minnie - Kryminalistka [dostęp: 15.01.2023].



Rys. 11. Technologia rozpoznawania geometrii dłoni
Źródło: https://www.bing.com/ [dostęp: 15.01.2023].

W systemach kontroli dostępu niewątpliwą zaletą technologii jest to, że w przeciwieństwie do odcisku palca trójwymiarowy obraz dłoni nie jest nigdzie pozostawiany.

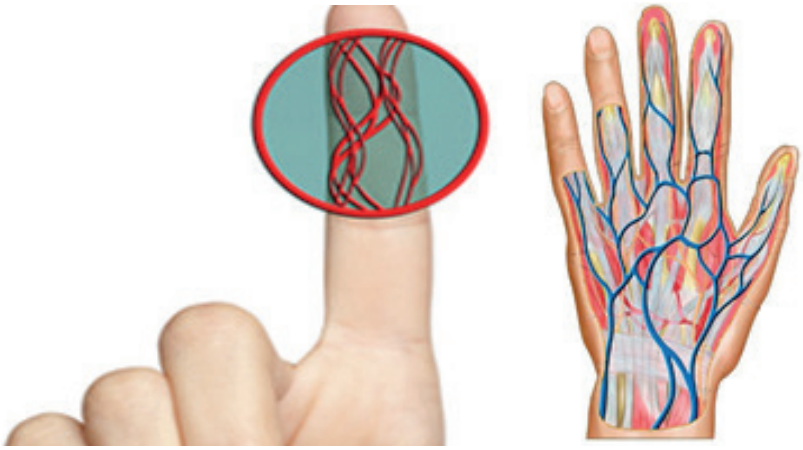
Rozpoznanie układu żył należy do technologii biometrycznych, z którymi wiąże się najwięcej nadziei. Wzorzec biometryczny żył znajduje się pod skórą, więc stosowanie tej technologii jest bezpieczne.



Rys. 12. Zasada działania techniki skanowania układu naczyń krwionośnych dłoni
Źródło:https://zabezpieczenia.com.pl/images/old/stories/zdjecia_artykuly/biometria/2/1_biometria_schemat_rozpoznawania.jpg [dostęp: 15.06.2023].

Wzór naczyń krwionośnych dłoni, palca, a nawet całego ciała każdej osoby jest niepowtarzalny (różnice istnieją nawet pomiędzy bliźniętami jednojajowymi oraz np. pomiędzy prawą i lewą dłonią jednej osoby). Wzór ten nie zmieni się w ciągu życia danej osoby – zmieni się bowiem tylko rozmiar układu

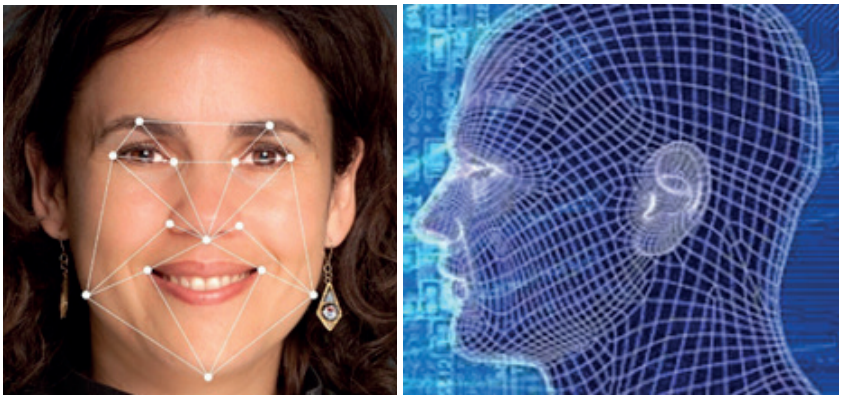
krwionośnego. Opisywana technologia została stworzona przez Josepha Rice'a. W 1985 roku jego determinacja przyczyniła się do powstania pierwszego prototypu rozpoznającego układ naczyń krwionośnych. Technologia ta zapewnia absolutną higienę, co wynika z braku kontaktu identyfikowanego ze skanerem. Sprawdzanie nieinwazyjnej tożsamości osoby odbywa się przez wykorzystanie efektu absorpcji fal podczerwonych przez komórki ciała/skórę/tłuszcz/ hemoglobinę. W jaki sposób rozpoznawany jest wzór naczyń krwionośnych? Otóż światło bliskiej podczerwieni (np. z diod LED) transmitowane jest przez dłoń, palec, nadgarstek i zostaje częściowo zaabsorbowane przez hemoglobinę znajdującą się w żyłach. Umożliwia to uzyskanie obrazu struktury znajdującej się poniżej zewnętrznej warstwy skóry, dając unikatowy wzór układu naczyń krwionośnych.



Rys. 13. Rozpoznanie układu żył jako jedna z technologii biometrycznych

Źródło: https://www.bing.com/images/search?q=%c5%bby%c5%82y+R%c4%99ki&form=RESTAB&first=1 [dostęp: 15.06.2023].

Kolejnym narzędziem do pobierania próbek jest aparat fotograficzny lub kamera, dzięki którym z uzyskanego w ten sposób obrazu tworzony jest wzór matematyczny opisujący cechy geometryczne, takie jak owal twarzy, szerokość twarzy, kształt ust, kształt nosa, kształt czoła, kształt brwi, kształt podbródka, kształt uszu. Istotnym faktem jest tutaj, że zależności pomiędzy poszczególnymi częściami twarzy nie ulegają znacznym zmianom z wiekiem.

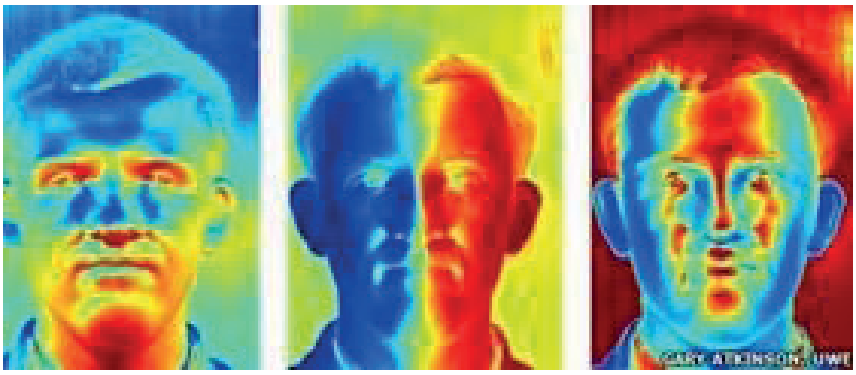


Rys. 14. Biometria twarzy

Źródło: https://biosys.pl/media/images/twarz-kobiety-biometria.width-1170.jpges_[dostęp: 20.01.2023].

Systemy weryfikujące użytkownika przy pomocy czytnika geometrii twarzy dążą do tego, aby w procesie tworzenia wzorca, wybrać cechy niezmienne (np. wielkość oczu) tak, aby móc go wykorzystywać w zmieniających się warunkach (np. zmiana uczesania). W przypadku tego typu metod identyfikacja użytkownika może napotkać na problemy przy niewłaściwym kącie nachylenia głowy, ale też zbyt słabym oświetleniu. To twarz z punktu widzenia biometrii charakteryzuje się cechami geometrycznymi, np.: kształt brwi, nosa, ust, podbródka oraz cechami antropometrycznymi, dotyczącymi np.: odległości między środkami oczu oraz pomiędzy oczami i nosem oraz linią oczu i linią ust.

Skonstruowanie automatycznego systemu, rozpoznającego ludzkie twarze zbliżonego do rozwiązania, w jaki robią to ludzie, jest trudnym wyzwaniem. Jedną z głównych zalet systemu rozpoznawania twarzy jest jego pasywność, tzn. system biometryczny nie wymaga szczególnych zachowań ze strony użytkowników, co nie jest ciągle możliwe do osiągnięcia przy zastosowaniu innych technik biometrycznych. Choć obecnie korzystanie z systemu biometrii twarzy jest dla użytkowników mniej wymagające niż korzystanie z innych systemów biometrycznych, to jednak ciągle wymaga ono pewnego zaangażowania ze strony użytkownika, np. zatrzymania się na moment przed obiektywem kamery.



Rys. 15. Układ temperatur twarzy

Źródło: https://ichef.bbci.co.uk/news/466/amz/worldservice/live/assets/images/2010/03/02/100302093657_1.jpg [dostęp: 20.01.2023].

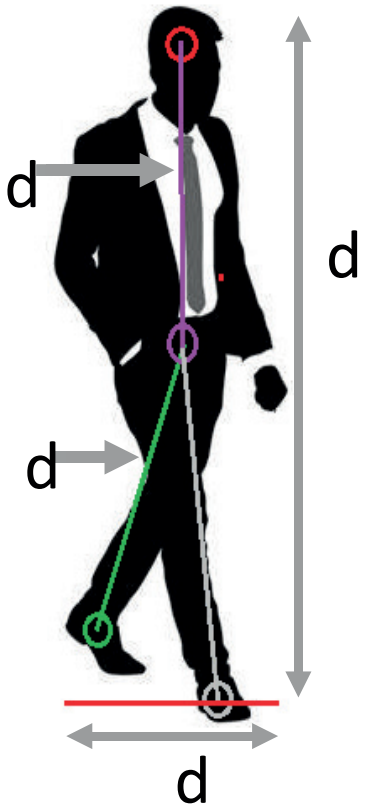
Dopiero kilka lat temu odkryto, że u każdego z nas układ temperatur na twarzy jest niepowtarzalny. Można go dojrzeć dzięki specjalnej kamerze termowizyjnej wychwytującej zmiany temperatury w dalekiej podczerwieni. W przeciwieństwie do skanowania tęczówki nie jest to metoda inwazyjna. Można też identyfikować osobę w całkowitych ciemnościach. Są też jednak wady – temperatura twarzy zależy częściowo od temperatury na zewnątrz, trudniej też ocenić tożsamość osoby w okularach, ponieważ odbijają promieniowanie. Najnowsze badania prowadzone przez Amerykanów donoszą o identyfikacjiosób z dokładnością 99%.

Rozpoznawanie chodu to proces identyfikowania osobnika na podstawie sposobu poruszania się. Metoda ta oferuje możliwość identyfikacji na odległość, a więc jest bezinwazyjna i bezkontaktowa (nie ma interakcji z urządzeniem biometrycznym). Już z daleka wiemy, z kim mamy do czynienia. Monitorowany nie musi o tym wiedzieć, a więc nie musi zachowywać się w sposób szczególny (wymuszony przez daną metodę biometryczną), jak to jest w przypadku innych technik biometrycznych. Jeszcze trudniej jest naśladować czyjś chód tak, by sensory i algorytmy komputerowe tego nie wykryły – przecież oprócz indywidualnej specyfiki chodu i budowy ciała ruch zależy od indywidualnego charakteru, umysłu.

Możemy wyróżnić dwie metody rozpoznawania chodu:

- w oparciu o analizę obrazu z kamer (np. monitoringu); najczęściej obliczany jest model ruchu obiektu;

- z użyciem radaru analogicznego, jak w przypadku pomiaru prędkości samochodów rejestrowany jest sposób poruszania się poszczególnych części ciała.



Rys. 16. Rozpoznanie za pomocą identyfikacji sposobu chodu

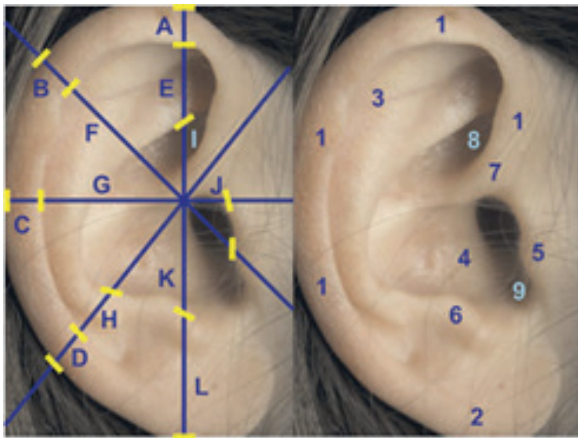
Źródło: opracowano na podstawie https://www.researchgate.net/figure/a-The-truncated-cone-body-model-b-Joint-positions-c-Kinematic-tree_fig1_220866810 [dostęp: 15.04.2024].

Własności ucha z punktu widzenia biometrii to unikalny kształt dla każdego człowieka, który nie ulega zmianie z wiekiem, indywidualny rozkład naczyń krwionośnych.

Zalety biometrii kształtu ucha to:

- większa ochrona danych osobowych niż w przypadku weryfikacji na podstawie rozpoznawania twarzy;
- koszty elementów dokonujących akwizycji próbki biometrycznej niższe niż koszty czytników linii papilarnych;

- niewrażliwość na mimikę;
- bogactwo cech biometrycznych w przestrzeni 3D.



Rys. 17. Rozpoznanie za pomocą identyfikacji ucha

Źródło: https://zabezpieczenia.com.pl/images/old/stories/zdjecia_artykuly/biometria/2/9_ biometria_ucho.jpgs [dostęp: 25.01.2023].

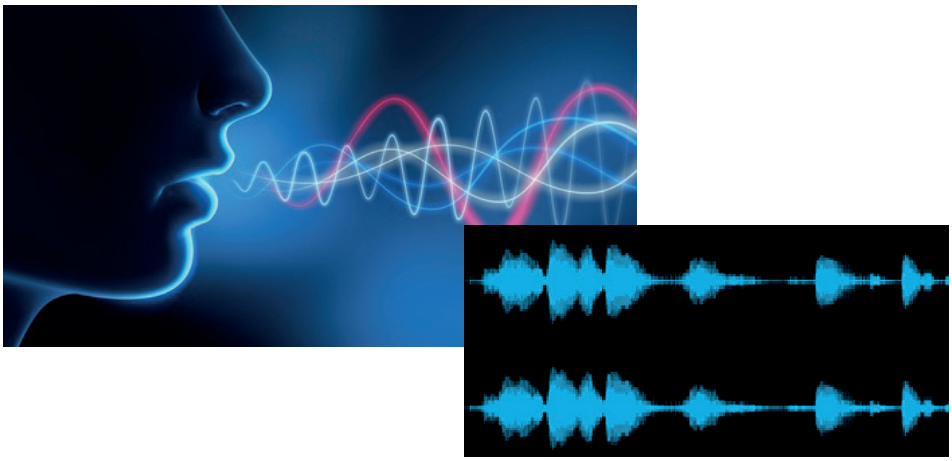
Odczytywanie stanu zdrowia z tęczówki (irydologia) było znane już w starożytności.Od lat 50. XX wieku proponowano wykorzystanie wzorów tęczówki do identyfikacji. Prototyp algorytmu rozpoznawania powstał w 1991 roku. Metoda oparta na analizie zdjęcia tęczówki oświetlonego światłem podczerwonym. Z obrazu ekstrahowane są punkty charakterystyczne i zapisywane w skróconej postaci. Obecne systemy rozpoznawania tęczówki najpierw robią ogólne „rozpoznanie'' zarysów twarzy w celu znalezienia oczu. Następnie specjalna kamera wykonuje zdjęcie tęczówki o bardzo wysokiej rozdzielczości.

Rys. 18. Rozpoznanie za pomocą identyfikacji tęczówki oka

Źródło: https://kurs-na-funta.pl/informacje/wp-content/uploads/2021/04/biometrics-eye--1024x683.jpg [dostęp: 25.06.2023].

Systemy radzą już sobie z przypadkowymi i celowymi ruchami głowy, mrugnięciem czy przymknięciem powieki. Nie stanowią problemu okulary czy szkła kontaktowe. Następnie system ze zrobionego zdjęcia przygotowuje kod zawierający skrócony opis punktów charakterystycznych. W systemach zaawansowanych taki kod jest następnie szyfrowany (z zastosowaniem szyfrów jednokierunkowych) i porównywany z zaszyfrowanym kodem oryginału – zapisanym w bazie danych. W tego typu systemach nawet po wykradzeniu zaszyfrowanego kodu nie jest możliwe odtworzenie na jego podstawie zarysu tęczówki. Tęczówka oka jest uznawana obecnie za najdoskonalszy identyfikator człowieka. Zostaje ona ukształtowana już pod koniec 15. tygodnia życia płodowego i pozostaje dalej w niezmienionej postaci (pomijając uszkodzenia mechaniczne i poważne choroby). Jej dodatkową zaletą jest fakt, że jest chroniona przez inne narządy przed ewentualnymi uszkodzeniami. Potwierdzeniem posiadania przez nią wielu indywidualnych cech jest fakt, iż do tej pory nie znaleziono dwóch identycznych tęczówek – pozwala ona na rozróżnienie nawet bliźniąt jednojajowych. Systemy biometryczne dokonujące identyfikacji na podstawie tęczówki oka porównują badaną tęczówkę z zapamiętanym wcześniej wzorcem. Zdjęcie tęczówki wykonywane jest w wysokiej rozdzielczości i na jego podstawie określane są cechy charakterystyczne.

Rozpoznanie mowy – technologia pozwalająca komputerowi lub przy pomocy innego urządzeniu interpretować mowę ludzką, na przykład do celów transkrypcji lub jako alternatywną metodę interakcji.



Rys. 19. Rozpoznanie za pomocą identyfikacji mowy

Źródło: https://www.soitron.pl/wp-content/uploads/2017/01/speaking-clearly-the-case-for-voice-biometrics-image-1-21.jpg [dostęp: 25.01.2023].

Wartości skuteczności systemów rozpoznawania mowy zależą najczęściej od przyjętego scenariusza testu. Dlatego informacje liczbowe, wbrew intuicji, zwykle nie są dobrym odzwierciedleniem jakości takich systemów.

Najskuteczniejszą metodą jest porównanie dwóch lub więcej systemów na takim samym scenariuszu testowym. Jakość systemów może jednak także zależeć od tego, jak sygnał jest rejestrowany. Przykładowo wiele z systemów oferowanych dla języka polskiego działa dużo gorzej dla sygnału z sieci GSM. Ogólnie należy przyjąć, że rozpoznawanie mowy polskiej działa poprawnie tylko dla pojedynczych słów lub dla ustalonych zbiorów scenariuszy dialogów. Próg komercyjnej akceptowalności systemów rozpoznawania mowy zwykle przyjmuje się jako 95% poprawności rozpoznania.

Każdy człowiek posiada unikatową barwę głosu, jest to cecha osobnicza wynikająca z budowy anatomicznej traktu głosowego. Na barwę ludzkiego głosu mają wpływ:

- budowa fizyczna kanału głosowego wpływająca na: pozycję, energię oraz kształt formantów głosowych;
- kształt jamy nosowej wpływa na brzmienie głosek nosowych.

Cechy behawioralne: idiolekt, dialekt, prozodia, nawyki mówcy:

- krtań – ton krtaniowy, fonacja, energia dźwięku;
- jama ustna –artykulacja, seria rezonansów związanych z kształtem jamy ustnej;

- pozycją artykulatorów (język, języczek, podniebienie, zęby, usta, jama nosowa),
- jama nosowa – rezonans nosowy.

Od kilkunastu lat jest absolutnie jasne, że ciała różniących się genami ludzi wydzielają różne zapachy. Każdy człowiek wydziela niepowtarzalny zapach, który jest kombinacją w przybliżeniu trzydziestu różnych woni. Celem systemów rozpoznawania zapachu ludzkiego ciała nie jest tylko to, by zdefiniować te wszystkie komponenty, ale także to, by ocenić ich koncentrację. Aby zidentyfikować człowieka na podstawie zapachu jego ciała, używa się specjalnych urządzeń elektronicznych, tzw. sztucznych nosów (lub e-nosów). Dwa główne komponenty tych nosów to system wyczuwania (detekcji) i system rozpoznawania na podstawie wzorców.

Rys. 20. Weryfikacja podpisu z prototypem

Źródło: Opracowano na podstawie: https://www.bing.com/images/search?q=podpis+odr%C4%99czny &qpvt=podpis+odr%c4%99czny&form=IQFRML&first=1&cw=1905&ch=961 [dostęp: 15.04.2024].

Podpis był przez wiele lat przyjętą ogólną formą stwierdzenia wiarygodności. Istotną właściwością automatycznych systemów identyfikacji podpisu jest zdolność do rozróżniania pomiędzy postacią podpisu nawykowego (regularnego), a postaciami trochę zmienionymi, które pojawiają się za każdym razem, gdy osoba pisze swoje nazwisko.

Istnieje ponad 100 patentów na tego rodzaju systemy. Ogólnie sprowadzają się one do tego, że na podstawie treningowego zbioru podpisu tworzony jest prototyp podpisu, następnie pozwala to na weryfikację podpisu z prototypem.

Podpis biometryczny to podpis składany specjalnym rysikiem na specjalnie do tego dostosowanym, dotykowym urządzeniu elektrycznym – miedzy innymi tablecie, telefonie lub też urządzeniu stacjonarnym. Jego rolą jest połączenie standardowych funkcji biometryczno-grafologicznych podpisu odręcznego z funkcjonalnością i oszczędnością. Możliwość lub całkowite wyeliminowanie dokumentów papierowych to nie tylko oszczędne, ale również ekonomiczne rozwiązanie. Znacznie szybsza obsługa klientów, biometria podpisu (rozpoznawanie kształtu, siły nacisku, tempa pisania, itp.), wysokie standardy bezpieczeństwa oraz postępujący proces *paperless* sprawiają, że elektroniczne podpisywanie dokumentów cieszy się coraz większą popularnością.

Metody analizy podpisu:

- **metody statyczne** (obraz statyczny podpisu, brak informacji o kolejności występowania elementów podpisu);
- **metody dynamiczne** (pozyskiwanie podpisu metodą elektroniczną – rejestracja procesu podpisywania się, zachowanie informacji o kolejności występowania elementów podpisu).

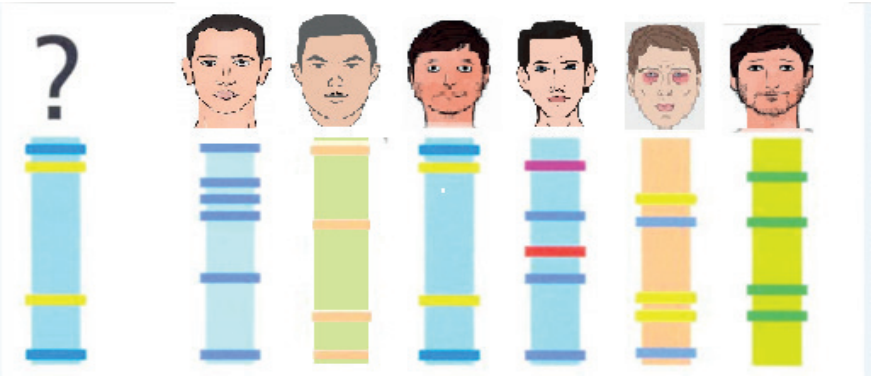
DNA w biometrii to przyszłość. Będzie to technika najbardziej wiarygodna, ponieważ gen ludzki reprezentowany przez helisę DNA jest unikalny i na tyle skomplikowany, że nie daje się podrobić, a pomyłka jest praktycznie niemożliwa.

Rozpoznawanie DNA różni się znacząco od wcześniej opisanych technik. Wymaga namacalnej próbki do zbadania, a nie, jak poprzednio, obrazu optycznego, podczerwonego, czy w przypadku metod zachowawczych – nagrania. Rozpoznanie nie jest wykonywane w trybie rzeczywistym i obecnie nie wszystkie jego fazy są zautomatyzowane.

Rys. 21. Kod genetyczny

Źródło: https://i0.wp.com/www.info24service.com/wp-content/uploads/Fremde-Gene_2019-065-0000.png?ssl=1 [dostęp: 15.01.2022].

W celu identyfikacji i weryfikacji osobnika należy pobrać próbkę jego tkanki. Zwykle dla uzyskania lepszego, nieprzekłamanego efektu, naukowcy zalecają pobranie tkanki z kilku źródeł, takich jak: krew, kości, włosy. Obecnie zastosowanie metody ogranicza się głównie do medycyny sądowej, włączając w to pełną weryfikację ojcostwa.



Rys. 22. Identyfikacja za pomocą kodu genetycznego

Źródło: A. Czyżewski, P. Hoffmann, *Przegląd technologii biometrycznych Katedra Systemów Multimedialnych*, Wydział Elektroniki, Telekomunikacji i Informatyki Politechnika Gdańska.

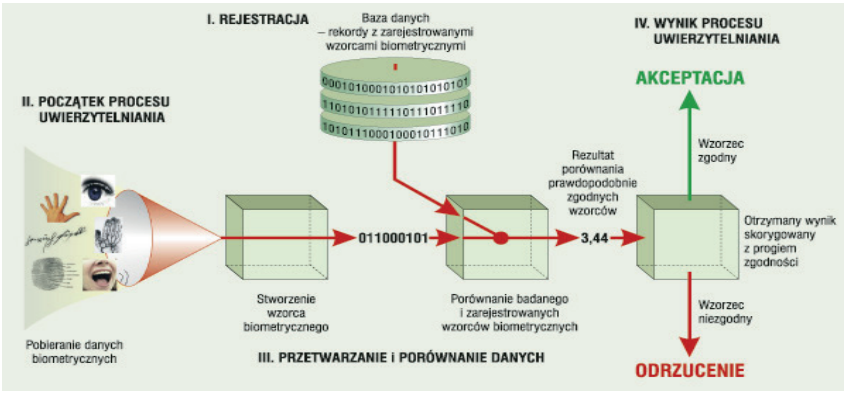
DNA w biometrii to jedno z głównych narzędzi kryminalistyki:

- blisko 3 miliony elementów DNA definiują różnice międzyosobnicze;
- różnicowanie polega na badaniu polimorfizmu sekwencji i ich długości;
- cechy biometryczne to liczby powtórzeń konkretnych sekwencji nukleotydów.

Jak to możliwe? Już nawet znikoma ilość materiału biologicznego pozostawiona na miejscu popełnienia przestępstwa może naprowadzić organy ścigania na właściwy trop. Źródło takiego materiału mogą stanowić włosy, ślina, niedopałek papierosa, ślady krwi czy spermy, ponieważ DNA znajduje się prawie w każdej komórce ludzkiego ciała. Warunkiem odpowiedniej identyfikacji przestępcy jest oczywiście pewność, że próbka należy do właściwej osoby. Eksperci zajmujący się badaniem miejsc zbrodni muszą zatem bardzo uważać, aby nie zanieczyścić znalezionego materiału genetycznego materiałem należącym do zupełnie innej osoby. Laboratoria kryminalistyczne wykonują tego typu badania m.in. w sprawach dotyczących morderstw, przestępstw na tle seksualnym, jak i narkotykowych.

5.3. Zastosowanie wybranych rozwiązań biometrycznych

W zastosowaniu praktycznym identyfikacja osób w oparciu o indywidualne niepowtarzalne cechy stwarza nowe możliwości w wielu obszarach związanych z bezpieczeństwem informacji. Przedstawione wybrane niepowtarzalne cechy człowieka przynoszą szereg różnorodnych możliwości, dzięki którym przykładowo systemy kontroli dostępu stosują zasadę **„Kim jesteś i co robisz”**. Takie rozwiązanie nazywamy **biometrycznym systemem kontroli dostępu**. System ten w ogólności złożony jest z czytnika biometrycznego lub urządzenia skanującego, oprogramowania konwertującego pobraną z czytnika informację do postaci cyfrowej oraz bazy danych, która przechowuje dane biometryczne – wzorce niezbędne do porównania z danymi pochodzącymi od użytkownika z czytnika. W czasie konwersji informacji pobranej w czytniku oprogramowanie identyfikuje określone punkty charakterystyczne, które następnie są przetwarzane przy użyciu wybranego (optymalnego) algorytmu matematycznego do postaci, która może być w skuteczny sposób porównana z rekordem w bazie danych. Zasadę działania przedstawiono na rysunku.



Rys. 23. Przetwarzanie i porównywanie danych

Źródło: http://www.kamery.pl/storage/arty/zasada_biometria.jpg [dostęp: 25.01.2023].

Pierwszym krokiem przy zastosowaniu biometrycznego systemu kontroli dostępu jest tzw. rejestracja poszczególnych użytkowników w systemie. Polega ona na pobraniu od nich odpowiednich dla sytemu unikatowych cech biometrycznych w postaci próbek. Dedykowane algorytmy matematyczne przetwarzają pobrane dane w cyfrowy wzorzec biometryczny. Pozyskane biometryczne wzorce cyfrowe przechowywane są w zależności od zastosowanego systemu w bazie danych urządzenia biometrycznego, zewnętrznego serwera lub na samodzielnym nośniku informacji (na dyskietce, w pamięci flash, na karcie magnetycznej itp.).

Działanie algorytmów wykorzystywanych w systemach biometrycznych polega na analizie związków i relacji pomiędzy określonymi punktami charakterystycznymi w przetwarzanej próbce. W zależności od wykorzystywanej techniki pod uwagę branych jest nawet do kilkudziesięciu tysięcy punktów charakterystycznych.

Dzięki wykorzystaniu algorytmów sprawdzających relacje pomiędzy poszczególnymi punktami istnieje możliwość optymalnego i skutecznego rozpoznania osoby. W zależności od rodzaju mierzonych cech biometrycznych można zastosować **dwie podstawowe grupy technik biometrycznych**. Pierwsza grupa to systemy **bazujące na pomiarach anatomicznych** (cechy fizyczne – genotyp) i druga grupa **behawioralnych** (to cechy związane z zachowaniem – fenotyp).

Biometria wykorzystywana jest nie tylko jako sposób kontroli dostępu do chronionych pomieszczeń lub autoryzacji użytkowników korzystających z określonych danych, programów czy urządzeń. Uniemożliwia także realizację nieautoryzowanego dostępu do bankomatów, komputerów osobistych, sieci

komputerowych, telefonów komórkowych, telefonów domowych, systemów alarmowych, zamków drzwiowych, kart procesorowych itp. Ponadto w obiektach użyteczności publicznej i firmach systemy biometryczne wspomagają wyszukiwanie miejsca pobytu wybranych osób oraz rejestrację czasu pracy.

W biometrii do często używanych pojęć możemy zaliczyć: **uwierzytelnianie, identyfikację, autoryzację i weryfikację**.

- **uwierzytelnianie** (nazywane często, lecz niepoprawnie **„autentykacją")** to potwierdzanie tożsamości, autentyczności, stwierdzenie prawdziwości również z uwzględnieniem określonego prawdopodobieństwa czy tożsamość, którą deklaruje osoba, jest zgodna z prawdą. Stuprocentowa pewność w przypadku uwierzytelniania nie jest w praktyce możliwa, stąd mowa o prawdopodobieństwie;
- **identyfikacja użytkownika** (ang. *identification*) jest procesem polegającym na przedstawieniu przez użytkownika przyznanego mu w procesie rejestracji identyfikatora i odpowiedzi na pytanie „Kim jest osoba identyfikowana??, czyli porównanie przyznanego w procesie rejestracji identyfikatora ze wszystkimi rekordami w bazie danych (tzw. porównanie 1:N – jeden do wielu);
- **autoryzacja** jest procesem weryfikacji uprawnień osoby do określonych zasobów. Autoryzację zwykle poprzedza **uwierzytelnienie**: najpierw „kto", potem „do czego ma prawo"; polega na przedstawieniu się użytkownika i uzyskaniu odpowiedzi na pytanie „Czy osoba, za którą on się podaje, jest tą osobą?", czyli porównanie przedstawionego identyfikatora z wzorcem wcześniej przydzielonym i zapisanym w bazie danych (tzw. porównanie 1:1 – jeden do jeden).

Często **pojęcia uwierzytelniania, identyfikacji i weryfikacji** używane są zamiennie bądź też utożsamiane są ze sobą bez postrzegania różnic. Jest to błędne rozumowanie. W istocie **weryfikacja i identyfikacja** są **różnymi procesami** (mającymi praktyczne zastosowanie w różnych systemach bezpieczeństwa i charakteryzującymi się różnymi czasami reakcji) i stanowią podzbiór procesu uwierzytelniania.

Przykładowo, w usługach bankowości biometrycznej mamy możliwość zmiany transakcji tradycyjnych (papierowych) związanych z wypłatą gotówki.

Jak to działa?

W celu udostępnienia usług bankowości biometrycznej bank pobiera od użytkownika trzy wzorce biometryczne z jednego palca prawej oraz lewej dłoni przy użyciu czytnika biometrycznego – urządzenia do skanowania układu naczyń krwionośnych. Wprowadza te dane do systemu wraz z pozostałymi danymi osobowymi. Gdy użytkownik posiada tylko jedną dłoń, bank pobiera wzorzec z dwóch palców tej dłoni. Skaner naczyń krwionośnych prześwietla palec niewidzialnym, nieszkodliwym dla człowieka światłem w podczerwieni w krótkim czasie wynoszącym ok. 1.5 sekundy, które jest absorbowane przez hemoglobinę znajdującą się w płynącej „żywej" krwi w żyłach palca, powodując tworzenie cienia. Taki cień widziany w kamerze to sieć naczyń krwionośnych. Obraz jest następnie przetwarzany na krótki kod biometryczny, który staje się osobistym, niepowtarzalnym PIN-em klienta.

Bankowość biometryczna to nowoczesność, bezpieczeństwo i wygoda. Usługa bankowości biometrycznej opiera się na zastosowaniu nowoczesnych systemów do weryfikacji tożsamości. Usługi bankowości biometrycznej obejmują:

- wypłatę gotówkową;
- wypłatę w bankomacie biometrycznym (w sieci bankomatów);
- przelewy na rachunki prowadzone w bankach, w których weryfikacja tożsamości oraz autoryzacja transakcji odbywa się za pomocą wzorca biometrycznego klienta.

Cechy biometryczne pozwalają wyeliminować słabe punkty innych, starszych sposobów identyfikacji i weryfikacji osób. Jak powszechnie wiadomo kody PIN mogą być zapomniane lub ukradzione, a dowody osobiste mogą ulec zagubieniu lub kradzieży. Tych wad nie posiadają systemy identyfikacji biometrycznej, gdyż hasłem, numerem PIN lub kartą dostępu jest sam człowiek, z własnym indywidualnym kluczem przewidzianym przez naturę. Tak więc systemy biometryczne odznaczają się dodatkową bardzo przydatną zaletą – wykluczają przykrości związane z zapomnieniem lub zgubieniem nośnika identyfikacji.

W przypadku kontroli dostępu za pomocą linii papilarnych weryfikacja musi się odbywać bardzo szybko i z dużą dokładnością. Służą do tego czytniki linii papilarnych. Urządzenia takie wyposażone są w odpowiednie pole skanujące, do którego należy przyłożyć opuszkę dowolnego palca prawej lub lewej dłoni. System sprawdza linie papilarne, bada układ punktów charakterystycznych i innych cech identyfikujących palec. Stosowane mogą tu być dwa rozwiązania:

identyfikacja jest dokonywana w samym czytniku (jest to wtedy urządzenie dość złożone) albo (częściej) w połączonym z nim komputerze PC. Banki z biometrii odnoszą znaczne korzyści, które polegają głównie na:

- wyższym bezpieczeństwie wykonywanych operacji;
- pełnej niezaprzeczalność wykonania transakcji przez klienta;
- transakcje bez kart i brak konieczności pamiętania numerów PIN przez klientów;
- usprawnienie procesu autoryzacji i większy komfort klientów w korzystaniu z urządzeń;
- niższe koszty poprzez lokalnie realizowaną autoryzację biometryczną;
- brak opłat zewnętrznych i dodatkowych za korzystanie z usługi;
- możliwa równoległa autoryzacja PIN i biometria;
- bank zyskuje wizerunek nowoczesnego i innowacyjnego.

Czytniki geometrii dłoni wykonują trójwymiarowe zdjęcie dłoni, rejestrując długość, szerokość, grubość czterech palców oraz wielkość obszarów pomiędzy kostkami. Łącznie wykonywanych jest ponad 90 pomiarów różnych cech charakterystycznych dłoni. Wynik tych pomiarów jest przechowywany w pamięci urządzenia w formie 9-bajtowego wzorca, co w teorii daje ponad 4 tryliardy możliwych kombinacji. Identyfikator ten jest praktycznie unikatowy dla każdego człowieka. Wiele przenośnych komputerów już dziś wyposaża się w skanery odcisków palców. Użytkownik, aby się zalogować, musi położyć palec na skaner. Producenci niektórych profesjonalnych notebooków idą jeszcze dalej. W zaawansowanych urządzeniach można wykorzystywać odciski palców nie tylko do logowania, ale również do kodowania danych na dysku twardym. Jeśli taki notebook zgubimy, znalazca nie może nic zrobić z zapisanymi danymi, nawet jeśli zamontuje dysk twardy w innym komputerze.

Rys. 24. Czytniki i skanery lini papilarnych

Źródło: https://www.bing.com/search?q=skaner+linii+papilarnych&form=ANSPH1&refig= dbb595696ccc419e87501ac08ef29a74&pc=U531 [dostęp: 25.05.2023].

Systemy rejestracji czasu pracy (RCP – rejestracja czasu pracy) dokonały rewolucji w zakresie kontroli i rozliczania pracowników w zakresie dyscypliny pracy. Błyskawiczne, wykonywane bez żadnego wysiłku szczegółowe raporty komputerowe i analizy, stały się podstawą do pełniejszej oceny wydajności pracy poszczególnych pracowników oraz lepszej kontroli ewentualnego naruszenia przez nich regulaminu pracy. Kontrola czasu pracy jest po prostu opłacalna. Ewidencja czasu pracy RCP wykorzystuje nowoczesne technologie, takie jak biometria – rozpoznawanie odcisków palca, RFID/MIFARE – zbliżeniowe karty radiowe, LCD – mini monitory do prezentacji zdjęcia pracownika, Wi-Fi – radiowa łączność bezprzewodowa.

Rys. 25. Polski paszport biometryczny

Źródło: https://www.bing.com/images/search?q=Paszport+Polski&form=RESTAB&first=1 [dostęp: 25.05.2023].

Paszport biometryczny – dokument tożsamości odczytywany przy pomocy urządzeń optycznych i elektronicznych, zawiera dane biometryczne. Dokument pozwala zidentyfikować tożsamość na podstawie cech ciała, takich jak linie papilarne czy wzór siatkówki oka. Informacje są przechowywane na chipie EEPROM o pojemności minimum 32 KB według standardu ISO 14443, a także w kartotekach lub bazach danych urzędów – najczęściej w sposób zdecentralizowany, według miejsca zameldowania.

W Polsce paszporty biometryczne weszły w życie 28 sierpnia 2006 roku. Książeczki polskich paszportów biometrycznych produkuje Polska Wytwórnia Papierów Wartościowych S.A. Dane obywateli nanoszone są w Centrum Personalizacji Dokumentów MSWiA. Polskie paszporty biometryczne zawierają wizerunek twarzy i odciski palców zapisane w formie elektronicznej. Paszporty wydane do 29 czerwca 2009 roku zawierają tylko wizerunek twarzy. Od 28 czerwca 2009 roku zaczęto wydawać biometryczne paszporty serii EA z odciskami palców zapisanymi w chipie RFID.

Także biometria tęczówki oka znalazła po raz pierwszy zastosowanie w bankowości w Jordanii (Cairo Amman Bank) – na potrzeby bankomatów oraz oddziałów banku, a w dalszej kolejności – w bankowości internetowej. W Polsce historia biometrii w bankowości rozpoczęła się w 2010 r. – Bank Polskiej Spółdzielczości oraz Podkarpacki Bank Spółdzielczy zastosowały biometrię odcisku palca. W późniejszym okresie rozwiązania biometryczne zaczęły być oferowane przez inne banki, np. przez Bank BPH czy Getin Bank. Obecnie najbardziej atrakcyjne wydaje się jednak zastosowanie biometrii w bankowości mobilnej.

Wraz z rozwojem technologii biometrycznych zyskuje się coraz większą trafność odpowiedzi i szybkość działania, czego efektem jest zwiększenie obszaru ich zastosowań. Opracowane z myślą o służbach bezpieczeństwa mogą być użyte do wykrywania niepożądanych osób na lotniskach, dworcach, stadionach czy w centrach handlowych. Od kilku lat w miejscach publicznych umieszczane są systemy rozpoznawania twarzy w celu zwiększenia skuteczności wykrywania poszukiwanych przestępców. Monitoring coraz powszechniej stosowany jest na stacjach paliw, osiedlach mieszkaniowych, placach miejskich, w sklepach, a także prywatnych nieruchomościach. W połowie 2014 r. media donosiły o ujęciu w Chicago pierwszego przestępcy dzięki uruchomionemu systemowi kamer miejskich sprzężonych z technologią rozpoznawania twarzy NeoFace (jego zdjęcie znajdowało się w policyjnej bazie danych). Technologie te mogą być również stosowane np. do identyfikacji ważnych osób w miejscach publicznych, takich

jak hotele, luksusowe sklepy, kasyna itd. Na niektórych lotniskach dla często podróżujących osób posiadających dokumenty z identyfikatorami biometrycznymi już dawno udostępniono specjalne przejścia przyspieszające odprawę. Największą zaletą identyfikacji i weryfikacji osób w wyniku cyfrowej analizy przy zastosowaniu komputerowych urządzeń biometrycznych jest bezsporna, porównawcza, indywidualna identyfikacja niepowtarzalnych i charakterystycznych cech budowy wybranych elementów ciała ludzkiego. Obecnie techniki biometryczne mają zastosowanie:

- jako zabezpieczenia systemów informatycznych,
- jako kontrola dostępu oraz identyfikacja użytkownika związana z bezpieczeństwem obiektów,
- przy identyfikacji stron transakcji finansowych.
- Wady:
- użycie biometrycznych identyfikatorów w handlu elektronicznym może oznaczać, że informacja jest globalnie osiągalna, ale dostępna tylko przy pomocy klucza biometrycznego;
- taki klucz biometryczny jest rzeczywiście przenośny i może dostarczyć niezbitych dowodów identyczności;
- pozostaje problem pewności bezpieczeństwa i prywatności transakcji. Teoretycznie technologia biometryczna może dostarczyć zarówno perfekcyjne bezpieczeństwo, jak i prywatność;
- zarówno bezpieczeństwo i prywatność może być kompromisem w systemie biometrycznym, jeśli zapis biometryczny lub używanie danych zostaną sprzedane, ukradzione lub użyte do śledzenia określonej osoby, wymagane jest wprowadzenie z wyprzedzeniem odpowiednich systemów zabezpieczeń
- system biometryczny musi być zaimplementowany wewnątrz właściwego otoczenia zabezpieczającego, aby był wiarygodny i użyteczny.

Największą zaletą komputerowych urządzeń biometrycznych jest **bezsporna, kategoryczna identyfikacja i weryfikacja** osób w wyniku cyfrowej analizy porównawczej indywidualnych, niepowtarzalnych cech budowy wybranych elementów ciała ludzkiego. **Podstawową funkcją biometrii** jest uniemożliwianie realizacji nieautoryzowanego dostępu do bankomatów, komputerów osobistych, sieci komputerowych, telefonów komórkowych, domowych systemów alarmowych, zamków drzwiowych, kart procesorowych itp. **Ponadto w obiektach użyteczności publicznej i firmach,** systemy biometryczne wspomagają wyszukiwanie miejsca pobytu wybranych osób oraz rejestrację czasu pracy.

System kontroli dostępu, w którym wykorzystuje się zasadę „Kim jesteś i co robisz", nazywamy **biometrycznym systemem kontroli dostępu**. System ten w ogólności złożony jest z **czytnika biometrycznego lub urządzenia skanującego**, **oprogramowania, które konwertuje pobraną z czytnika informację do postaci cyfrowej oraz bazy danych**, która przechowuje dane biometryczne – wzorce niezbędne do porównania z danymi pochodzącymi z czytnika.

W czasie konwersji informacji pobranej w czytniku oprogramowanie identyfikuje określone punkty charakterystyczne, które następnie są przetwarzane przy użyciu wybranego **(optymalnego) algorytmu matematycznego** do postaci, która może być w skuteczny sposób porównana z rekordem w bazie danych. **Działanie algorytmów** wykorzystywanych w systemach biometrycznych polega na analizie związków i relacji pomiędzy określonymi punktami charakterystycznymi w przetwarzanej próbce. W zależności od wykorzystywanej techniki pod uwagę branych jest nawet do kilkudziesięciu tysięcy punktów charakterystycznych.

Przedstawiony opis biometrii potwierdza, że jest ona wykorzystywana jako sposób kontroli dostępu do chronionych pomieszczeń lub autoryzacji użytkowników korzystających z określonych danych, programów czy urządzeń. Ma także zastosowanie przy zapewnieniu bezpieczeństwa i ochrony dostępu do przechowywanych informacji. Przez zastosowanie biometrii wspartej nowoczesnymi rozwiązaniami w systemach i sieciach komputerowych możemy zapewnić poufność, integralność, rozliczalność i bezpieczeństwo informacji. To dzięki rozwiązaniom biometrycznym możemy także dokonać uwierzytelnienia, identyfikacji i autoryzacji, a tym samym poprawić bezpieczeństwo w wielu obszarach naszego funkcjonowania.

6. KRYPTOGRAFIA NA POTRZEBY BEZPIECZEŃSTWA INFORMACJI

6.1. Wprowadzenie do kryptografii

Na przełomie wieków człowiek korzystał z informacji stosując różne rozwiązania. Zazwyczaj wynikały one z rozwoju w poszczególnych okresach cywilizacyjnych i korzystały z dostępnych w tym czasie metod. Informacja nie stanowiła problemu, gdy jej przeznaczenie dotyczyło ogółu obywateli, była ogólnie dostępna i nie zawierała tajemnych treści. Gdy w grę wchodziły niejawne informacje należało sięgnąć po takie rozwiązania, które mogły zapewnić im odpowiednią ochronę. Nie ulega wątpliwości, że dla informacji (danych) zarezerwowanych dla ograniczonej grupy osób czy pojedynczych odbiorców należy zastosować takie rozwiązanie, które zapewnią im odpowiednie bezpieczeństwo. Można to osiągnąć różnymi sposobami, chociaż najskuteczniejszym rozwiązaniem jest zapewne kryptografia.

Celem tej części opracowania jest przedstawienie kryptografii zajmującej ważne miejsce w zapewnieniu bezpieczeństwa informacji. W tym celu przeprowadzono analizę rozwoju kryptografii od początku jej funkcjonowania do czasów współczesnych. Dokonana analiza pozwoliła na przedstawienie praktycznego zastosowania kryptografii do ochrony informacji w różnych okresach jej rozwoju. Za szczególnie ważne w obecnych czasach proponuje się uznać popularyzację rozwiązań kryptograficznych umożliwiających zapewnienie bezpieczeństwa informacji w systemach i sieciach komputerowych.

W opracowaniu zaproponowano stanowiącą przypuszczenie następującą **hipotezę roboczą**: dla zapewnienia bezpieczeństwa gromadzonym,

przetwarzanym i przesyłanym informacjom wymagane jest poszukiwanie skutecznych nowoczesnych rozwiązań. Na wstępie założono, że rozwiązań takich może dostarczyć kryptografia, wykorzystująca wiedzę matematyczną do skutecznej ochrony informacji w systemach i sieciach komputerowych.

W celu weryfikacji zaproponowanej hipotezy wykorzystano dwie metody badawcze: **analizę i syntezę** oraz ich wzajemną interakcję. Analiza jako metoda badawcza polegająca na operacji myślowej opierającej się na rozłożeniu badanej części, dotyczącej bezpieczeństwa informacji, obejmie okres niemal od początku jej powstania do czasów współczesnych. Metoda ta pozwoli również na rozłożenie na poszczególne części rozwiązań kryptograficznych i badaniu każdego z nich osobno. Pozwoli także na ustalenie, które z rozwiązań są najbardziej efektywne i mogą zapewnić odpowiedni poziom bezpieczeństwa informacji. Natomiast druga zastosowana metoda badawcza to **synteza** polegająca na składaniu i zestawianiu oraz ujednolicaniu w całość najskuteczniejszych rozwiązań kryptograficznych, zapewniających odpowiedni poziom bezpieczeństwa informacji. Metoda ta pozwoli także na przedstawienie w końcowej części opracowania syntetycznych wniosków generalizujących.

Dotychczasowe analizy rozwoju kryptografii w początkowym okresie jej funkcjonowania wskazują, że zajmowała się ona ochroną informacji ogólnie. W szczególności ochrona ta podyktowana była potrzebami, jakie niósł ze sobą rozwój informacji równolegle wraz z rozwojem społeczeństwa. Rozwój ten obejmował obszar tzw. informacji niepisanych. Zaliczymy do nich:

- **ogień** – **ognisko** rozpalone na szczycie wzgórza było doskonałym sygnałem: widać je z dużej odległości, zwłaszcza w nocy;
- **ręce – machanie rękami** stanowiło sposób sygnalizacji, wymagana była jednak widoczność osoby przekazującej sygnały;
- **język gestów i język migowy** mogą być zaliczane do metod bezpiecznej komunikacji. Posiadają jednak ograniczenia, gdyż są słabo widoczne z dużej odległości;
- **wykorzystanie chorągiewek** - stosowane przez żołnierzy, żeglarzy przesyłający wiadomości za pomocą tej metody;
- **flagi** – od stuleci za ich pomocą przesyłano wiadomości między statkami;
- **dźwięk – rogi, kotły, bębny, gwizdki, dzwony**, wszystkie służyły i czasami nadal służą do przekazania wiadomości na odległość znacznie dalszą, niż pozwala ludzki głos.

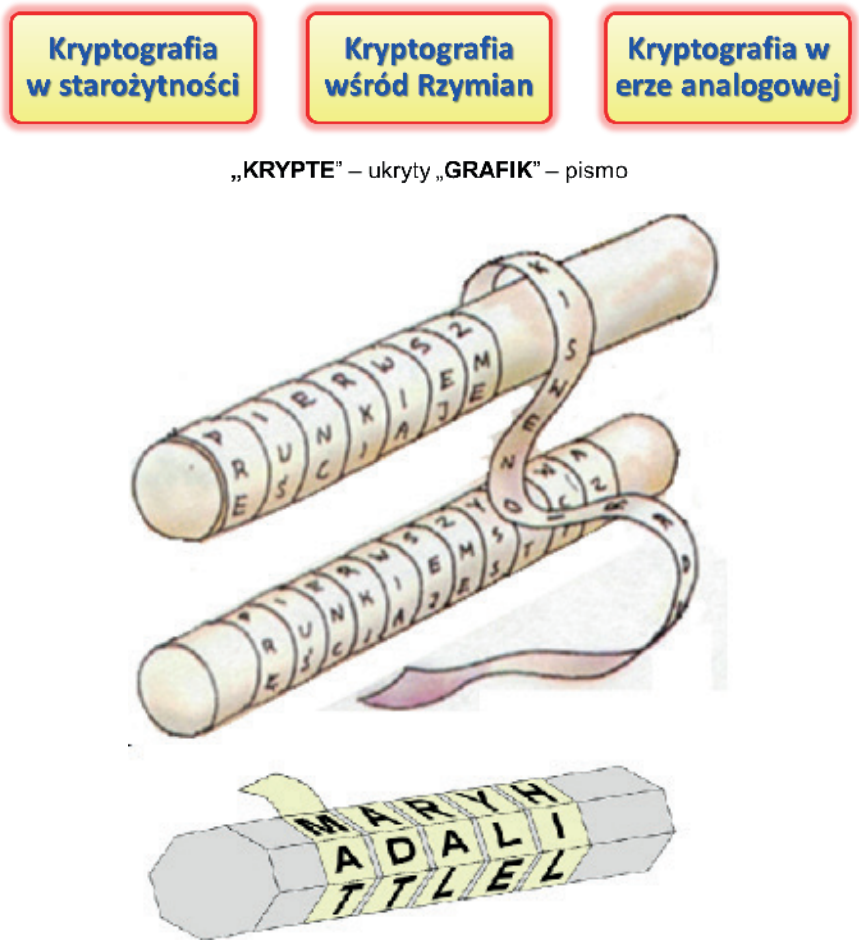
Rys. 26. Sposoby przekazywania informacji z wykorzystaniem: gołębi, ognia i listonosza

Rys. 27. Sygnały dźwiękowe i alfabet Morsa

Źródła: **dzwony kościelne** - https://www.ekai.pl/wp-content/uploads/2019/02/poland-393957_960_720.jpg, alfabet morsa - https://economic-historian.com/wp-content/ uploads/2021/03/20131011082040telegraph-470.jpg [dostęp: 05.06.2023].

W dzisiejszych czasach większość z tych rozwiązań ma już raczej tylko znaczenie historyczne. Gdy pojawiły się informacje, które ze względu na zawarte w nich tajemnice należało chronić, podejmowano różne próby zastosowania nowatorskich rozwiązań. Proste techniki kryptograficzne stosowane były w starożytności. Okazuje się, że większość cywilizacji w różnym stopniu wykorzystywało kryptografię w swoim codziennym życiu. Do najpopularniejszych należała podmiana symboli, a więc najbardziej podstawowa forma kryptografii, która pojawia się zarówno w antycznych pismach egipskich, jak i mezopotamskich[183]. Najstarszy znany przykład szyfrowania wiadomości znaleziono w grobowcu Egipcjanina, który żył około 3900 lat temu. W późniejszych okresach kryptografia zaczęła być coraz szerzej wykorzystywana do ochrony ważnych informacji wojskowych, dyplomatycznych i cywilnych (w tym handlowych, bankowych, gospodarczych), co ma miejsce do dzisiejszych czasów[184].

[183] Historia kryptografii - https://www.slideserve.com/stella/maszyny-szyfruj-ce [dostęp: 05.02.2023].
[184] Tamże.



Rys. 28. Kryptografia w starożytności, w okresie Rzymian i erze analogowej historia kryptografii - Skytale

Źródło: https://www.slideserve.com/stella/maszyny-szyfruj-ce [dostęp: 05.02.2023].

Pierwsze w historii urządzenie kodujące nie było maszyną, lecz zwykłym kijem (Skytale) i było stosowane przez Spartan w V wielu p.n.e. Osoba chcąca wysłać tajny meldunek (wiadomość) owijała walec (kij) o określonym rozmiarze parcianą taśmą spiralnie, unikając nakładania się na siebie zwojów, a następnie wystarczyło tylko odwinąć taśmę. Po rozwinięciu materiał pokrywały pozornie chaotyczne rozrzucone znaki. Taka forma zapisu sprawiała, że wiadomość była nieczytelna, dopóki nie została przymocowana do podobnego walca przez odbiorcę. Odbiorca wiadomości miał identyczny walec co nadawca, na który nawijał tajemniczy zwój. Wtedy litery znów układały się w logiczny przekaz.

Rys. 30. Znaki systemu migowego, alfabet grecki, znaki kanji.

Źródła: https://i.pinimg.com/originals/40/16/22/401622b5813bb403710fb797298949d2.jpg, https://www.bing.com/search?q=znakikanji&form=ANNTH1&refig=b5bce915ab1543e9849dda05933f5bd4 [dostęp: 05.01.2023].

Jednym z podstawowych podziałów kodów pisanych są alfabety. Mimo, że alfabet łaciński jest znany setkom milionów ludzi, dla jeszcze większej rzeszy stanowi zagadkę. Podobnie sprawa ma się z rosyjską grażdanką, japońskimi kanji czy starożytną greką. Kody pisane można przedstawić w różnej postaci, niezrozumiałej dla osoby postronnej, np. pisząc odbiciem lustrzanym lub zygzakiem. Kody pisane stanowią największą kategorię koncepcyjną zasad bezpiecznej komunikacji.

Obecnie wiemy również, że szpiedzy żyjący w starożytnych Indiach również korzystali z zakodowanych wiadomości już w II wieku p.n.e. Dla potwierdzenia jaką wagę w starożytności przywiązywano do ochrony informacji, analizie poddanych zostało kilka rozwiązań z tego okresu. Analizowane przykłady są potwierdzeniem, że kryptografia, tak jak nauka, liczy kilka tysięcy lat. Zapiski na temat stosowanych szyfrów znaleziono na pochodzących z Mezopotamii tabliczkach z pismem klinowym datowanych na 1500 rok p.n.e.

Analiza stosowanych rozwiązań kryptografii potwierdza, że ich rozwój był powolny i nierówny. Kryptografia w wielu kręgach kulturowych powstawała i funkcjonowała niezależnie, przybierając różne formy oraz stopnie zaawansowania. Jej rozwój przebiegał równolegle z rozwojem matematyki. W VIII i IX wieku naszej ery Arabowie wymyślili kryptoanalizę, czyli sztukę łamania kodów. W roku 1587 Maria, królowa Szkocji, używa tajnego kodu w spisku przeciwko Elżbiecie I – szyfr zostaje złamany, a Maria stracona. Dopiero pod koniec XVII wieku Antoine Rossignol wraz z synem wynaleźli na użytek króla Ludwika XIV Wielki Szyfr, który został złamany dopiero po 200 latach.

6.2. Maszyny i inne rozwiązania szyfrujące

Pierwsza maszyna szyfrująca została wynaleziona w XV wieku przez Leona Albertiego. Nie tylko pierwszy wpadł on na pomysł użycia kilku alfabetów szyfrowych, ale również doszedł do wniosku, że przydała by się maszyna, która ułatwi kodowanie i rozkodowywanie tekstów. Dysk szyfrowy Albertiego składał się z dwóch miedzianych kół o różnej średnicy, obracających się na wspólnej osi. Dysk uosabia pierwszy przykład podstawienia polialfabetycznego z mieszanymi alfabetami i zmiennym okresem. Na brzegu większego kółka rozmieszczone były litery alfabetu źródłowego, zaś na mniejszym – alfabetu tekstu szyfrowego zapisanych w dowolnej i niepowtarzającej się kolejności. To urządzenie, zwane Formula, składało się z dwóch koncentrycznych dysków połączonych **wspólnym kołkiem,** które mogły obracać się jeden względem drugiego[185].

W latach 90. XVIII wieku **Thomas Jefferson**[186] skonstruował maszynę zwaną **kołem szyfrowym.** Składała się ona z osadzonych na okrągłym metalowym pręcie 26 drewnianych dysków. Na obwodzie każdego dysku rozmieszczone były litery alfabetu, na każdym w innej kolejności. Szyfrowanie kołem polegało na ustawieniu tekstu jawnego poprzez obracanie dysków, a potem spisaniu tekstu zaszyfrowanego z dowolnie wybranego rzędu liter. Odbiorca, w celu odczytania wiadomości, musiał mieć identyczne koło szyfrowe. W jednym rzędzie należało ustawić litery szyfrówki, później szukać sensownie brzmiącej wiadomości[187].

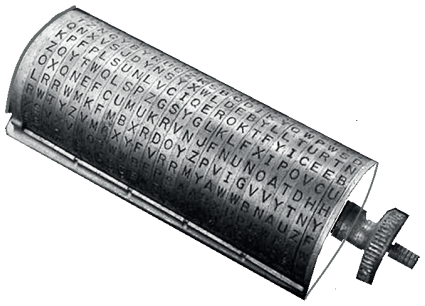
[185] Dysk szyfrowy Albertiego składał się z dwóch miedzianych kół - https://www.bing.com/search?q=Dysk+szyfrowy+Albertiego&form=ANSPH1&refig=b0ae363f56b44c5cba8af8adb30062bd&pc=U531 [dostęp: 10.02.2023].

[186] Thomas Jefferson - trzeci prezydent Stanów Zjednoczonych, był nie tylko politykiem, ale także naukowcem i wynalazcą. Jego działalność obejmuje wiele dziedzin, w tym **kryptografię**.

[187] http://pl.wikipedia.org/wiki/Strona_g%C5%82%C3%B3wna [dostęp:10.02.2023].

Rys. 31. Dysk szyfrowy Albertiego

Źródło:https://pl.abcdef.wiki/wiki/Alberti_cipher [dostęp: 05.06.2023].



Rys. 32. Koło szyfrowe Thomasa Jeffersona

Źródło: https://image2.slideserve.com/4562172/ko-o-szyfrowe-n.jpg [dostęp: 05.06.2023].

W XVIII wieku Wiedeń staje się centrum łamaczy kodów zgromadzonych w tzw. Czarnej Komnacie. Także Napoleon Bonaparte w 1812 roku doświadczył nie tylko srogiej rosyjskiej zimy, ale i skutecznych działań rosyjskich kodołamaczy, co niewątpliwie przyczyniło się do klęski jego wojsk.

Kiedy w 1844 roku pojawia się telegraf elektryczny, który umożliwił błyskawiczne przekazywanie wiadomości alfabetem Morse'a, szybkość przekazywania informacji znacznie przyspiesza. Kolejne wynalazki przypadają na okres 1914-1918 rok, kiedy zastosowanie radia ułatwia przekazywanie depesz, ale także ich przechwytywanie. To wtedy drastycznie wzrasta wartość każdego skutecznego systemu kodowania.

Źródłowy	a	b	c	D	e	f	G	h	i	j	k	l	m	n	o	P	Q	r	s	t	u	v	W	x	y	z
Wynikowy	z	y	x	W	v	u	T	s	r	Q	p	o	n	m	l	K	J	i	h	g	f	e	D	c	b	a

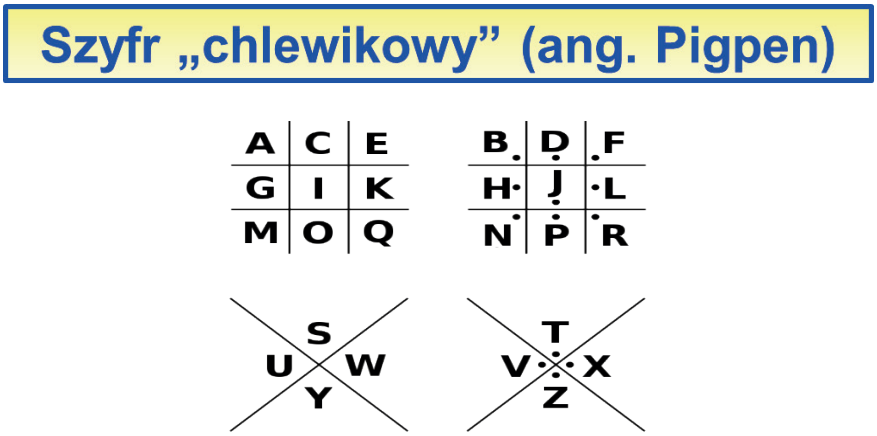
Rys. 33. Szyfr substytucyjny

Źródło: opracowanie własne.

W tej części opracowania analizie zostaną poddane sposoby przemiany tekstu jawnego na postać niezrozumiałą. Jednym z takich sposobów był **szyfr substytucyjny**, który polega na zastąpieniu każdego znaku **alfabetu źródłowego** wcześniej ustalonym innym znakiem **alfabetu wynikowego**.

Rozwiązanie było używane od stuleci osobno lub jednocześnie. Teoretycznie rzecz biorąc litery alfabetu można zastępować dowolnymi znakami. Problem polega na tym, że przeciętnemu użytkownikowi trudno byłoby taki szyfr zapamiętać, dlatego występuje tutaj konieczność noszenia przy sobie takiego szyfru, a to nie zapewnia bezpieczeństwa. Lepszym rozwiązaniem jest szyfr stworzony według zasad, które łatwo zapamiętać.

Szyfr monoalfabetyczny podstawieniowy – zamiast każdej z liter alfabetu jawnego podstawia się literę, która leży w takiej samej odległości od końca alfabetu, co dana litera od początku. W praktyce polega to na odwróceniu alfabetu. Szyfr ten jest przez to bardzo łatwy do zapamiętania. Szyfr tworzy się poprzez wpisanie liter alfabetu w takie oto kratki (lub podobne o tej samej koncepcji). Znakiem szyfrowym jest obraz tego fragmentu siatki, w który została wpisana litera.



Rys. 34. Szyfr chlewikowy

Źródło: https://www.szkolneblogi.pl/static/media/users/private/JASIENICA/szyfr-czekolada_sko_thumb.jpg [dostęp: 05.02.2023].

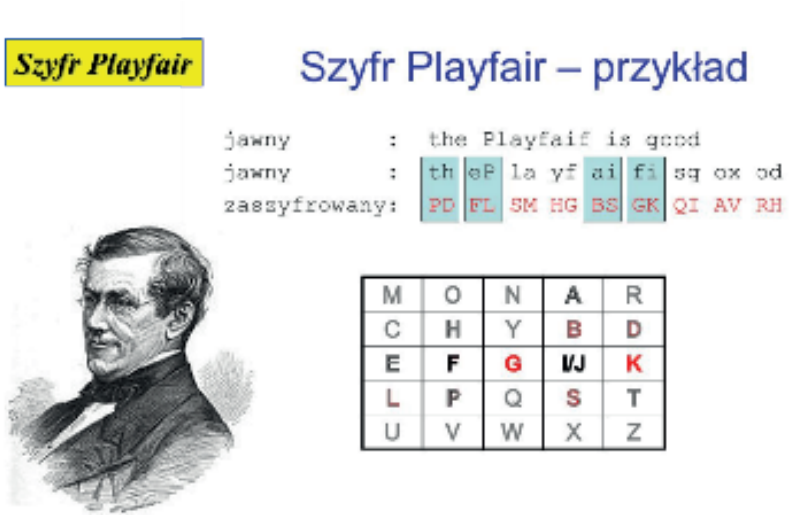
Wpisujemy litery alfabetu łacińskiego w kwadratową tablicę wymiaru 5×5. Tak skonstruowaną tablicę nazywamy **tablicą Polibiusza**. Każdą literę tekstu jawnego zastępujemy parą liczb, z których pierwsza jest numerem wiersza, a druga numerem kolumny zawierających daną literę.

Rys. 35. Tablica Polibiusza

Źródło: https://pl.wikipedia.org/wiki/Szachownica_Polibiusza [dostęp: 12.02.2023].

Najbardziej znanym szyfrem wieloliterowym jest **Playfair**, w którym dwuznaki tekstu jawnego są traktowane jako osobne jednostki i są tłumaczone na dwuznaki zaszyfrowane.

Algorytm Playfair zbudowany jest na matrycy liter o rozmiarze 5x5, zbudowanej przy użyciu słowa kluczowego. Matrycę buduje się wpisując litery słowa kluczowego (bez powtarzających się) od lewej do prawej i z góry do dołu, a następnie wypełnia się resztę matrycy pozostałymi literami w porządku alfabetycznym. Litery I i J liczą się jako jedna litera.



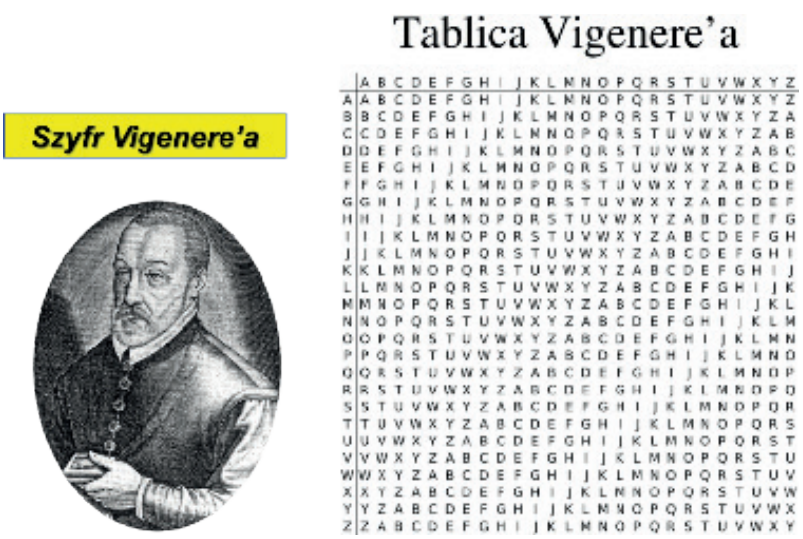
Rys. 36. Szyfry wieloliterowe

Źródło: https://pl.wikipedia.org/wiki/Szyfr_Playfai [dostęp: 12.02.2023].

Jednym ze sposobów polepszenia szyfrowania jednoalfabetowego jest zastosowanie różnych podstawień jednoalfabetowych podczas szyfrowania jednej wiadomości. Wszystkie techniki tego rodzaju mają dwie wspólne cechy:

- stosuje się zestaw powiązanych reguł podstawienia jednoalfabetowego;
- klucz określa, która reguła zostanie użyta dla danego przekształcenia.

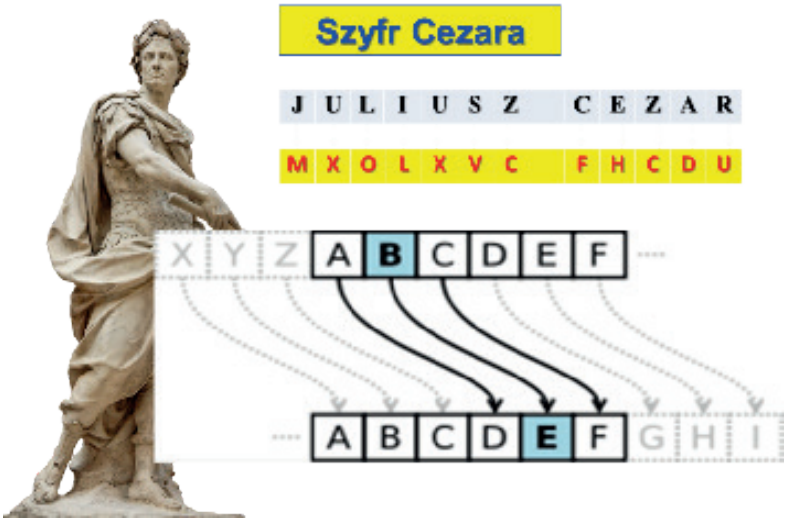
Najprostszym i najbardziej znanym jest szyfr Vigenere'a. Do pomocy w korzystaniu z tej metody buduje się tablicę. Każdy z 26 szyfrów jest umieszczony poziomo, litery kluczowe im odpowiadające znajdują się po lewej stronie, natomiast alfabet tekstu jawnego znajduję się na górze tablicy. Technika podstawiania polega na zamianie liter tekstu jawnego innymi literami lub jakimiś symbolami.



Rys. 37. Szyfrowanie wieloalfabetowe

Źródło:https://www.bing.com/images/search?q=Szyfr+Vigen%c3%a8re%e2%80%99A&form=RESTAB&first=1 [dostęp: 10.02.2023].

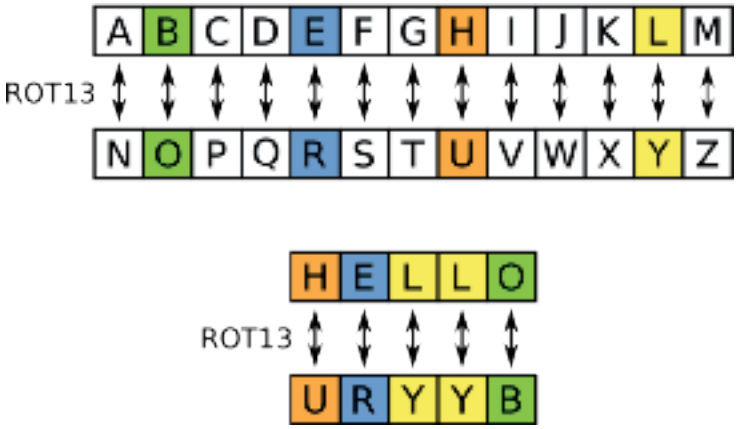
Pierwszym historycznie potwierdzonym użyciem właściwych metod kryptograficznych była wymiana zaszyfrowanej korespondencji między Cezarem i Cyceronem w I wieku p.n.e. Stosowany przez nich szyfr polegał na zastępowaniu każdej litery inną, według z góry ustalonego klucza.



Rys. 38. Szyfr Cezara

Źródło: https://pl.wikipedia.org/wiki/Szyfr_Cezara [dostęp: 12.02.2023].

W szyfrze zwanym dziś szyfrem Cezara, każdą literę alfabetu łacińskiego zastępowano o trzy dalsze. Zasada działania szyfru ROT13 jest identyczna jak w przypadku szyfru Cezara – różnica polega na wartości przesunięcia. W tym przypadku każdą literę tekstu jawnego zamieniamy na literę, znak przesunięty o 13 miejsc w prawo podczas szyfrowania. W celu odszyfrowania tekst powtarzamy operację tym razem przesuwając litery, znaki o 13 pozycje w lewo.



Rys. 39. Szyfr ROT 13

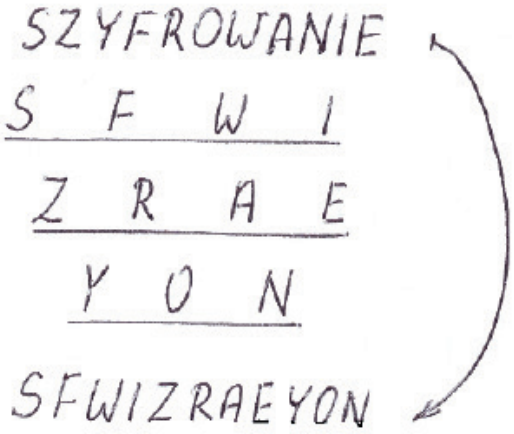
Źródło: https://www.lo69.pl/liceum/strony/obraz/album/rot13.png [dostęp: 10.02.2023].

Nie wszystkie kody polegają na zastępowaniu liter innymi znakami. Szyfrowanie transpozycyjne nie zmienia liter, lecz porządek, w jakim zostaną zapisane. Najprostszym sposobem na szyfrowanie transpozycyjne jest pisanie wiadomości od końca do początku. Kolejnym sposobem jest pisanie zygzakiem, co przedstawia tabela, a następnie przepisanie kolejno górnego i dolnego rzędu, co daje wiadomość.

Rys. 40. Przykłady szyfrów transpozycyjnych

Źródło: Opracowanie własne [dostęp: 12.02.2023].

Szyfr sztachetowy polega na spisaniu wiadomości w kilku rzędach, a następnie spisaniu kolumn. Szyframi takimi nazywamy wszystkie przekształcenia, które opierają się na permutacji liter tekstu jawnego. Najprostszym takim szyfrem jest tak zwana technika płotu, która polega na tym, że tekst jawny zapisuje się w postaci ciągu kolumn, a następnie odczytuje się jako ciąg wiersza. Oczywiście rozszyfrowanie takiego komunikatu byłoby bardzo proste, dlatego można zastosować bardziej skomplikowany system, polegający na zapisaniu wiadomości w prostokącie, a następnie odczytaniu kolumna po kolumnie, lecz ze zmianą ich kolejności.

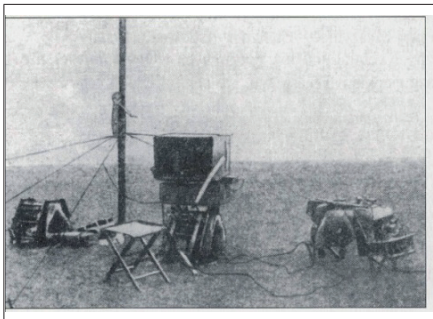


Rys. 41. Techniki transpozycyjne

Źródło: Opracowanie własne.

6.3. Wpływ kryptografii na losy konfliktów zbrojnych

Szczególne działania matematyków mają miejsce w czasie I i II wojny światowej i przyczyniają się do kojarzenia ich z kryptologią. To wybitni kryptolodzy w okresie 1939-1945 roku, łamiąc kody niemieckiej maszyny szyfrującej Enigmy, pomogli aliantom nie tylko wygrać II wojnę światową, ale znacząco przyspieszyć jej zakończenie. Jak widać w przekroju historycznym, tajne kody wywierały znaczący wpływ na losy świata. Osiągnięcia te pozostawały tajemnicą i zostały ujawniane dopiero po latach.



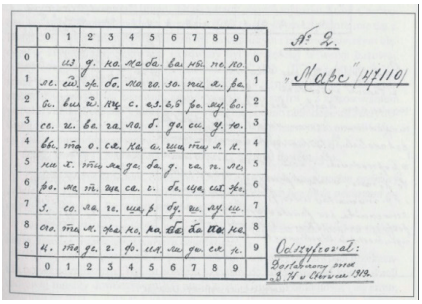
Rys. 42. Rosyjska radiostacja polowa

Źródło: rosyjska radiostacja polowa - Bing images [dostęp: 12.02.2023].

Rys. 43. Polska stacja nasłuchowa

Źródło: https://bi.im-g.pl/im/da/fd/18/z26 202842 AMP,Przewozna-radiostacja-Marconi-YB1--podstawowe-wypo.jpg [dostęp: 12.06.2023].

Rys. 44. mjr Jan Kowalewski Naczelnik Radiowywiadu Biura Szyfrów188



Rys. 45. Uzyskany szyfrogram

Po ujawnieniu skrywanych przez dziesięciolecia tajemnic funkcjonowania Polskiego Biura Szyfrów i jego niezwykłych sukcesów odniesionych podczas wojny z bolszewicką Rosją dowiadujemy się, że w tym czasie systematyczne łamanie kluczy szyfrowych nieprzyjaciela umożliwiło odczytanie kilku tysięcy bolszewickich szyfrogramów i miało wielki wpływ na zwycięstwo odniesione w tej wojnie. W tym okresie było to możliwe dzięki porucznikowi Janowi Kowalewskiemu i profesorowi Stefanowi Mazurkiewiczowi – prorektorowi Uniwersytetu Warszawskiego, który zajmował się logiką i topologią, profesorowi Wacławowi Sierpińskiemu specjaliście od teorii liczb oraz profesorowi Stanisławowi Leśniewskiemu z Uniwersytetu Warszawskiego zajmującemu się logiką.

Dużym sukcesem Polaków w ramach prowadzonej wojny w eterze było złamanie bolszewickiego szyfru Diwizija oraz rozszyfrowanie około 500 sowieckich depesz radiowych. Ponadto przez dwa dni po przejęciu rosyjskiej radiostacji Polacy nadawali tekst Biblii, a rosyjscy telegrafiści zamiast rozkazów ze zdziwieniem go słuchali. To polscy kryptolodzy sprawili, że Marszałek Józef Piłsudski miał tak dokładne informacje, jakich do jego czasów nie miał żaden dowódca.

188 Jan Kowalewski – ur. 1892 w Łodzi, zm. w 1965 roku w Londynie. Wojskowy, matematyk, lingwista i kryptolog, oficer wywiadu Polskiej Organizacji Wojskowej, szef wywiadu w 4. Dywizji Żeligowskiego. W Polsce w latach 1919-1924 naczelnik Wydziału II Radiowywiadu Biura Szyfrów przy Sztabie Generalnym. Skuteczność zorganizowanego przez Jana Kowalewskiego wywiadu była jednym z kluczowych elementów zwycięstwa Polski w Bitwie Warszawskiej i całej wojnie polsko-bolszewickiej.

Do bardzo ciekawych rozwiązań kryptograficznych należy historia Enigmy. Sięga ona 1919 roku, kiedy holenderski wynalazca Hugo Koch skonstruował i opatentował maszynę szyfrującą, której patent kilka lat później odkupił Artur Scherbrus, niemiecki inżynier, z przeznaczeniem dla potrzeb przemysłu. Maszyna miała strzec tajemnic wielkich koncernów, firm handlowych i przedstawicieli finansjery[189].

David Kahn, specjalista od historii kryptografii, autor książki Łamacze kodów twierdzi, że dobrzy specjaliści pochodzą z krajów wielojęzycznych i wielokulturowych. Istotną rolę odgrywają uniwersytety, z matematyką na wysokim poziomie, oraz muzyka, króamusi być komponowana.

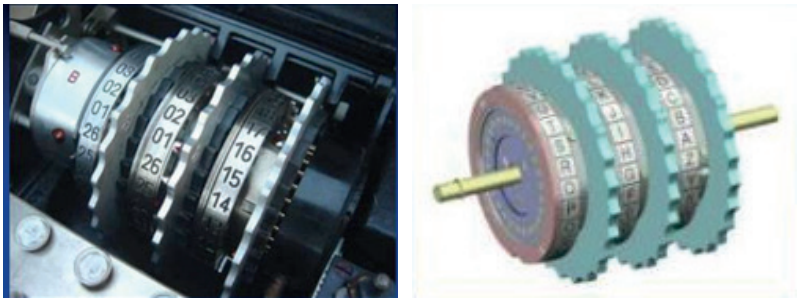
Rys. 46. Niemiecka maszyna szyfrująca Enigma

Źródło: https://www.bing.com/images/search?q=enigma&qpvt=Enigma&form= IQFRML&first=1 [dostęp: 10.02.2023].

Niemiecka marynarka wojenna zaczęła stosować Enigmę (z greckiego – tajemnicę, zagadkę) już w roku 1926. Kilka lat później stała się niemiecką maszyną szyfrującą, używaną przez wywiad oraz armię niemiecką, a także w innej wersji przez prywatnych przedsiębiorców. Z przodu maszyny znajduje się 26-literowa klawiatura, a za nią płytka z drugim zestawem znaków podświetlanych żarówkami, które podświetlają umieszczone wyżej okienka z literami alfabetu uszeregowanymi tak jak w klawiaturze. Mieszacz to zasadnicza tajemnica Enigmy. Są to trzy ruchome bębenki szyfrujące, umieszczone na wspólnej osi, mogące się

[189] https://www.slideserve.com/stella/maszyny-szyfruj-ce [dostęp: 10.02.2023].

obracać niezależnie względem siebie. Z jednej strony każdego z bębenków znajduje się 26 równomiernie rozmieszczonych styków sprężynujących, a z drugiej 26 styków stałych. Wewnątrz bębenka jest wirnik. Każdy z bębenków szyfrujących posiada pierścień z wyrytymi na obwodzie literami alfabetu.



Rys. 47. Bębny maszyny szyfrującej Enigmy (z literami lub cyframi)
Źródło: https://www.slideserve.com/stella/maszyny-szyfruj-ce [dostęp: 10.02.2023].

Na rysunku przedstawiono trzy bębny szyfrujące umieszczone wewnątrz maszyny szyfrującej Enigmy. W czasie pracy prąd przepływał od strony prawej do lewej, dlatego bęben odwracający znajduje się na końcu po lewej stronie, a bęben wejściowy jest bębnem po prawej stronie[190]. Enigma nie tylko dawała ponad 17 000 możliwości kodowania jednego znaku (10 stron maszynopisu), możliwe było również przestawienie rotorów, co jeszcze zwiększało ilość kombinacji.

Dla sprawnego funkcjonowania Enigmy niezbędna jest łącznica, która znajduje się z przodu maszyny i jest podobna do ręcznej łącznicy telefonicznej. Posiada 26 par gniazdek, które mogą być połączone ze sobą dwużyłowymi przewodami zakończonymi z obu stron wtyczkami. Poszczególne pary gniazdek odpowiadają literom alfabetu. Połączenie przewodem gniazdka jednej pary z gniazdkiem innej z nich powoduje, że górne gniazdka pierwszej pary zostają połączone z dolnymi drugiej i na odwrót. Tym sposobem łącznica umożliwia zamianę parami określonej liczby liter alfabetu. Bateria – obwód elektryczny zasila bateria umieszczona z prawej strony bębenków szyfrujących. Napięcie może być również doprowadzone za pomocą transformatora z sieci. Naciśnięcie klawisza powoduje ruch obrotowy bębenków szyfrujących. Karbowany pierścień umożliwia obrót bębna o jedną literkę, gdy sąsiedni bęben wykona pełny obrót.

[190] https://www.slideserve.com/stella/maszyny-szyfruj-ce [dostęp: 10.02.2023].

W trakcie pracy prąd przepływa od strony prawej do lewej, zatem bęben odwracający znajduje się na końcu po lewej stronie, a bęben wejściowy jest pierwszym bębnem po stronie prawej (bęben w ciemnym kolorze).

Mechanizm obrotowy działa w następujący sposób: po naciśnięciu klawisza prawy bębenek szyfrujący obraca się o 1/26 kąta pełnego, natomiast bębenki lewy i środkowy pozostają nieruchome do momentu, kiedy bębenek prawy osiągnie pewną wyróżnioną pozycję. Wówczas bębenek środkowy obraca się o jedną pozycję. Gdy z kolei bębenek środkowy osiągnie pozycję obrotową, wówczas bębenki lewy i środkowy obracają się o 1/26 kąta pełnego. W ten sposób każda następna litera jest szyfrowana przy innych położeniach bębenków co sprawia, że naciskając kilka razy z rzędu ten sam klawisz uzyskuje się zapalanie coraz to innych lampek. Tak w bardzo wielkim skrócie można opisać konstrukcję Enigmy typu wojskowego[191].

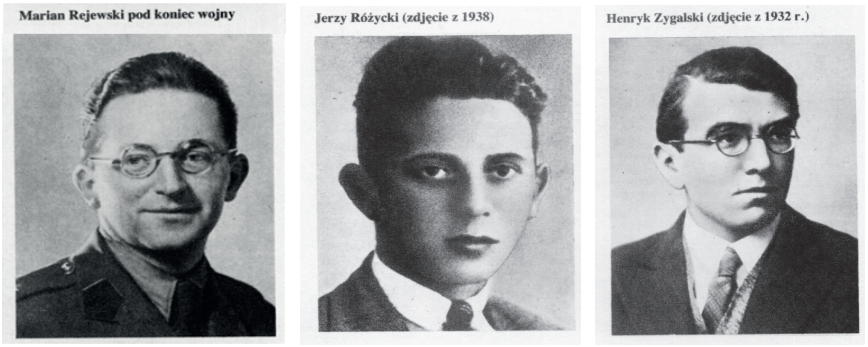
Marian Rejewski[192], jeden z polskich matematyków, który złamał szyfr Enigmy, tak zobrazował liczbę: „jest ona większa od liczby sekund, jakie upłynęły od początku świata, jeśli przyjąć, że świat istnieje od pięciu miliardów lat". Dzięki temu uważana była za najdoskonalszą maszynę szyfrującą na świecie. Oprócz Mariana Rejewskiego do załamania szyfru Enigmy przysłużyli się także **Jerzy Różycki**[193] i **Henryk Zygalski**[194].

[191] http://pl.wikipedia.org/wiki/Strona_g%C5%82%C3%B3wna [dostęp: 22.02.2023].

[192] **Marian Rejewski** – ur. 1905 w Bydgoszczy – zm. 1980 w Warszawie. Polski matematyk i kryptolog, pracownik Uniwersytetu Poznańskiego oraz wywiadu wojskowego. Kierował pracą zespołu pod kryptonimem Wicher polskich kryptologów pracujących nad Enigmą.

[193] **Jerzy Różycki** – ur. 1909 w Olsztynie – zm. 1942 Balcarów. Polski matematyk i kryptolog, pracownik Uniwersytetu Poznańskiego oraz kontrwywiadu wojskowego Oddziału II Sztabu Generalnego. W styczniu 1933 pomógł złamać kod niemieckiej maszyny szyfrującej Enigmy. Wkład Różyckiego polega na tzw. Metodzie zegara, pozwalającej określić wybór i ustawienie wirnika w maszynie Enigma.

[194] **Henryk Zygalski** – ur. 1908 w Poznaniu – zm. 1978 w Londynie. Polski matematyk i kryptolog, pracownik Uniwersytetu Poznańskiego oraz kontrwywiadu wojskowego. Wynalazca koncepcji tzw. płacht Zygalskiego, bardzo pracochłonnych w wykonaniu perforowanych arkuszy, pomagających w ustaleniu kolejności wirników kodujących Enigmy.

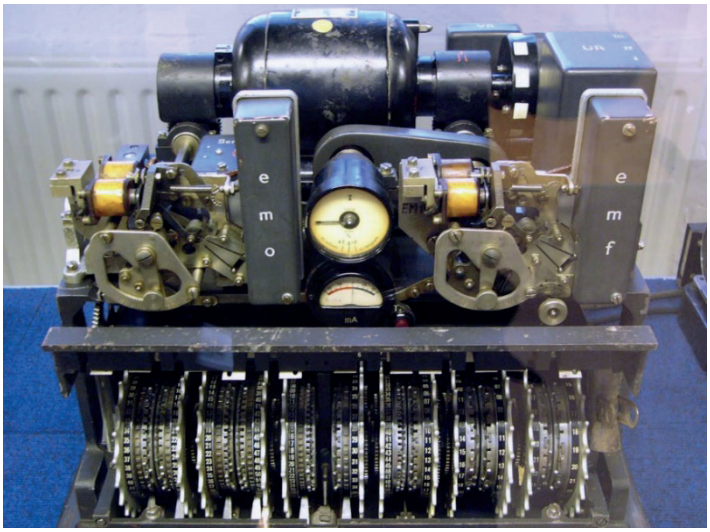


Rys. 48. Polscy naukowcy, którzy wnieśli wkład w rozszyfrowanie Enigmy. Źródło: http://pl.wikipedia.org/wiki/Strona_g%C5%82%C3%B3wna [dostęp: 10.02.2023].

Enigma systematycznie ulepszana o kombinacje rotorów miała stać się niezwyciężonym narzędziem Niemców do bezpiecznego przekazywania informacji (szyfrowania meldunków). Możliwe, że tak by się stało, gdyby nie praca polskich badaczy.

Rys. 49. Dar Polaków dla wywiadu brytyjskiego, skonstruowana kopia maszyny szyfrującej Enigmy. Źródło: https://pl.wikipedia.org/wiki/Enigma [dostęp: 12.02.2023].

„Gdyby nie dar Polaków, wywiad brytyjski prawdopodobnie nadal uważałby problem Enigmy za niemożliwy do rozwiązania" – przyznał Gordon Welchman, brytyjski matematyk. Podczas II wojny światowej pracował w brytyjskim tajnym centrum dekryptażu w Bletchley Park, gdzie był jednym z najważniejszych współpracowników.



Rys. 50. Maszyna Lorenza

Źródło: https://www.slideserve.com/stella/maszyny-szyfruj-ce [dostęp: 10.02.2023].

Analizując okres II wojny światowej należy przedstawić także maszynę Lorenza, która była niemieckim rozwiązaniem szyfrującym używanym w tym okresie do przekazu informacji przez dalekopisy. jO ile Enigma używana była przez jednostki liniowe, o tyle maszyna Lorenza służyła do komunikacji na wysokim szczeblu, gdzie można było ją wykorzystać z dalekopisem przez dedykowane łącza. Maszyna ta wykorzystywała szyfr strumieniowy (rodzaj szyfru symetrycznego). Do łamania szyfru maszyny Lorenza Brytyjczycy zbudowali wiele maszyn, a informacje na ich temat odtajniono dopiero w roku 1975.

Przed pojawieniem się komputerów kryptografia opierała się na wykorzystaniu szyfrów. **Szyfr to odwzorowanie tekstu czytelnego na „bełkot" i z powrotem**. Na przykład, prosty szyfr polegałby na przesunięciu o cztery pozycje każdej litery w tekście (więc A staje się E). **Odkodowanie polega na odjęciu czterech pozycji od każdej litery. Procesy te nazywane są szyfrowaniem i deszyfrowaniem**.

Przesunięcie o cztery miejsca w alfabecie jest bardzo oczywiste i nie jest bezpieczne. Bezpieczniejsze jest tworzenie złożonych odwzorowań, które wymagają klucza do translacji. Taki klucz musi być rozprowadzony wśród wszystkich uczestniczących stron. Konieczność ta pociąga za sobą wszelkiego rodzaju słabości logistyczne. Słynnym przykładem szyfru symetrycznego jest maszyna Enigma używana w czasie II wojny światowej.

Obecnie kryptografia, ze względu na ciągłe doskonalenie systemów komputerowych, będzie się dalej rozwijać. Stałe zwiększanie mocy obliczeniowej komputerów wymusza potrzebę udoskonalania już istniejących sposobów ochrony informacji. Wraz z rozwojem komputerów, kryptografia stała się znacznie bardziej zaawansowana niż w erze analogowej. 128-bitowe matematyczne szyfrowanie, które jest o wiele silniejsze niż jakikolwiek pradawny lub średniowieczny szyfr, jest obecnie standardem dla wielu urządzeń i systemów komputerowych.

6.4. Kryptologia, kryptografia i kryptoanaliza

Analizując obecnie wpływ nowych technologii informacyjnych na bezpieczeństwo państwa dochodzimy do przekonania, że wśród tych rozwiązań czołowe miejsce zajmuje kryptografia. Rozwiązania te wykorzystują w praktyce wiedzę kryptograficzną w celu ochrony informacji podczas ich pozyskiwania, gromadzenia, przetwarzania, kopiowania i przesyłania. Poddane analizie dotychczas zaprezentowane rozwiązania zapewniające bezpieczeństwo informacji mają ogromne znaczenie i pozwalają na podjęcie próby ich zdefiniowania oraz usystematyzowania.

Kryptologia (z gr. κρυπτός – *kryptos* – ukryty i λόγος – *logos* – słowo) jest nauką o szyfrowaniu, czyli bezpiecznych sposobach przekazywania informacji. Współcześnie kryptologia jest uznawana za gałąź zarówno matematyki, jak informatyki; ponadto jest blisko związana z teorią informacji, inżynierią oraz bezpieczeństwem komputerowym i sieciowym.

Kryptografia (*cryptography*, z języka greckiego *krypto* – ukryty, tajny, *graph* – pismo słowo). Pierwotnie oznaczała tajne pismo. Zajmuje się utajnionym zapisem informacji, czyli szyfrowaniem (*encryption* – kodowaniem), przekształceniem tekstu z postaci jawnej na niezrozumiałą (tekst zaszyfrowany, tajny)[195].

[195] https://pl.wikipedia.org/wiki/Kryptologia#Historia_kryptografii_i_kryptoanalizy [dostęp: 01.02.2023].

Rys. 51. Podział kryptologii

Źródło: opracowanie własne.

Kryptoanaliza to dziedzina kryptologii zajmująca się łamaniem szyfrów, czyli odczytywaniem zaszyfrowanych danych bez posiadania kluczy rozszyfrowujących[196]. Łamiąc szyfr kryptoanalityk zazwyczaj zna algorytm kryptograficzny. Nawet jeżeli algorytm ten jest tajny, to jego odtworzenie jest jedynie kwestią czasu. Teoretycznie wszystkie szyfry można złamać, jednak w praktyce zależy to głównie od czasu i mocy obliczeniowej użytej do złamania, więc zazwyczaj uznaje się szyfry za bezpieczne, jeśli nie da się ich złamać w stosunkowo długim czasie. Do zasadniczych różnic charakteryzujących kryptografię oraz kryptoanalizę możemy zaliczyć fakt, że pierwsza zajmuje się utajnianiem danych, natomiast druga łamaniem szyfrów. Kryptografia zabezpiecza przesyłane wiadomości przed niepożądanym dostępem. Dzięki niej informacje (np. wiadomości) są trudne do rozszyfrowania przez osobę, czyli podmiot, który nie zna klucza rozszyfrowującego. Jedyna informacja, jaką podmiot ten otrzyma, to trudno zrozumiały ciąg znaków. Możemy wyróżnić trzy rodzaje przełamywania szyfrów:

- **w pierwszym** występuje atak bez tekstu jawnego, gdzie kryptoanalityk musi określić klucz znając tekst zaszyfrowany. W tym przypadku mogą być też znane: metoda szyfrowania, język tekstu jawnego, a także tematyka badanego tekstu oraz słowa charakterystyczne dla tej tematyki, z określonym prawdopodobieństwem wystąpienia;
- **w drugim** przypadku mamy do czynienia z atakami z tekstem jawnym, gdzie kryptoanalityk zna pary tekstów zarówno jawnego, jak i zaszyfrowanego;

[196] https://wazniak.mimuw.edu.pl/images/0/0f/Bsi_04_wykl.pdf [dostęp: 12.02.2023].

- **w trzecim** występuje atak z wybranym tekstem jawnym, gdzie kryptoanalityk może zdobyć tekst zaszyfrowany odpowiadający wybranemu fragmentowi zaszyfrowanego tekstu.

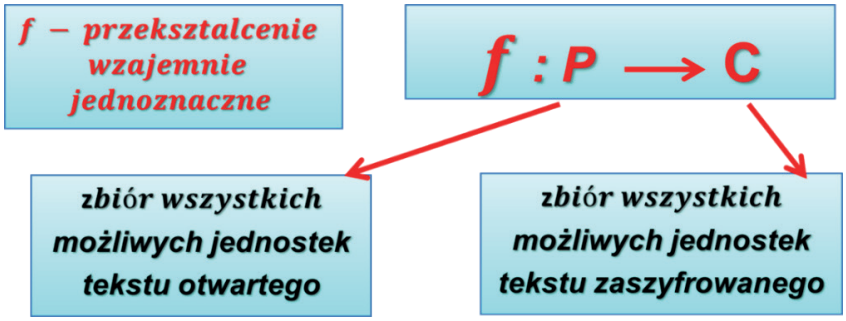
Łamanie szyfru to określenie dotyczące uzyskania dostępu do jawnego tekstu zaszyfrowanych danych środkami innymi niż normalny proces deszyfrowania, stosowany przez zamierzonych odbiorców tych danych. Aby złamać szyfr, trzeba zdobyć klucz deszyfracji za pośrednictwem specjalnej usługi odtwarzania klucza lub znaleźć klucz, posługując się kryptoanalizą[197]. Bardzo ważnym elementem jest pewność dostępu do informacji w razie zgubienia, uszkodzenia, lub zniszczenia klucza szyfrującego. Utrata wartościowych informacji może mieć podobne konsekwencje jak przekazanie ich nieupoważnionym osobom. Szpiegowanie swoich wrogów, czy też konkurentów, stwarza możliwość deszyfracji danych, przechwyconych podczas operacji wywiadowczych, w celu ochrony interesów kraju, a także wspomagania operacji wojskowych. Wiele przestępstw związanych z nieuprawnionym dostępem do danych ma zasięg międzynarodowy, co niejednokrotnie utrudnia wykrywalność tego rodzaju przestępczości. Mogą one wyrządzić szkodę zarówno pojedynczym firmom, jak i stabilności ekonomicznej państw.

Steganografia – dział kryptografii jest nauką o komunikacji określającą w jaki sposób postępować, by obecność komunikatu nie mogła zostać wykryta. Jej nazwa wywodzi się od greckich słów steganos (ukryty) oraz graphen (pisać). Nauka ta znajduje zastosowanie wszędzie tam, gdzie istnieje potrzeba sekretnej komunikacji, jednak jej metody różnią się od metod kryptograficznych. W odróżnieniu od kryptografii (gdzie obecność komunikatu nie jest negowana, natomiast jego treść jest niejawna) steganografia próbuje ukryć fakt prowadzenia komunikacji. Jest to zatem zespół metod ukrywania tajnych przekazów w wiadomościach, które nie są tajne, aby nie zostały one odczytane przez osoby do tego niepowołane. Można podać wiele historycznych przykładów użycia technik steganograficznych. Najbardziej popularną jest użycie atramentu sympatycznego. Atrament sympatyczny to bezbarwny i bezwonny płyn, który w odpowiednich warunkach (np. po podgrzaniu) zaczyna być widoczny[198].

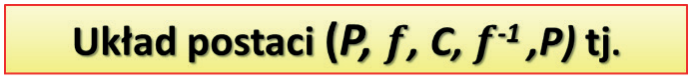
[197] Tamże.
[198] https://pl.wikipedia.org/wiki/Steganografiaeganografia [dostęp: 12.02.2023].

System kryptograficzny – tekst jawny i kryptonim, podzielone są na jednostki tekstu. Jednostką tekstu może być pojedyncza litera (diagram), trójka liter (trigram) czy nawet blok 50 liter. Przekształcenie szyfrujące jest to funkcja, która każdej jednostce tekstu otwartego przyporządkowuje jednostkę tekstu zaszyfrowanego.

Przekształcenie szyfrujące jest to funkcja, która każdej jednostce tekstu otwartego przyporządkowuje jednostkę tekstu zaszyfrowanego.



Szyfr – metoda utajnionego zapisywania w taki sposób, by tekst jawny (*plaintext*), otwarty (*cleartext*) był przekształcany w tekst zaszyfrowany, kryptogram, szyfrogram (*ciphertext*). Nie ulega wątpliwości, że jedną z najskuteczniejszych technologii zapewniającą bezpieczeństwo współczesnym systemom i sieciowym komputerom jest szyfrowanie. Stosowane jest zarówno w odniesieniu do pojedynczych dokumentów, jak i ciągłych transmisji sieciowych. Stosowane jest również do uwierzytelniania, w tym integralności dokumentów, jak i potwierdzenia tożsamości osób.



Deszyfrowanie (*decryption*) – proces odwrotny do szyfrowania, umożliwia przekształcenie tekstu zaszyfrowanego do postaci jawnej. **Szyfrowanie i deszyfrowanie** w nowoczesnej kryptografii są sterowane przez klucz lub klucze

kryptograficzne. Czasem deszyfrowanie nie jest potrzebne, tzw. szyfrowanie jednokierunkowe, np. przy hasłach dostępu.

Do podstawowych zadań kryptografii należy zapewnienie informacji **poufności, uwierzytelnienia, integralności i niezaprzeczalności:**

- **poufność** zapewnia tylko i wyłącznie uprawnionym do tego jednostkom na korzystanie i oglądanie danych w czytelnej formie;
- **uwierzytelnianie** jest to proces potwierdzający podaną tożsamość użytkownika, urządzenia końcowego, bądź jednego i drugiego. Może to być klient, serwer, zwrotnica, router, ściana ogniowa;
- **integralność** zapewnia, że dane nie zostały w żaden sposób zmienione lub zniszczone przez osoby niepowołane;
- **niezaprzeczalność** tworzenie zaszyfrowanych dowodów przesłania wiadomości, uniemożliwiających nadawcy wyparcie się autorstwa[199].

Do podstawowych zastosowań metod kryptograficznych należy zaliczyć:

- ochronę przed nieautoryzowanym ujawnieniem informacji przechowywanej na serwerze czy komputerze;
- ochronę informacji przesyłanej między komputerami;
- potwierdzanie tożsamości użytkownika;
- potwierdzanie tożsamości programu żądającego obsługi;
- uniemożliwianie nieautoryzowanej modyfikacji danych[200].

Istotą kryptografii jest zamiana tekstu jawnego na zaszyfrowany. Kryptografia jest to dziedzina zajmująca się praktycznym zastosowaniem wiedzy matematycznej w celu ochrony danych, podczas przesyłu informacji, w której występują dane. Współcześnie ma ona ogromne znaczenie w ochronie informacji. Powszechnie też wykorzystuje się kryptografię w bankowości internetowej, gdzie wszystkie transakcje odbywają się w tak zwanym bezpiecznym połączeniu, a dodatkowo każda operacja jest zatwierdzana przy użyciu klucza prywatnego. Które z metod zostaną zastosowane, zależy od konkretnego w tym przypadku banku czy instytucji, dokonujących wyboru sposobu szyfrowania lub uwierzytelnienia.

[199] https://www.soczko.pl/iod-soczko-partnerzy/blog-ochrona-danych/integralnosc-poufnosc/ [dostęp: 12.02.2023].

[200] https://pl.wikipedia.org/wiki/Kryptologia [dostęp: 12.02.2023].

6.5. Przykłady praktycznych zastosowań – kryptografia symetryczna i asymetryczna

Można wyróżnić dwa nurty kryptografii, które stosuje się obecnie. Jest to kryptografia symetryczna oraz asymetryczna:

- pierwszy rodzaj algorytmu kryptograficznego polega na tym, że do zaszyfrowania oraz odszyfrowania używa się tego samego klucza. Tekst wiadomości może zostać podzielony na bloki o długości 64 lub 128 bitów albo strumień, który polega na szyfrowaniu tekstu bit po bicie;
- drugi rodzaj algorytmu kryptograficznego polega na wykorzystaniu klucza publicznego osoby, do której przesyłana jest wiadomość, natomiast do odszyfrowania osoba ta używa własnego, prywatnego klucza.

Rys. 52. Szyfrowanie symetryczne

ródło: https://i0.wp.com/www.diwebsity.com/wp-content/uploads/2019/11/15.-Symetryczne.png?resize=768%2C420&ssl=1 [dostęp: 12.02.2023].

Przy **szyfrowaniu symetrycznym** używa się tego samego klucza do szyfrowania i do deszyfrowania wiadomości, albo klucz deszyfrujący da się bezpośrednio wyprowadzić z klucza szyfrującego. Znajomość zatem dobrego klucza służącego do zakodowania wiadomości umożliwia także jej odczytanie. Rozwiązanie to jest szybsze od asymetrycznego i dzieli się na:

- **strumieniowe** – kodują jedną jednostkę informacji (bit) w tym samym czasie;
- **blokowe** – kodują grupę informacji (wiele bitów) w tym samym czasie.

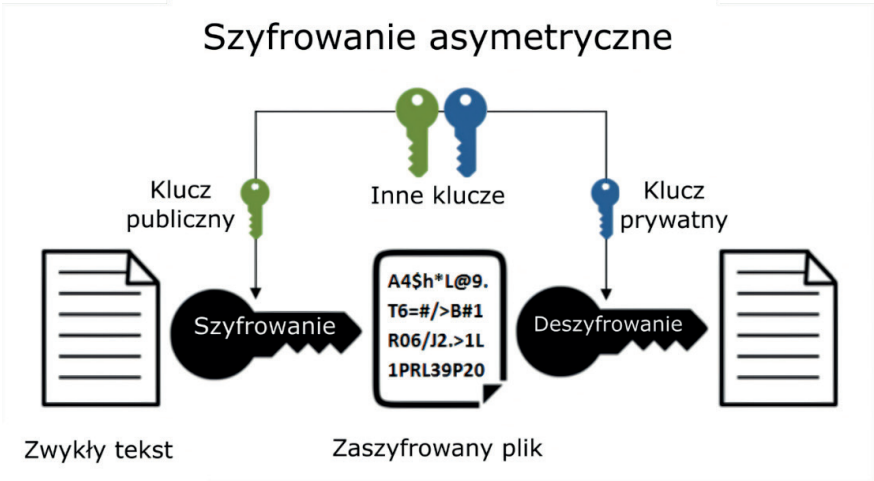
Do najczęściej używanych i obecnie stosowanych algorytmów z kluczem symetrycznym należą:

- **DES** – jest szyfrem blokowym z blokami o długości 64 bitów;
- **3 DES** – polega na trzykrotnym wywołaniu zwykłego algorytmu DES;
- **RC-2** – szyfr blokowy z kluczem o zmiennej długości, zaprojektowany w celu zastąpienia szyfru DES;
- **RC-4** – to symetryczny szyfr strumieniowy, szczególnie znany i ceniony za prostotę implementacji i szybkość działania;
- **RC-5** – szybki szyfr blokowy. RC5 nie jest kolejną wersją algorytmu RC4, który jest szyfrem strumieniowym szyfrującym pojedyncze bajty, a nie całe bloki;
- **IDEA** – szyfr blokowy, operujący na 64-bitowych blokach wiadomości i wykorzystujący do szyfrowania 128-bitowy klucz;
- **Blowfish** – jest wykorzystywany w wielu produktach kryptograficznych i zapewnia wysoką jakość zabezpieczenia. Nie istnieje żaden znany efektywny atak na ten szyfr;
- **Rijndael –** jest szyfrem blokowym operującym na 128 bitowych blokach danych. Wykonuje 10 (klucz 128 bitów **–** standard przyjęty przez **NIST**[201]), 12 (klucz 192 bity) lub 14 (klucz 256 bitów) rund szyfrujących typu substitution-permutation. Składają się one z substytucji wstępnej, permutacji macierzowej (mieszanie wierszy oraz mieszanie kolumn) i modyfikacji za pomocą klucza. Funkcja substytucyjna ma konstrukcję, która uodparnia ten algorytm na znane ataki kryptoanalizy różnicowej i liniowej.

W algorytmach symetrycznych klucze są wybierane losowo, a ich długość wynosi zwykle 128 lub 256 bitów, w zależności od wymaganego poziomu bezpieczeństwa. Z kolei w przypadku szyfrowania asymetrycznego, aby miało miejsce

[201] **Advanced Encryption Standard** (krócej AES, nazwa oryginalna: Rijndael) – symetryczny szyfr blokowy przyjęty przez **NIST** jako standard FIPS-197 w wyniku konkursu ogłoszonego w 1997 roku. W 2001 roku został przyjęty jako standard. https://pl.wikipedia.org/wiki/RSA_(kryptografia) [dostęp: 12.02.2023].

szyfrowanie i deszyfrowanie, musi istnieć matematyczny związek między kluczem publicznym a prywatnym. Oznacza to, że musi istnieć między nimi unikalna formuła matematyczna. Z uwagi na fakt, że ten wzorzec może zostać potencjalnie wykorzystany przez osoby atakujące do złamania szyfrowania, klucze asymetryczne muszą być znacznie dłuższe, aby zapewnić równoważny poziom bezpieczeństwa. Ostatecznie 128-bitowy klucz symetryczny i 2048-bitowy klucz asymetryczny oferują w przybliżeniu podobny poziom bezpieczeństwa[202].



Rys. 53. Szyfrowanie asymetryczne

Źródło: https://i2.wp.com/www.diwebsity.com/wp-content/uploads/2019/11/15.-Asymetryczne.png?fit=640%2C353&ssl=1 [dostęp: 12.02.2023].

W porównaniu do kryptografii symetrycznej, algorytm asymetryczny wymaga zastosowania złożonych operacji, takich jak mnożenie lub potęgowanie. Z tego względu bardzo często stosuje się systemy mieszane, wykorzystując szybki szyfr symetryczny, oraz wiadomość zaszyfrowaną algorytmem asymetrycznym.

Szyfrowanie asymetryczne (z kluczem publicznym) – używa się odmiennego klucza do szyfrowania i deszyfrowania, a klucza deszyfrującego nie da się wyprowadzić z klucza szyfrującego. Klucz szyfrujący jest zwykle udostępniany publicznie , więc każdy może zakodować informację, jednak jej odczytanie możliwe jest jedynie przez adresata, który posiada odpowiedni klucz deszyfrujący – nie ujawniany. Klucze asymetryczne:

[202] https://monitorfx.pl/kryptografia-symetryczna-i-asymetryczna [dostęp: 12.02.2023].

- być może najbardziej pomysłowym i wpływowym osiągnięciem w nowoczesnej kryptografii jest para kluczy asymetrycznych, zwanych również parami kluczy publiczno-prywatnych. Podstawowa idea polega na tym, że generowane są dwa klucze, jeden do szyfrowania, a drugi do deszyfrowania. Klucz szyfrowania jest bezpieczny do rozpowszechniania, klucz deszyfrowania jest utrzymywany w tajemnicy;
- innowacja ta została zapoczątkowana w późnych latach 70. XX w. przez dwóch programistów i matematyka, którzy nadali swoje inicjały – RSA[203] – przełomowemu systemowi kryptograficznemu, który wymyślili. Podobny system został wynaleziony kilka lat wcześniej przez matematyka z brytyjskiego wywiadu, ale wynalazek ten został utrzymany w tajemnicy, a system uznano wówczas za niepraktyczny ze względu na ograniczenia systemów komputerowych.

Obecnie kryptografia z kluczem publiczno-prywatnym stanowi podstawę większość nowoczesnej infrastruktury bezpieczeństwa internetowego, w tym bezpieczeństwa warstwy transportowej[204].

Do wykorzystywanych obecnie algorytmów opartych o metodę klucza asymetrycznego należą:

- DSS – to metoda korzystająca z **funkcji haszującej**[205]. Na dane wejściowe składają się wyniki haszowania oraz liczby losowej k, generowanej specjalnie dla danej sygnatury;
- ElGamal – to jeden z dwóch najważniejszych algorytmów kryptografii asymetrycznej;
- RSA – jeden z pierwszych i obecnie najpopularniejszych asymetrycznych algorytmów kryptograficznych z kluczem publicznym. Pierwszy algorytm, który może być stosowany zarówno do szyfrowania, jak i do podpisów cyfrowych.

---

[203] Algorytm Rivesta-Shamira-Adlemana (RSA) – *jeden z pierwszych i obecnie najpopularniejszych asymetrycznych algorytmów kryptograficznych z kluczem publicznym, zaprojektowany w 1977 przez Rona Rivesta, Adiego Shamira oraz Leonarda Adlemana.*

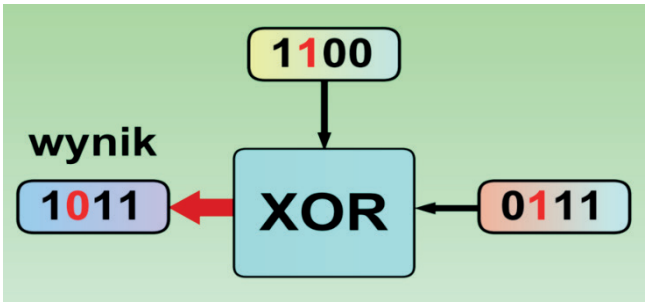
[204] Warstwa transportowa jest zazwyczaj ***chroniona przez protokół bezpieczeństwa warstwy transportowej (TLS)*** lub mTLS (TLS z uwierzytelnianiem wzajemnym). Jest to ***ugruntowany*** standard ***ochrony*** *warstwy transportowej w technologiach internetowych, stosowany na całym świecie w odniesieniu do dużej liczby usług. TLS/mTLS zapewnia szyfrowanie i uwierzytelnianie kanału transportowego.*

[205] **Funkcja hashująca,** zwana także funkcją skrótu, ***generuje unikalny skrót (ciąg znaków) dla konkretnych danych***.

Cyfrowe podpisy – niektóre algorytmy z kluczem publicznym mogą być używane do generowania cyfrowych podpisów. Podpis cyfrowy jest blokiem danych, który został wygenerowany za pomocą określonego tajnego klucza oraz istnieje klucz publiczny, który może być użyty do weryfikacji, czy podpis został naprawdę wygenerowany za pomocą odpowiadającego klucza prywatnego. Algorytm użyty do generowania podpisu musi być taki, że bez znajomości klucza prywatnego nie jest możliwe stworzenie podpisu, który byłby zweryfikowany jako ważny.

Algorytmy ograniczone – istotne jedynie z historycznego punktu widzenia; nie są akceptowalne dla potrzeb prawdziwego bezpieczeństwa. Wystarczy bowiem odkryć jeden algorytm, aby możliwe było odszyfrowanie wszystkich wiadomości, które zostały nim zakodowane. Algorytmy z kluczem – by odczytać konkretną wiadomość musimy posiadać właściwy klucz. Operacja XOR to operacja na dwóch bitach zwracająca wartość 1 lub 0.

0 XOR 0 = 0
1 XOR 1 = 0
0 XOR 1 = 1
1 XOR 0 = 1



Rys. 54. Operacja XOR

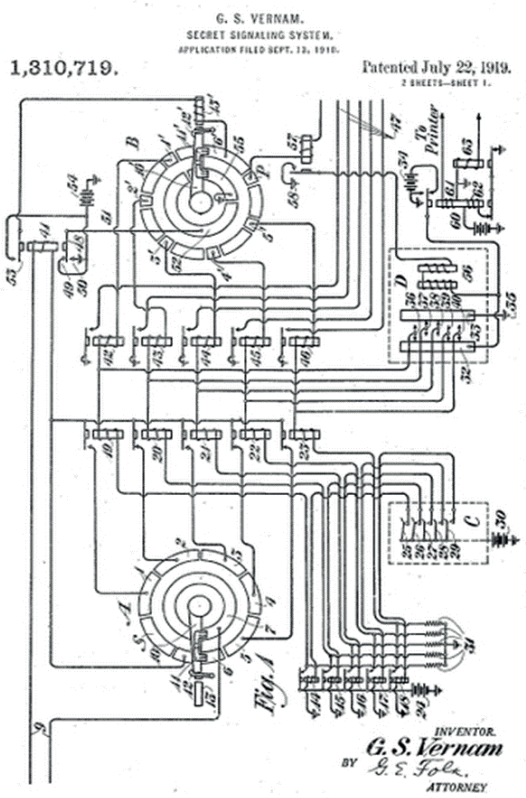
Źródło: Opracowanie własne.

Procedura szyfrowania/deszyfrowania zostaje wykonana tak, że każdy znak tekstu jawnego/zaszyfrowanego zostaje xorowany (XOR -logiczny funktor zdaniotwórczy)[206] przez określoną wartość i następnie zapisany do pliku wyjściowego. Po kolejnym dokonaniu operacji XOR z pliku zaszyfrowanego otrzymamy plik z tekstem jawnym. Procedury szyfruj/deszyfruj są identyczne.

[206] https://pl.wikipedia.org/wiki/Alternatywa_roz%C5%82%C4%85czna [dostęp: 16.04.2024].

Dobrym przykładem są urządzenia do monitorowania pomieszczenia, w którym przebywa dziecko, na odległość. Haker włamywacz, który odpowiednio przeprogramuje tzw. elektroniczną nianię, może na przykład za jej pośrednictwem podsłuchiwać lub podglądać to, co się dzieje w domu, dzięki czemu może na przykład sprawdzać, czy w danym momencie ktoś w nim przebywa. W dobie upowszechniania się Internetu niebezpieczna mogłaby także być sytuacja, w której hakerzy spowodują, że urządzenie będzie działało nieprawidłowo albo w sposób nieprzewidywalny. Łatwo można sobie wyobrazić skutki rozregulowania przez przestępców, na przykład systemu automatyki domowej, do którego włamali się, przeprogramowując jeden z jego elementów. Aby takich sytuacji uniknąć, należy zadbać o to, by oprogramowanie instalowane lub aktualizowane pochodziło z pewnego źródła i nie mogło później zostać zmodyfikowane przez osoby nieuprawnione. W tym celu firmware[207] instalowany na etapie produkcji i wszelkie jego kolejne aktualizacje powinny być podpisywane cyfrowo.

[207] Oprogramowanie sprzętowe, oprogramowanie wbudowane, oprogramowanie układowe, oprogramowanie wewnętrzne, mikrooprogramowanie (ang. ***firmware***) – ***oprogramowanie*** **zainstalowane na stałe w urządzeniu, zapewniające podstawowe procedury jego obsług**
[h]ttps://www.bing.com/search?q=firmware&form=ANSPH1&refig=21f78294364c4711b60eced3f1a4c370&pc=U531&sp=1&qs=AS&pq=firmware&sc=10-8&cvid=21f78294364c4711b60eced3f1a4c370 [dostęp: 12.02.2023].



Szyfr Vernama

Ala ma kota

DSB XC NVUL

Rys. 55. Szyfr Vernama z kluczem jednorazowym

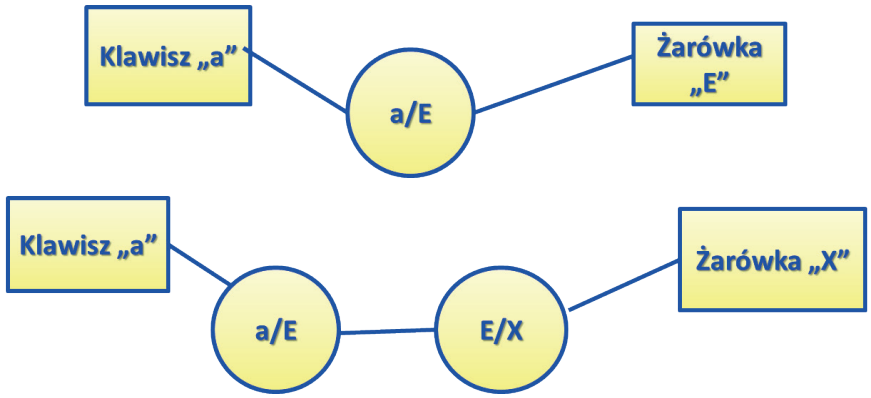
Źródło:https://wykop.pl/cdn/c3201142/comment_eaL5OHTHsNLzgYztL3HrcvnbmJj-sHfoV.jpg [dostęp: 12.02.2023].

Szyfr z kluczem jednorazowym – szyfr zaproponowany w 1917 roku przez Gilberta Vernama, którego, przy poprawnym wykorzystaniu, nie można złamać. Szyfr z kluczem jednorazowym jest dużym zbiorem o niepowtarzalnych i przypadkowych sekwencjach znaków. W pierwotnej postaci była to jednorazowa taśma perforowana do dalekopisu. Nadawca używa każdej litery z tego zbioru do zaszyfrowania jednego znaku tekstu jawnego. Szyfrowanie to dodanie modulo 26 (arytmetyka modularna) jednego znaku tekstu jawnego i znaku jednorazowego klucza. Jest udoskonaleniem szyfru podstawieniowego, w którym kolejna litera tekstu zaszyfrowanego zależy nie tylko od odpowiedniej litery tekstu otwartego, ale również od miejsca, w którym ta litera się znajduje. Weźmy ciąg kilku liczb np. 3,7,1,11,2. Sposób szyfrowania polega teraz na tym, że zamiast pierwszej litery tekstu piszemy literę znajdującą się w alfabecie 3 miejsca dalej,

zamiast drugiej litery literę znajdującą się 7 miejsc dalej, zamiast trzeciej literę o 1 miejsce dalej. Metoda Vernama zapewniała prawie doskonałe zabezpieczenie treści przekazu, ale wymagała użycia dalekopisu lub maszyny szyfrującej.

Rozwiązanie to funkcjonuje na 64-bitowych blokach tekstu jawnego. Po początkowej permutacji blok wejściowy jest dzielony na lewą i prawą połowę, każdą o długości 32 bitów. Następnie jest wykonywanie 16 cykli jednakowych operacji, nazwanych funkcjami f, w czasie których dane są łączone w klucze. Po szesnastym cyklu lewa i prawa połowa są łączone z kluczem. Następnie są one łączone i ostatnia permutacja kończy przebieg algorytmu.

Dysk szyfrowy zasilany prądem to inaczej rotor, który można zastosować do szyfrowania wiadomości. Na obydwu jego powierzchniach znajduje się po 26 styków elektrycznych, a styki przeciwległych stron połączone są przewodami w nieregularnie rozmieszczone pary. Styki jednej strony rotoru są połączone z baterią za pośrednictwem 26 wyłączników oznaczonych literami tekstu jawnego. Styki przeciwległego rotora są połączone z 26 żarówkami podświetlającymi litery tekstu szyfrowanego. Reasumując, jest to po prostu bardziej skomplikowanie zbudowany i zasilany prądem dysk szyfrowy.



Rys. 56. Rotory

Źródło: Opracowanie własne.

Na takiej właśnie zasadzie 3 rotorów działała Enigma, czyli najsłynniejsza maszyna szyfrująca świata. Trzy rotory można ustawić na 6 różnych sposobów, co daje sumę 105 456 możliwości kodowania jednego znaku. Wprowadzona została tablica do dodatkowych połączeń, która zwiększyła możliwości Enigmy do astronomicznych 100 miliardów kombinacji. Systematycznie ulepszana o kombinacje

rotorów miała stać się niezwyciężonym narzędziem Niemców do szyfrowania meldunków.

W obecnych czasach komputery świetnie nadają się do wykonywania zadań wymagających powtórzeń, takich jak szyfrowanie. Można za ich pomocą błyskawicznie i bez żadnych błędów posługiwać się systemami o wiele bardziej skomplikowanymi niż Enigma. Komputer otwiera zupełnie inne możliwości szyfrowania zarówno w kwestii transmisji, jak i przesyłu szyfrowanych danych.

Binarnie	Heksadecymalnie
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

Tablica 1 Liczby binarne i heksadecymalne

Litera	Kod binarny ASCII
k	1101011
o	1101111
t	1110100
K	1001011
O	1001111
T	1010100

Rys. 57. Szyfry komputerowe

Źródło: Opracowanie własne.

Komputery umożliwiają nie tylko szyfrowanie, ale i łamanie szyfrów. Ich moc obliczeniowa pozwala na błyskawiczne dokonywanie analizy frekwencyjnej, poszukiwanie powtarzalnych znaków i testowanie tysięcy kluczy kodowych. Kodotwórcy zostali zmuszeni do opracowywania szyfrów będących poza zasięgiem możliwości człowieka.

Upowszechnienie Internetu spowodowało, iż olbrzymia ilość danych dotycząca nas samych swobodnie wędruje przez sieć i aż prosi się o ich przechwycenie. Przedsiębiorcy, rządy, a także zwykli ludzie chcący bezpiecznie przekazywać informacje, również płacić kartami kredytowymi, zaczęli poszukiwać bezpiecznej metody. Tak właśnie powstały popularne dzisiaj szyfry komputerowe (DES – przekształcony w 3DES, IDEA, AES – Rijndael, RC6, MARS, MD5 i wiele innych).

Mimo, iż porozumiewamy się z komputerami za pomocą słów lub kliknięć myszką, wewnątrz krążą wyłącznie liczby. Komputery posługują się liczbami będącymi sumami potęg liczby, 2 – liczbami dwójkowymi, czyli binarnymi. W układzie binarnym występują tylko dwie cyfry: 0 i 1. Zamiana liter i innych znaków na liczby binarne odbywa się na komputerze zgodnie z kodem ASCII.

Słowo „kod" w zależności od wielkości liter stanie się różnym ciągiem zer i jedynek. Każda pozycja liczby zerojedynkowej nazywana jest bitem. Ciąg binarny odpowiadający słowu „kod" ma więc „21 bitów". Do dostępnych w Internecie programów szyfrujących możemy dla przykładu zaliczyć:

- **VMPCrypt – pozwala** na ukrycie poufnych plików, pozwala przesłać zaszyfrowane emaile, przeprowadzić szyfrowaną rozmowę on-line, ukryć prywatne kontakty i listę haseł. Przy pomocy tego programu możemy w nieodwracalny sposób pozbyć się niepotrzebnych plików i wygenerować bezpieczne hasła;
- **Blowfish Advanced CS** (znany również jako Blue Coat) – narzędzie do usuwania złośliwego oprogramowania, które zostało stworzone przez hakerów w celu szpiegowania użytkowników systemu Windows i kradzieży ich danych osobowych. To nie jest zwykłe narzędzie złośliwego oprogramowania, ponieważ jest to klon „Spyware Zoom", który sam był klonem Spyware Protect 2009;
- **CrypTool** – edukacyjny, z dziedziny kryptologii. Zaimplementowano w nim wiele algorytmów i protokołów kryptograficznych, a także narzędzia kryptoanalizy. Program został zaplanowany w taki sposób, aby nawet osoba bez przygotowania informatycznego mogła eksperymentować i uczyć się o współczesnych metodach zabezpieczania danych. Zasady działania większości algorytmów klasycznych, a także algorytmów asymetrycznych RSA, ECC, podpisów cyfrowych czy protokołu uzgadniania kluczy Diffiego-Hellmana, zostały zaprezentowane przy pomocy czytelnych animacji. Do programu dołączona jest elektroniczna wersja podręcznika zawierającego teoretyczne wprowadzenie do współczesnej kryptologii[208].

Jeśli polecić komputerowi, aby zaszyfrował jakąś wiadomość, najpierw zostanie ona zamieniona na ciąg zer i jedynek. Następnie odpowiednie oprogramowanie szyfrujące spowoduje, że owe bity zostaną pozamieniane i poprzestawiane w sposób bardziej skomplikowany niż można to sobie wyobrazić. Nie wszystkie oprogramowania szyfrujące są tajne. Przykład stanowią tu DES i IDEA, które są używane na całym świecie. Mimo to zaszyfrowana przez nie

[208] https://pl.wikipedia.org/wiki/CrypTool [dostęp: 12.02.2023].

wiadomość jest niemalże nie do złamania bez znajomości klucza. Jeśli klucz ma długość dwóch bitów, można przyjąć tylko cztery wartości: 00, 01, 10 i 11.

Pierwszym powszechnie stosowanym systemem szyfrowania był DES z kluczem 56-bitowym, co daje ponad 72 biliardy (10*15) możliwych wartości. Został wprowadzony w 1976 roku, więc ówczesne komputery nie posiadały możliwości jego złamania ze względu na brak mocy obliczeniowej. Wraz ze wzrostem mocy obliczeniowej komputerów rośnie również długość kluczy. Wprowadzony względnie niedawno system IDEA ma 128-bitów, co daje ponad 300 sekstylionów możliwości kodowania (10*36).

Pojawienie się komputerów, Internetu i łączenie ich w sieci, a co za tym idzie przesyłanie sobie danych za pomocą komputera, spowodowało wzrost znaczenia kryptografii stosowanej. Zniknęła granica fizycznych zabezpieczeń naszych danych, należało więc odpowiednio dostosować standardy, aby każdy czuł się w sieci tak bezpiecznie, jak to tylko możliwe. Z komputerów przestało korzystać wyłącznie wojsko, lecz także użytkownicy komercyjni, banki, międzynarodowe przedsiębiorstwa. Dlatego też globalna współpraca firm przyniosła nie tylko poprawę standardów bezpieczeństwa, ale także stały ich rozwój. Naturalne potrzeby użytkowników idealnie pokrywały się z tym, czego kryptografia komputerowa może dostarczyć: bezpieczne przesyłanie danych bez zbędnych trudności i olbrzymią wiedzę matematyczną. Stąd wprowadzenie protokołu SSL, bezpiecznych sieci VPN, kluczy WPA itp.

Warto dla własnego bezpieczeństwa zainteresować się komercyjnymi programami szyfrującymi. Nie zapewnią one oczywiście 100% ochrony, ale będą stanowiły dodatkową osłonę. Haker lub osoba postronna widząc, iż zaszyfrowaliśmy pliki i hasła, prawdopodobnie podda się bez próby ich łamania, czekając na łatwiejszy sposób i miejsce, niż nasz komputer.

Niektóre algorytmy z kluczem publicznym mogą być używane do generowania cyfrowych podpisów. Podpis cyfrowy jest blokiem danych, który został wygenerowany za pomocą określonego tajnego klucza oraz istnieje klucz publiczny, który może być użyty do weryfikacji, czy podpis został naprawdę wygenerowany za pomocą odpowiadającego klucza prywatnego. Algorytm użyty do generowania podpisu musi być taki, że bez znajomości klucza prywatnego nie jest możliwe stworzenie podpisu, który byłby zweryfikowany jako ważny.

Podpisy cyfrowe są używane do weryfikacji, czy wiadomość naprawdę pochodzi od właściwego nadawcy (zakładając, że tylko nadawca zna klucz prywatny odpowiadający jego kluczowi publicznemu). Mogą być również używane

do datowania dokumentów: zaufana strona podpisuje dokument i jego datę używając klucza prywatnego, w ten sposób poświadczając wiarygodność dokumentu.

Rys. 59. Podpisy cyfrowe

Karty elektroniczne, czyli karty stykowe (znane pod nazwą karty chipowe) pamięciowe i procesorowe oraz karty zbliżeniowe – w dzisiejszych czasach znajdują szerokie zastosowanie w wielu dziedzinach życia. Pojawiają się jako karty identyfikacyjne, karty ubezpieczenia zdrowotnego, karty do kontroli dostępu do pomieszczeń, identyfikacji do systemów informatycznych, obiektów sportowych, karty wykorzystujące podpis elektroniczny lub wykorzystywane w systemach lojalnościowych itp.

Rys. 59. Karty elektroniczne

Źródło: https://www.epuzzle.info/es/rompecabezas/jugar/tecnolog%C3%ADa/115468-tarjeta-de-cr%C3%A9dito#16x10

https://pl.wikipedia.org/wiki/CrypTool [dostęp: 12.02.2023].

Najbardziej znanym przedstawicielem technik klucza publicznego jest algorytm RSA, który opiera się na założeniu, że mnożenie dwóch liczb jest prostą operacją, natomiast proces odwrotny, pierwiastkowanie wyniku, wymaga ogromnej mocy obliczeniowej, zwłaszcza wtedy, gdy wynik trzeba rozłożyć na czynniki pierwsze. Odbiorca wykonuje przy odszyfrowaniu takie same operacje, jak nadawca podczas szyfrowania. W podobny sposób można zastosować algorytm RSA do generowania i weryfikacji podpisów.

Coraz więcej urządzeń jest łączonych w sieci i korzysta z Internetu. Wraz z rozwojem inteligentnych sieci elektroenergetycznych i Internetu oraz wprowadzeniem do użytku samochodów autonomicznych, ataków hakerskich będzie przybywać. Skutkami ich działania będą nie tylko straty materialne, lecz zagrożone będzie też ludzkie zdrowie i życie. Kwestię bezpieczeństwa konstruktorzy elektroniki powinni więc traktować bardzo poważnie, wykonując analizę ryzyka dla danej aplikacji, a następnie, na jej podstawie, wybierając **zabezpieczenia** w danym przypadku najskuteczniejsze. Warto przy tym przyjąć założenie, że jeżeli urządzenie znajdzie się na celowniku hakerów, których wyróżnia motywacja, wiedza oraz doświadczenie oraz dysponowanie odpowiednim sprzętem, możliwe jest pokonanie przez nich w zasadzie każdego zabezpieczenia, pomimo najlepszej ochrony.

Obecnie na naszych oczach pojawiła się kryptowaluta, rzadziej waluta kryptograficzna – rozproszony system księgowy bazujący na kryptografii, przechowujący informację o stanie posiadania określonej wartości w umownych jednostkach. Stan posiadania związany jest z poszczególnymi węzłami systemu („portfelami") w taki sposób, aby kontrolę nad danym portfelem kryptowalutowym miał wyłącznie posiadacz odpowiadającego mu klucza prywatnego i niemożliwe było dwukrotne wydanie tej samej jednostki. Kryptowaluta jest szczególnym przypadkiem waluty wirtualnej[209].

[209] https://pl.wikipedia.org/wiki/Kryptowaluta [dostęp: 12.02.2023].

Rys. 60. Kryptowaluty

Źródło: https://medium.com/@markmuskardin/not-your-keys-not-your-crypto-373945c8d46d [dostęp: 15.07.2023].

Ludzie od dawna starali się ukrywać różne informacje z różnych powodów. Pojawienie się komputerów spowodowało powstanie nowych możliwości zabezpieczania danych przed dostępem do nich osób niepowołanych. W większości przypadków popularne metody kryptograficzne w wystarczający sposób zapewniają ukrycie danych przed innymi. Należy jednak pamiętać, że nie istnieje idealny algorytm, którego nie dałoby się złamać (wymaga to tylko czasu). Przyjmuje się, że algorytm kryptograficzny jest bezpieczny, jeśli w momencie jego powstania nie istnieją metody i środki mogące go złamać (dobry algorytm powinien zapewniać bezpieczeństwo przynajmniej na kilkadziesiąt lat). Kryptografia zmienia się wraz z ciągłym unowocześnianiem systemów komputerowych. Tworzone są nowe algorytmy, bądź też udoskonalane są już te znane. Wszystko to jest celem jak najlepszego zabezpieczenia informacji w systemach i sieciach komputerowych.

Tworzenie szyfrów spełnia kilka podstawowych funkcji. Jedną z nich jest na przykład ochrona przez ujawnieniem informacji przesyłanych oraz przechowywanych w systemach i sieciach komputerowych. W kwestii biznesowej wiąże się to z funkcją ochrony firmowych informacji przed szpiegostwem innych członków firm, a także do ochrony własności handlowych. W kwestii osób prywatnych chodzi głównie o ustrzeżenie się plotek, osobistych wrogów, a także przed złodziejami tożsamości i instytucjami nadużywającymi swojej władzy. Kwestia szyfrowania jest także bardzo bliska rządom państw w celu zachowania tajemnic wojskowych oraz dyplomatycznych, ochrony komunikacji związanej

z dochodzeniami w sprawach kryminalnych i z terroryzmem przed ludźmi śledzonymi oraz do ochrony innych informacji wrażliwych będących w posiadaniu rządu. Tworzenie szyfru odgrywa ważną rolę w zapobieganiu przestępstwom[210].

Bezpieczeństwo komunikacji systemów komputerowych jest bardzo ważne w naszym życiu. Obecnie jednak spotyka się ono z wieloma problemami, dotyczącymi chociażby niskiego poziomu zabezpieczeń, czy też kwalifikacji technologicznych w tym zakresie. Wszystko to wiąże się ścisłe z niskim poziomem świadomości na czyhające niebezpieczeństwa. Metody zabezpieczania komunikacji komputerowej zależą głównie od danej sytuacji. Standardem protokołów komunikacyjnych używanych w sieciach komputerowych TCP/IP w architekturze klient-serwer jest SSH (ang. *secure shell*). W szerszym znaczeniu SSH to wspólna nazwa dla całej rodziny protokołów, nie tylko terminalowych, lecz także służących do przesyłania plików (SCP, SFTP), zdalnej kontroli zasobów, tunelowania i wielu innych zastosowań. Wspólną cechą wszystkich tych protokołów jest identyczna z SSH technika szyfrowania danych i rozpoznawania użytkownika. Obecnie protokoły z rodziny SSH praktycznie wyparły wszystkie inne, mniej bezpieczne protokoły[211].

Celem tego rozdziału było przedstawienie kryptografii, która zajmuje ważnie miejsce w zapewnieniu bezpieczeństwa informacji. Dla realizacji wyznaczonego celu w opracowaniu dokonano analizy rozwoju kryptografii, od początku jej powstania aż do czasów współczesnych. Dokonana analiza pozwoliła na ustalenie jej praktycznego zastosowania w celu ochrony informacji w różnych okresach jej rozwoju. Analizie poddano również rozwiązania kryptograficzne, umożliwiające bezpieczeństwo informacji przetwarzanych w komputerach i przesyłanych za pomocą sieci komputerowej.

Potwierdzona została również stanowiąca przypuszczenie następująca **hipoteza robocza,** w której założono, że w celu zapewnienia bezpieczeństwa gromadzonym, przetwarzanym i przesyłanym informacjom wymagane jest poszukiwanie skutecznych nowoczesnych rozwiązań. W świetle przeprowadzonej analizy nie ulega wątpliwości, że rozwiązń takich może dostarczyć kryptografia, która wykorzystuje wiedzę matematyczną do skutecznej ochrony informacji w systemach i sieciach komputerowych.

[210] D. E. Denning, *Wojna informacyjna i bezpieczeństwo informacji,* WNT, Warszawa 2002, s. 466.
[211] E. Schetina, K. Green, J. Carlson, *Bezpieczeństwo w sieci*, Helion, Gliwice 2002, s. 154.

Poddane analizie w opracowaniu rozwiązania pozwalają na przedstawienie następujących wniosków generalizujących:

- współczesna kryptografia **istnieje** na skrzyżowaniu dyscyplin matematycznych, informatycznych, elektrotechnicznych, komunikacyjnych i fizycznych;
- kryptografia znajdowała i nadal znajduje zastosowanie w wielu obszarach naszego życia, w tym szczególnie służy do ochrony informacji (danych) w wojsku, wywiadzie, jednostkach specjalnych, policji, dyplomacji, biznesie i administracji publicznej itp.;
- dzięki rozwiązaniom kryptografii można zapewnić bezpieczeństwo podczas: transakcji internetowych, kryptowalutowych, kontroli dostępu do pomieszczeń i korzystania z niejawnych zasobów informacyjnych;
- jest niezbędna do zabezpieczenia sprzętu komputerowego hasłami, realizacji transakcji bankowych i handlowych wykonywanych przez Internet i zapewnienia ochrony informacji w plikach czy folderach;
- zabezpiecza dane przed cyberatakami i atakami przestępców komputerowych;
- systemy i sieci komputerowe mogą być zabezpieczone w zależności od potrzeb, jednym lub za pomocą wielu mechanizmów kryptograficznych;
- szyfrowanie to proces, który koduje wiadomość lub pliki, dzięki czemu mogą je odczytać wyłącznie upoważnione osoby;
- z technicznego punktu widzenia szyfrowanie jest to proces przekształcenia zwykłego tekstu na tekst zaszyfrowany. Algorytm szyfrowania pobiera czytelne dane i zmienia je tak, aby wyglądały jak losowy zbiór symboli;
- podstawowe formy szyfrowania mogą być tak proste, jak zamiana liter. Jednak rozwój technik kryptograficznych sprawił, że algorytmy szyfrujące są coraz bardziej rozbudowane, a deszyfrowanie coraz trudniejsze;
- zawansowane współczesne procedury szyfrowania są na tyle skomplikowane, że jest bardzo mało prawdopodobne, by jakakolwiek nieuprawniona osoba lub algorytm były w stanie odszyfrować tekst zgadując;
- poznając podstawy kryptografii, pojęcia i zasadę działania oraz praktyczną różnorodność metod i funkcji, możemy osiągnąć wymierne korzyści organizacyjne i ekonomiczne, co pozwoli zapewnić wymagany poziom bezpieczeństwa chronionym informacjom;
- dobrym rozwiązaniem zapewniającym bezpieczeństwo informacji są technologie szyfrowania, które powodują, że **wykradzione dane** nie będą mogły

zostać odczytane przez osobę nieuprawnioną, która chce je wykorzystać dla własnych celów;

- włamanie do prywatnego komputera może skończyć się dostępem do najbardziej osobistych informacji. W gorszej sytuacji są jednak firmy, ponieważ w ich przypadku wyciek poufnych lub wrażliwych danych może wiązać się z naruszeniem prawa, wysokimi grzywnami, stratami finansowymi i utratą zaufania klientów;
- przez zapewnienie poufności informacji **mechanizmy kryptograficzne** gwarantują, że wyłącznie upoważnieni użytkownicy będą mogli je odczytać. Jeśli poufność nie jest zapewniona, na przykład w przypadku komunikacji sieciowej, każdy, kto ma dostęp do sieci i jest w stanie monitorować ruch sieciowy oraz przechwytywać transmitowane dane, będzie się mógł z nimi bez problemu zapoznać;
- ważną funkcją **mechanizmów kryptograficznych** jest uwierzytelnianie, polegające na weryfikacji tożsamości podmiotów, które na przykład komunikują się ze sobą za pośrednictwem sieci. Dzięki zidentyfikowaniu nadawcy oraz odbiorcy wiadomości, na przykład na podstawie posiadanych przez nich certyfikatów uwierzytelniających, nie jest możliwe podszycie się osób nieuprawnionych;
- **integralność informacji** jest gwarantowana przez sprawdzenie, czy ich oryginalna treść nie została zmodyfikowana lub uszkodzona. W tym celu danemu zbiorowi danych przypisywana jest unikalna, zależna od jego zawartości, wartość. Jest ona znana odbiorcy wiadomości. Osoba, która nie ma do tego uprawnień, zmieniając jej oryginalną treść, modyfikuje też tę wartość. Porównując ją z tą oczekiwaną, odbiorca może wykryć, że doszło do niepożądanej ingerencji z zewnątrz;
- należy również pamiętać, że mimo nawet najlepszej ochrony, bezpieczeństwo informacji jest zdeterminowane przez jego najsłabsze ogniwo, którym jest zazwyczaj człowiek.

Jeżeli działają **mechanizmy kryptograficzne**, nie dojdzie do sytuacji, w której którakolwiek ze stron komunikacji mogłaby się dopuścić przekłamania na temat przebiegu i/albo wyniku tego procesu. Oznacza to, że nadawca nie może zaprzeczyć, że wysłał dany komunikat lub stwierdzić, że zrobił to w innym czasie niż w rzeczywistości, zaś odbiorca nie może się wyprzeć, że wiadomość w danym momencie odebrał. Dowodami są na przykład sygnatury czasowe i podpisy cyfrowe.

7. ROLA I ZADANIA ADMINISTRATORA SYSTEMU (SIECI) INFORMATYCZNEGO

Administrator to osoba, która może na komputerze wprowadzić zmiany wpływające na innych użytkowników komputera. **Administratorzy** mogą zmieniać ustawienia zabezpieczeń, instalować oprogramowanie i sprzęt, uzyskiwać dostęp do wszystkich plików na komputerze i wprowadzać zmiany na kontach innych użytkowników[212].

Administrator systemów komputerowych (łac. *administrator* – zarządca), żargonowo „**sysadmin”** (ang. *system administrator*) – informatyk zajmujący się zarządzaniem systemem informatycznym i odpowiadający za jego sprawne działanie. Wyróżnić można administratorów między innymi:

- aplikacji,
- baz danych,
- kopii bezpieczeństwa,
- sieci LAN/MAN/WAN,
- systemów operacyjnych (serwerów)[213].

Administrator systemu (sieci) komputerowej to specjalista wysokiej klasy, zajmujący się budowaniem, integracją oraz obsługą systemu (sieci) komputerowych opartych na różnych architekturach. Może to być pracownik zatrudniony w firmie na podstawie umowy cywilno-prawnej lub umowy o pracę (osoba z wewnątrz organizacji) lub ktoś spoza niej (tzw. outsourcing). Należy

[212] https://www.bing.com/search?q=administrator&form=ANSPH1&refig=c71a146f2a634fd4bb823cd738e13358&pc=U531 [dostęp: 10.06.2023].

[213] https://pl.wikipedia.org/wiki/Administrator_system%C3%B3w_komputerowych [dostęp: 10.06.2023].

zaznaczyć, że taka osoba powinna przede wszystkim posiadać odpowiednią wiedzę w zakresie IT, ale również być na bieżąco w temacie nowych zagrożeń oraz pojawiających się na rynku rozwiązań w tematyce bezpieczeństwa informacji. W celu uzyskania fachowej wiedzy w tej materii należy brać udział w szkoleniach specjalistycznych oraz uczestniczyć w konferencjach i innych spotkaniach dotyczących takich zagadnień[214].

Administrator sieci powinien mieć **wykształcenie informatyczne**, najlepiej wyższe lub ewentualnie zaświadczone certyfikatem znanej firmy (Microsoft, Cisco itp.). Musi posiadać także **umiejętności programistyczne** (często sam pisze programy). Powinien mieć **teoretyczną i praktyczn**ą wiedzę o lokalnych sieciach informatycznych oraz o Internecie. Zwykle wymaga się też **doświadczenia** zawodowego, umiejętności administrowania zarówno systemami i sieciami opartymi na Windows, Novell, Linuksie itp.., znajomości zagadnień baz danych, funkcjonujących w sieciach (np. MySQL, Postgres, Oracle, IBM), a także wiedzy na temat sprzętu. Administrator może także zarządzać sieciami teleinformatycznymi (np. szkieletowymi), przeznaczonymi do przesyłu sygnału internetowego w różnych prędkościach – zarówno za pomocą kabli miedzianych, światłowodowych, jak i bezprzewodowo.

Najlepszymi kandydatami na administratorów są osoby posiadające dobry zmysł organizacyjny, rozwinięte umiejętności analityczne i lubiące pracę z ludźmi. W pracy pomaga też komunikatywność, otwartość i wyrozumiałość. Niezbędna jest też cierpliwość względem osób korzystających z sieci, którym często trzeba wyjaśnić zagadnienia będące dla informatyka czymś oczywistym. Administrator sieci powinien podejmować zdecydowane i szybkie, ale racjonalne decyzje. To często od niego zależy, czy uda się uchronić firmę przed stratami w przypadku awarii sieci. Praca administratora ma duży wpływ na sprawne działanie każdego nowoczesnego przedsiębiorstwa.

Administrator opiekuje się systemem, to od niego w dużym stopniu zależy funkcjonowanie całego systemu w firmie. To administrator przydziela prawa poszczególnym osobom, sprawuje nadzór nad systemem, dążąc do utrzymania jego maksymalnej efektywności i ochrony jego zasobów. Zapewnienia każdemu użytkownikowi przeznaczone dla niego usługi i dostęp do oprogramowania. Administrator ma za zadanie:

[214] https://odo24.pl/blog-post.obow [dostęp: 10.06.2023].

- współpracować z pracownikami z firmy, kontrolować dostęp (rejestrowanie i wyrejestrowywanie użytkowników, zarządzanie hasłami, użycie uprzywilejowanych programów narzędziowych);
- formułować politykę realizacji przedsięwzięć informatycznych;
- planować i stosować środki ochrony biometrycznej i kryptograficznej;
- planować zabezpieczenia fizyczne, techniczne, środowiskowe, personalne i organizacyjne[215];
- decydować o zakupie sprzętu informatycznego;
- instalować i konfigurować sprzęt;
- decydować o doborze i zakupie licencjonowanego oprogramowania;
- instalować i konfigurować oprogramowanie, co należy do wyłącznej jego kompetencji;
- planować i wykonywać uaktualnienia oprogramowania;
- monitorować i uzupełniać brakujące komponenty w systemie;
- prowadzić szkolenia w zakresie zainstalowanego oprogramowania;
- tworzyć i uaktualniać dokumentację elementów systemu;
- minimalizować zagrożenia wynikające z przeoczeń, błędów, nadużyć i nieupoważnionych działań podejmowanych przez ludzi;
- prowadzić przegląd rejestrów zawierających informacje o zdarzeniach w systemie operacyjnym.

Zakres zadań administratora zależy od wielkości sieci (firmy), którą musi administrować. W małej firmie, gdzie do sieci podpiętych jest kilka lub kilkanaście komputerów, taka osoba w zasadzie najczęściej pełni rolę fachowca od wszystkiego, co się wiąże z elektroniką i komputerami. Tak więc oprócz tego, że powinien dbać o całą infrastrukturę sieciową (konfiguracja, dbanie o bezpieczeństwo sieci, archiwizowanie danych itp.), administrator musi również być jednocześnie serwisantem sprzętu komputerowego, szkoleniowcem osób zatrudnionych w firmie, a dodatkowo często musi być grafikiem (przygotowywanie ulotek, wizytówek, folderów, ofert itp.).

W większych firmach, zwłaszcza związanych z IT, podział obowiązków jest jasno określony. W przypadku dużej sieci w firmie zatrudniony jest cały zespół administratorów. W takiej sytuacji jedna osoba odpowiada za konkretny wycinek działalności sieci. Inna osoba odpowiada za sprzęt sieciowy, a inna za

[215] https://odo24.pl/blog-post.obowiazki-administratora-systemow-informatycznych [dostęp: 10.06.2023].

zarządzanie użytkownikami, w tym ich rejestrację, nadawanie uprawnień, itd. Jeszcze inna troszczy się o oprogramowanie i licencje, a kolejna dba o zabezpieczenia, śledząc na bieżąco pracę systemu. Zadania administratora można pogrupować następująco:

- **zadania cykliczne:**
  - ✓ krótkookresowe (wykonywane codziennie);
  - ✓ średniookresowe (wykonywane co tydzień);
  - ✓ długookresowe (wykonywane co miesiąc);
  - ✓ zadania niecykliczne (wykonywane okazjonalnie).
- **zadania krótkookresowe:**
  - ✓ sprawdzenie dziennika (logi) systemowego;
  - ✓ monitorowanie bieżących alarmów;
  - ✓ monitorowanie bazy danych;
  - ✓ monitorowanie systemu ERP;
  - ✓ monitorowanie systemu operacyjnego;
  - ✓ sprawdzenie działania poszczególnych serwerów;
  - ✓ usuwanie nie zakończonych procesów i sesji użytkowników;
  - ✓ sprawdzanie statusu drukarek;
  - ✓ sprawdzenie wykonania zadań i prac w systemie;
  - ✓ wykonanie kopii zapasowej zmian dziennych;
- **zadania średniookresowe:**
  - ✓ sprawdzanie integralności systemu;
  - ✓ sprawdzanie poziomu wykorzystania systemu i efektywności funkcjonowania;
  - ✓ sprawdzenie wolnego miejsca na dyskach w tym: wielkość systemu plików, wielkość bazy danych, przyrost bazy danych.
- **zadania długookresowe:**
  - ✓ składowanie całego systemu (kopia zapasowa całego systemu przechowywana w bezpiecznym miejscu);
  - ✓ defragmentacja komponentów;
  - ✓ ponowne ustawianie parametrów systemu.
- **zadania okazjonalne:**
  - ✓ aktualizacje systemu operacyjnego;
  - ✓ ustalanie zezwoleń na korzystanie z oprogramowania;
  - ✓ zakładanie i usuwanie kont użytkowników;
  - ✓ przyłączanie terminali do systemu;

- ✓ przyłączanie dysków twardych.

- **zadania instalacyjne:**
  - ✓ fizyczne zainstalowanie komputera z pamięciami masowymi i kartami specjalizowanymi;
  - ✓ instalowanie oprogramowania podstawowego;
  - ✓ instalowanie terminali, modemów, drukarek;
  - ✓ instalowanie użytkowych pakietów programowych;
  - ✓ dostosowanie parametrów środowiska systemu do potrzeb użytkowników.
- **zadania pielęgnacyjne:**
  - ✓ kontrola poziomu wykorzystania zasobów;
  - ✓ strojenie systemu;
  - ✓ archiwizacja systemu plików;
  - ✓ kontrola zajętości przestrzeni dyskowej;
  - ✓ kontrola spójności systemu plików;
  - ✓ rekonfiguracja systemu plików;
  - ✓ kontrola atrybutów związanych z utrzymaniem bezpieczeństwa systemu;
  - ✓ podejmowanie działań dla utrzymania pożądanego poziomu bezpieczeństwa.
- **zadania wynikające z potrzeb bieżących:**
  - ✓ uruchamianie i zatrzymywanie systemu;
  - ✓ usuwanie zablokowanych procesów;
  - ✓ sprawdzanie plików kroniki systemu;
  - ✓ zapis wszystkich modyfikacji systemu i zdarzeń w dzienniku systemu.
  - ✓ usuwanie awarii
  - ✓ ustalanie przyczyn awarii;
  - ✓ rekonstrukcja systemu plików.

Administrator sieci jest odpowiedzialny za wdrażanie usług sieciowych oraz organizowanie i konfigurowanie zasobów sieciowych. Do jego obowiązków związanych z wdrażaniem usług sieciowych należy:

- konfigurowanie serwerów i stacji roboczych oraz urządzeń i programów niezbędnych do realizowania usług sieciowych;
- przygotowanie osobistych i współużytkowanych miejsc przechowywania plików z danymi i plików aplikacji;
- konfigurowanie stacji roboczych, tak aby automatycznie przyłączały się do sieci.

Do obowiązków związanych z organizowaniem i konfigurowaniem zasobów sieciowych należy:

- **zarządzanie siecią:**
  - ✓ ustanawianie i utrzymywanie sieciowego systemu zabezpieczeń;
  - ✓ ustanawianie i utrzymywanie systemu drukowania w sieci.
- **zabezpieczanie danych:**
  - ✓ zapewnienie spójności danych i ich bezpieczeństwa;
  - ✓ organizowanie systemowych procedur kontrolnych;
  - ✓ tworzenie zapasowych kopii danych — opracowanie procedur systematycznego sporządzania kopii oraz odtwarzania danych.
- **dokumentowanie pracy sieci:**
  - ✓ tworzenie drukowanej kopii drzewa NDS;
  - ✓ nadzorowanie uprawnień i dostępu użytkowników do sieci;
  - ✓ rejestrowanie decyzji dotyczących bezpieczeństwa.

Administrator jest odpowiedzialny za:

- zabezpieczenie i kontrolę pomieszczeń, w których przetwarzane są dane osobowe (informacje);
- zapewnienie awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych;
- dopilnowanie aby komputery przenośne, w których przetwarzane są dane osobowe, zabezpieczone były hasłem dostępu przed nieautoryzowanym uruchomieniem oraz nie były udostępniane osobom nieupoważnionym;
- nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych;
- nadzór nad przeglądami, konserwacjami oraz uaktualnieniami systemów służących do przetwarzania danych osobowych oraz wszystkimi innymi czynnościami wykonywanymi na bazach danych osobowych;
- nadzór nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji;
- dopilnowanie, aby ekrany monitorów stanowisk komputerowych, na których przetwarzane są dane osobowe, automatycznie się wyłączały po upływie ustalonego czasu nieaktywności użytkownika;
- wyznaczenie i opisanie pomieszczeń, w których znajdują się monitory stanowisk dostępu do danych osobowych i ustawienie ich w taki sposób, aby uniemożliwić osobom niepowołanym wgląd w dane;

- podjęcie działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie zasad bezpieczeństwa danych.

Cechy dobrego administratora:

- administrator powinien być osobą kompetentną (szczególnie w zakresie technicznym) i umiejętnie współpracować całym zespołem, być ciekawym i chętnym do nauki;
- musi chronić system, być etycznym, elastycznym, dbać o szczegóły i dobrze wiedzieć, kiedy potrzebna jest dodatkowa pomoc;
- od administratora systemu często wymaga się pracy poza zwyczajowymi godzinami pracy – niektóre zadania wymagają pracy po nocach i w weekendy;
- administrator musi dobrze znać czas potrzebny na wykonanie swoich zadań, aby użytkownicy mogli pracować bez przerw i utrudnień;
- ciągle musi się szkolić i dobrze orientować w nowych rozwiązaniach i możliwościach rozwoju systemu;
- potrafić dobrze organizować i dokumentować pracę.

Administrator i użytkownicy systemów i sieci komputerowych muszą przyjąć do wiadomości, że nawet najlepiej zorganizowana struktura informatyczna w funkcjonującym przedsiębiorstwie posiada silne i słabe strony. Do tych najsłabszych zawsze należy człowiek.

ZAKOŃCZENIE

Manuel Castells napisał w swojej publikacji zatytułowanej *Społeczeństwo informacyjne i państwo dobrobytu* następujące słowa: „Żyjemy w czasach rozwoju społeczeństwa w jego różnych postaciach. Fundamentem tego społeczeństwa jest informacjonizm, co oznacza, że najważniejsze czynności we wszystkich dziedzinach ludzkiej aktywności opierają się na technologiach informacyjnych (IT), są zorganizowane (globalnie) w sieci informacyjne oraz skupione wokół przetwarzania informacji (symboli)”[216]. Internet jest tworem żywym, otwartym, nieustannie rozwijającym się i ulęgającym dynamicznym zmianom. Jest tak samo zmienny jak język, którym się posługujemy (można by pokusić się o stwierdzenie, że nawet podlegającym większym zmianom, niżeli zmiany językowe). Obecny wiek niesie mnóstwo nowości, rozwiązań, przełomowych „skoków technologicznych”, ale również wiele związanych z tym zagrożeń. Większość społeczeństwa jest aktywna zawodowo. Następuje przełom w zakresie zbierania, gromadzenia i przekazywania informacji. Komputer, Internet stają się narzędziami na wyciągnięcie ręki, źródłem dobrych, ale i niebezpiecznych informacji, przekazów, zachowań. Z sieci należy korzystać odpowiedzialnie, z zachowaniem zasad zdrowego rozsądku, ponieważ każdy nierozważny krok może spowodować eskalację zagrożeń płynących z wirtualnej rzeczywistości.

Internet jest odpowiedzią na pytanie, które nie zostało jeszcze postawione – twierdził Stanisław Lem. On też przestrzegał: kolejnym problemem, kto wie czy nie najfatalniejszym, jest fakt, że Internet otwiera wrota – jako ziemia opleciona siecią elektroniczną wyzbyta kontroli i centrów zwiadowczych – wszelkiej działalności – a zatem i takiej, która jest występna, a nawet zbrodnicza. Mafie, camorry, gangi, gangsterzy, oszuści i „imposterzy” wszelkiej maści uzyskują

[216] M. Castells, P. Himanen, *Społeczeństwo informacyjne i państwo dobrobytu*, przeł. M. Penkala, M. Sutowski, „Krytyka Polityczna” 2009, nr 17, s. 20.

wstęp na arenę informacji na równi z potencjalnymi Einsteinami. Technologie informacyjne zmieniły i nadal zmieniać będą, niekiedy w sposób radykalny, styl życia, pracy, edukacji i rozrywki. Zjawiska i procesy zachodzące w cyberprzestrzeni znacznie wybiegają poza wymiar techniczny, przyjmując charakter społeczny. Jesteśmy obecnie świadkami kształtowania się tzw. społeczeństwa informacyjnego, czyli – niezależnie od różnych prób jego definiowania – społeczeństwa o głębokich zmianach w świadomości społecznej, wywołanych skutkami rewolucji cyfrowej, oddziałującej wielowymiarowo (gospodarczo, politycznie, kulturowo, społecznie, itp.) na otaczającą rzeczywistość za pomocą informacji. Społeczeństwo to bywa również określane mianem społeczeństwa ryzyka, z uwagi na możliwe implikacje występujących w cyberprzestrzeni zagrożeń dla bezpieczeństwa pojedynczego człowieka oraz zbiorowości ludzkich.

Zasadniczym celem pracy było przeanalizowanie i usystematyzowanie zagrożeń związanych z cyberterroryzmem i przestępczością komputerową oraz ustalenie jakie rozwiązania (metody) należy zastosować w celu ochrony ich przed tymi zagrożeniami.

Przeprowadzając analizę problemów badawczych postawionych we wstępnej fazie pisania pracy w ocenie autora cel pracy został osiągnięty. Przeprowadzona analiza pozwoliła na zdefiniowanie i opisanie cyberterroryzmu oraz przestępczości komputerowej, w tym zagrożeń dotyczących infrastruktury krytycznej państwa. Analizie poddano metody przeciwdziałania zagrożeniom związanym z atakami w cyberprzestrzeni.

Potwierdziło się założenie **hipotezy roboczej, że** cyberterroryzm i przestępczość komputerowa stanowią zagrożenie dla państw, organizacji i instytucji oraz firm, a tym samym i obywateli. Zagrożenia te można identyfikować i poszukiwać nowoczesnych, skutecznych rozwiązań ich eliminacji. Do tych rozwiązań, które mogą zapewni**ć** odpowiedni poziom bezpieczeń**stwa informacyjnego (informatycznego)**, zaliczyć należy biometri**ę** i kryptografi**ę**. Także obowiązujące akty prawne w Polsce zapewniają odpowiedni poziom bezpieczeństwa informacyjnego, a instytucje odpowiedzialne za jego utrzymanie realizują zawarte w nich ustalenia i współpracują z Unią Europejską i NATO.

Przeprowadzona **analiza** zagrożeń cyberterroryzmu i przestępczości komputerowej pozwala stwierdzić, że biometria i kryptografia oraz profesjonalna administracja systemem informatycznym zapewniają skuteczną ochronę przed zagrożeniami i pozwalają zabezpieczyć organizacje, instytucje i firmy oraz użytkowników przed kłopotami i stratami finansowymi.

Drugą metodą badawczą zastosowaną w pracy była **synteza**. Metoda ta pozwoliła opracować wnioski generalizujące dotyczące zagrożeń, z jednoczesnym wskazaniem dostępnych na rynku rozwiązań, które mogą zapewnić bezpieczne korzystanie z systemów informacyjnych. Zastosowane metody badawcze pozwoliły na zdefiniowanie następujących wniosk**ów** generalizujących:

- **po pierwsze:** ważnym elementem przeciwdziałania cyberterroryzmowi i przestępczości komputerowej jest poznanie zagrożeń, ich analiza oraz poszukiwanie skutecznych sposobów zapobiegawczych i zapewniających bezpieczeństwo informacji;
- **po drugie:** współpraca i wymiana informacji o zagrożeniach cyberterrorystycznych i przestępczości komputerowej ze specjalistami zajmującymi się tą problematyką w Unii Europejskiej i NATO może pozwolić na skuteczną walkę z tymi zagrożeniami;
- **po trzecie:** potencjalne zagrożenia stwarzane przez cyberterroryzm i przestępczość komputerową wywołują potrzebę sprawnego działania nie tylko ekspertów (administratorów), lecz wszystkich użytkowników systemów teleinformatycznych;
- **po czwarte:** istniejące rodzaje działalności cyberterrorystycznej i przestępczości komputerowej wskazuj**ą** na realne możliwości zaatakowania nie tylko prywatnych, lecz również rządowych systemów teleinformatycznych, co może spowodować realne niebezpieczeństwo, jakim jest atak na infrastrukturę krytyczną państwa;
- **po piąte:** niezwykle ważne jest dokonanie diagnozy możliwości oraz potrzeb służb odpowiedzialnych za bezpieczeństwo państwa w obszarach przeciwdziałania cyberterroryzmowi i przestępczości komputerowej. Pozwoli to wyposażyć służby w narzędzia i środki oraz umiejętności do przeciwdziałania aktualnym zagrożeniom;
- **po szóste:** dostrzegając realny wzrost zagrożeń ze strony terrorystów działających w sieciach publicznych, od których całkowita separacja nie jest możliwa, a także fakt rozproszonej odpowiedzialności za bezpieczeństwo teleinformatyczne, niezbędnym jest wprowadzenie systemowych rozwiązań w zakresie ścigania i zapobiegania cyberterroryzmowi i przestępczości komputerowej. Istniejące oraz na bieżąco doskonalone rozwiązania umożliwią szybkie i sprawne ujawnienie wszelkich zagrożeń oraz efektywne reagowanie na te zagrożenia;

- **po siódme:** korzystanie z Internetu oprócz korzyści stwarza również szereg zagrożeń. Każdy **użytkownik systemu teleinformatycznego zetknie się z nimi** wcześniej czy później, nawet jeśli będą one dla niego niezauważalne, dlatego ważne jest kształtowanie świadomości istnienia niebezpieczeństw w globalnej sieci oraz wskazywanie konieczności przeciwdziałania cyberzagrożeniom. Świadomość i wiedza na temat sposobów przeciwdziałania i zwalczania zagrożeń stanowią kluczowe elementy przeciwdziałania tym zagrożeniom;
- **po ósme:** niezmiernie ważny jest sposób zachowania użytkownika sieci – może on w dużym stopniu zminimalizować ryzyko wynikające z istniejących zagrożeń. Odpowiedzialność za bezpieczeństwo (w tym bezpieczeństwo informacji) w sieci spoczywa na każdym użytkowniku;
- **po dziewiąte:** celowym jest poznanie i zastosowanie rozwiązań, jakie stwarza obecnie biometria i kryptografia. Rozwiązania te zostały opisane w piątym i szóstym rozdziale tego opracowania;
- **po dziesiąte:** celowa jest identyfikacja potencjału infrastruktury teleinformatycznej, w tym sieci, systemów i programów komputerowych. Polegać to powinno na stworzeniu instytucji, która będzie dysponować aktualną bazą wiedzy o potencjale tych zasobów, które to mogą zostać wykorzystane w czasie zagrożenia, kryzysu czy wojny.
- **po jedenaste:** w systemow**ą** walkę z cyberterroryzmem konieczne wydaje się włączenie do współpracy podmiotów sektora prywatnego. Do grupy tej zaliczyć należy przede wszystkim operatorów i administratorów systemów telekomunikacyjnych i teleinformatycznych. Niezbędne jest jednak precyzyjne określenie obszarów odpowiedzialności oraz sposobów i form współdziałania, w szczególności:
  - ✓ współpraca w zakresie zapobiegania i zwalczania wszelkich form cyberterroryzmu i przestępczości komputerowej;
  - ✓ wspieranie działań zmierzających do ustalenia sprawców cyberterroryzmu i przestępczości komputerowej;
  - ✓ **ścisła współpraca i wymiana doświadczeń z przedstawicielami Unii Europejskiej i NATO;**
  - ✓ przekazywanie istotnych informacji dotyczących poważnych incydentów naruszenia bezpieczeństwa teleinformatycznego wykrytych we własnych systemach lub sieciach teleinformatycznych oraz o innych

istotnych faktach dla bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa;
- ✓ współpraca z organami ścigania w zakresie kontroli użytkowników sieci prowadzących działalność zagrażającą bezpieczeństwu sieciom i systemom komputerowym.

Bezpieczeństwo informacyjne, w dobie rosnącego znaczenia zasobów informacyjnych jako zasobów strategicznych państwa, staje się jednym z najbardziej kluczowych obszarów, na których skupiona powinna być aktywność służb i instytucji odpowiedzialnych za bezpieczeństwo państwa. Należy podkreślić, iż cyberterroryzm i przestępczość komputerowa zagrażać może państwu na co najmniej trzech poziomach:

- naruszanie bezpieczeństwa informacji stanowiących zasób strategiczny państwa, co powoduje zachwianie zdolności państwa w dziedzinie zapewnienia stabilności społecznej, politycznej i gospodarczej oraz zapewnienia bezpieczeństwa państwa, jego interesów i obywateli,
- atak przeciwko systemom informacyjnym kontrolującym funkcjonowanie infrastruktury krytycznej państwa, co może pociągnąć za sobą zagrożenie dla fizycznego bezpieczeństwa obywateli i mienia państwowego oraz dla ciągłości funkcjonowania podstawowych elementów infrastruktury krytycznej,
- atak na poziomie walki psychologicznej, co mo**że** podważać zaufanie obywateli do sprawności i profesjonalności funkcjonowania państwa, jego agend, służb i instytucji, podważając tym samym legitymację rządu do sprawowania suwerennej władzy w państwie.

Wypracowywanie przez państwo odpowiednich algorytmów postępowania w obszarze bezpieczeństwa informacji, inwestowanie w systemy bezpieczeństwa informacyjnego, chroniące zasoby informacyjne państwa, pozwolą prowadzić skuteczną walkę informacyjną ze wszystkimi podmiotami, które temu bezpieczeństwu zagrażają.

Wyzwanie to jest tym poważniejsze, że cyberterroryzm, podobnie jak sam terroryzm, jest zjawiskiem dynamicznym, którego rozwój i ewolucję dodatkowo wspiera ciągłe wzbogacanie narzędzi walki informacyjnej. W tym kontekście rozwój i rozprzestrzenianie się narzędzi walki informacyjnej jest zjawiskiem, któremu dotrzymywać kroku muszą narzędzia i metody zarówno ofensywne, jak i defensywne stosowane przez państwa w obszarze ochrony jego bezpieczeństwa informacyjnego.

CONCLUSION

Manuel Castells wrote in his book "The information society and welfare state" that we live in times when the society develops in different forms. The basis of the society is informationalism, which means that the most important activities in all human areas are based on ICT, are organized globally in information networks and concentrated on information (symbols) processing[217].Internet is alive and open construct, continually developing and dynamically changing. It changes in the same way as our language (it is tempting to sat that it undergoes even more changes than a language). Our age brings many novelties, breakthroughs, technological advances but also threats. Most of the society is economically active. The is a breakthrough in collecting, storing and disseminating information. Computer, Internet have become propinquitous tools, sources of good but also dangerous information. Messages and behaviors[218]. The net should be searched through in a responsible way, with common sense. Any careless action can cause escalation of virtual threats.

Internet is the answer to the question which has not been asked yet, claimed Stanisław Lem. He also warned that the next, who knows if not the most fatal is the fact that Internet opens gates- the earth entwined with an electronic network deprived of control and reconnaissance centers – to any activity – i.e., criminal and murderous. Mafias, camorras, gangs, gangsters, crooks and impostors of every kind gain the access to information on a par with potential Einsteins. ICT has changed and they will in a dramatic way lifestyle, work, education and

[217] M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2009, nr 798, s. 99-116.

[218] M. Castells, P. Himanen, *Społeczeństwo informacyjne i państwo dobrobytu*, przeł. M. Penkala, M. Sutowski, „Krytyka Polityczna" 2009, nr 17 s. 20.

entertainment trends. Phenomena and processes in cyberspace significantly go beyond the technical dimension and have a social nature. We are witnessing the process of the information society formation, thus- independently of attempts of defining it – formation of the society with deep changes in awareness resulting from digital revolution, having thanks to information multidimensional impact (economic, political, cultural, social) on the surrounding reality. Ulrich Beck named the society the risk society as it is affected by threats also in cyberspace. These threats affect an individual and societies.

The main aim of this book is to analyze the literature, provide deeper insight into threats of cyberterrorism, cybercrime and identify what solutions (methods) can be used to protection information against them.

In the Author's opinion the aim of the research has been completed. The analysis of the literature has resulted in defining and describing cyberterrorism and cybercrime and threats to the state critical infrastructure. The methods of preventing cyberattacks have been also analyzed.

The hypothesis is verified positively. Cyberterrorism and cybercrime pose a threat to states, organizations, institutions, companies and citizens. These threats can be identified and new, effective solutions (biometrics, cryptography) can be adopted to provide the expected level of information and computer security. The existing legal acts in Poland support the expected level of information security and the institutions responsible for information security implement them and cooperate with EU and NATO.

The analysis of cyberterrorism and cybercrimes leads to the conclusion that the biometric methods, cryptographic techniques and professional administration of information systems security can fight the frets effectively and protect organizations, institutions, companies and users against troubles and financial loss. The book includes also the analysis of the legal acts and regulations for ensuring an adequate level of information systems security.

The second method used in the research was synthesis to elaborate general conclusions about threats and indicate available solutions which ensure the secure information systems exploitation. The general conclusions drawn include:

- Firstly, the crucial element of cyberterrorism and cybercrime prevention is identification of threats, their analysis and looking for the effective preventive methods and methods that ensure the information security;

- Secondly, cooperation and exchange of information among experts about cyberterrorism and cybercrime threats in EU and NATO should foster the effective countering them;
- Thirdly, potential cyberterrorism and cybercrime threats require effective actions of not only experts (administrators) but all ICT users;
- Fourthly, the present cyberterrorism and cybercrime activities demonstrate potential capacity to attack not only private but also state ICT systems, which can cause the real threat to the state critical infrastructure;
- Fifthly, it is of top importance to identify the capacity and needs of security and cybersecurity services to equip them in an adequate means, tools and skills to prevent present threats;
- Sixthly, as a real increase in cyberterrorist incidents in public networks which cannot be separated completely and simultaneously scattered responsibility for ICT security are being observed, it is necessary to implement systemic solutions to prevent and fight cyberterrorism and cybercrime. The already implemented solutions and developed ones support quick and effective identification and effective response to any threats;
- Seventhly, Internet along with the benefits creates a lot of threats. Every ICT user will sooner or later face the threats even if they are unnoticeable. Therefore, it is crucial to shape awareness about the threats in a global network and necessity to prevent cyberthreats. Awareness and knowledge about prevention and fighting this threat are key elements of prevention;
- Eighthly, Network users' behaviors are extremely important - they can minimize risks to a great extent. Every user is responsible for security (including information security) in a network;
- Ninthly, it is reasonable to learn about and apply biometric and cryptographic solutions. They are described in chapter 5 and 6 in that book;
- Tenthly, it is reasonable to identify ICT infrastructure capacity: networks, systems, computer applications. For that purpose, the institutions should be established, which will collect updated database about the capacity of these assets potentially targeted during a crisis or war;
- Eleventhly, the systemic cyberterrorism prevention should include private sector stakeholders: operators and administrators of ICT systems. However, it is crucial to precisely define the areas of responsibility and forms of cooperation, especially:

- ✓ cooperation for prevention and countering any forms of cyberterrorism and cybercrime;
- ✓ Supporting actins that aim at identifying cyberterrorists and cybercriminals;
- ✓ Close cooperation and exchange of good practice with the EU and NATO;
- ✓ Exchanging important information about the incidents in ICT systems security identified in our systems, networks and about other facts important for state ICT infrastructure;
- ✓ Cooperation with law enforcement bodies to control network users whose activity threatens ICT systems security.

Information security in times of growing importance of information assets as a strategic state asset is becoming one of the key areas the security services and institutions responsible for state security concentrate on. It should be emphasized that cyberterrorism and cybercrimes threaten the state security on three levels:

- Violation security of information which is a strategic asset, which results in incapability of the state to assure the social, political, economic stability and single citizens safety;
- Attacks against information systems which control state critical infrastructure. They can threaten citizens' physical security, state assets and continuity of functioning of basic critical infrastructure elements;
- Attacks which are elements of the psychological warfare. Thay can damage the citizens' trust to state's institutions, agendas and services, questioning this way the state legitimacy.

Elaborating algorithms and procedures for security information, investments in information security systems that protect information assets of the state will support effective measures taken against entities that threaten security. This is a very serious challenge as the cyberterrorism like terrorism itself is dynamic and evolving and supported by continuously developing information warfare tools. For that reason, development of offensive and defensive information warfare methods and tools applied by a state should keep pace with the development and spread of information warfare tools.

BIBLIOGRAFIA

Akty prawne:

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2010 R. Nr 182, poz. 1228).

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2004 r. Nr 171, poz. 1800).

Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie. podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. z 2011 r. Nr 159, poz. 948).

Rozporządzenie Rady Ministrów z dnia 1 czerwca 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych (Dz. U. z 2010 r. Nr 114, poz. 765).

Rozporządzenia Rady Ministrów z dnia 20 maja 2012 r. w sprawie bezpieczeństwa fizycznego informacji niejawnych (Dz. U. z 2012 r., poz. 683).

Normy dotyczące bezpieczeństwa informacji:

PN - I - 13335 - 1:1999 – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych.

PN - I - 13335 - 2 :2003 – Zarządzanie i planowanie bezpieczeństwa systemów informatycznych.

PN - I - 13335 - 3 :2003 – Techniki zarządzania bezpieczeństwem teleinformatycznym.

PN - ISO/IEC - 27002:2005 – Technika informatyczna. Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji.

PN - ISO/IEC - 27001:2007 – Technika informatyczna – Technika bezpieczeństwa – System zarządzania bezpieczeństwem informacji.

Literatura:

Andrzejkowicz M., *Możliwości wzbogacenia biometrycznej analizy chodu*, Konferencja Naukowa *Postępy w technice biometrycznej*, Biometria 2002.

Bankowość elektroniczna i biometryczna – stan i perspektywy. Opracowanie: Departament Bankowości Internetowej i Mobilnej w Banku BPS S.A. Październik 2016.

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Wydawnictwo Adam Marszałek, Toruń 2006.

Bieniok H., *Sztuka komunikowania się, negocjacji i rozwiązywania konfliktów,* AE, Katowice 2005.

Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wydawnictwo Wyższej Szkoły Cła i Logistyki, Warszawa 2011.

Bógdoł-Brzezińska A., Gawrycki M., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Oficyna Wydawnicza Aspra, Poznań 2003.

Cieślar P., *Operacje i techniki operacyjne*, AON, Warszawa 2009.

Cheswick W.R., Bellovin S.M., *Firewalls and Internet Security: Repelling the Wily Hacker*, Reading 1991.

Czermiński J., *Budowanie systemu informacji strategicznej,* Wydawnictwo Dom Organizatora, Toruń-Gdańsk 2002.

Infrastruktura Teleinformatyczna Państwa, Praca nr: 10300038, Państwowy Instytut Badawczy – Instytut Łączności, Zakład Zastosowań Technik Łączności Elektronicznej (Z–10), Warszawa 2008.

Darczewska J., *Anatomia rosyjskiej wojny Informacyjnej. Operacja krymska – studium przypadku,* „Punkt Widzenia" 2014, nr 42, OSW.

Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*, WNT, Warszawa 2002.

Denning D. E., *Wojna informacyjna i bezpieczeństwo informacji*, WNT, Warszawa 2002.

Długosz J., *Nowoczesne technologie w logistyce,* wyd. PWE, Warszawa 2009.

Flakiewicz W., *Informacyjne systemy zarządzania, Podstawy budowy i funkcjonowania*, PWE, Warszawa 1990.

Grabowska M., *O komunikowaniu dawniej i dziś. Lekcja biblioteczna*, „Biblioteka" 2011, nr 3.

Gierszewska G., Romanowska M., *Analiza strategiczna przedsiębiorstwa,* Państwowe Wydawnictwo Ekonomiczne, Warszawa 1994.

Grzywna Z., *Bezpieczeństwo – Ujęcie kompleksowe*, wyd. UKiP J&D Gądka, Gliwice 2012.

Grzywna Z., Grzywna A., *Zarys bezpieczeństwa z uwzględnieniem infrastruktury krytycznej*, wyd. UKiP J&D Gądka, Gliwice 2011.

Gomółka Z., Twaróg B., Żesławska E., *Identyfikacja tożsamości z wykorzystaniem analizy geometrii dłoni*, „Edukacja – Technika – Informatyka" 2016, nr 4(18), s. 419-424.

Grudzewski W. M., Hejduk I. K., *Zarządzanie wiedzą w przedsiębiorstwach* , Difin, Warszawa 2004.

Hoc S., Szewc T., *Ochrona danych osobowych i informacji niejawnych*, wydanie 2, G.H. Beck, Warszawa 2014.

Informatyka ekonomiczna, E. Niedzielska (red.) Wydawnictwo AE im. Oskara Langego we Wrocławiu, Wrocław 1998.

Infrastruktura Teleinformatyczna Państwa, Praca nr: 10300038, Państwowy Instytut Badawczy – Instytut Łączności, Zakład Zastosowań Technik Łączności Elektronicznej (Z–10), Warszawa 2008.

Jaworska M., *Przegląd technik kryptograficznych w zabezpieczeniu urządzeń elektronicznych.* Portal branżowy Elektronika B2B.

Jańczak J., *Systemy analityki biznesowej narzędziem wspomagającym procesy decyzyjne w logistyce wojskowej*, AON, Warszawa 2012.

Janczak J., Nowak A., *Bezpieczeństwo informacyjne – wybrane problemy*, AON, Warszawa 2013.

Jabnoun N., Sahraoui S., *Enabling a TQM structure through information technology*, „Competitiveness Review" 2004, nr 1-2, American Society for Competitiveness, Pittsburg.

Jabłoński M., Radziszewski T., *Bezpieczeństwo fizyczne i teleinformatyczne informacji niejawnych*, PWN, Warszawa 2013.

Jasiński F., Narojek M., Rakowski P., *Wewnętrzne i zewnętrzne aspekty współpracy antyterrorystycznej w Unii Europejskiej w kontekście Polski, jako państwa członkowskiego*, Centrum Europejskie – Natolin, Warszawa 2006.

Kosiński J., Kmiotek S., *Międzynarodowa współpraca w zwalczaniu cyberprzestępczości,* w: *Cyberterroryzm – nowe wyzwania XXI wieku*, T. Jemioła, J. Kisielnicki, K. Rajchel (red. nauk.), Warszawa 2009.

Kaszubski R.W., *Biometria w bankowości i administracji publicznej*, praca zbiorowa pod redakcją R. W. Kaszubskiego, Związek Banków Polskich, Warszawa 2009.

Kasprowski P., Ober J., *Zastosowanie systemu pomiaru ruchu oka w biometrii*, Konferencja Naukowa *Postępy w technice biometrycznej*, Biometria 02.

Kisielnicki J., Sroka H., *Systemy informacyjne biznesu. Informatyka dla zarządzania*, Placet, Warszawa 2005.

Kisielnicki J., Sroka H., *Systemy informacyjne biznesu. Informatyka dla zarządzania*, Placet, Warszawa 2005.

Kowalski J., Kowalski M., *Polityka bezpieczeństwa informacji w praktyce*, Presscom Sp. z.o.o., Wrocław 2014.

Koblitz N., *Wykład z teorii liczb i kryptografii*, Wydawnictwa Naukowo-Techniczne, Warszawa 1996.

Kowalczyk E., *O istocie informacji*, wyd. WKŁ, Warszawa 1981.

Kral P., *Dane osobowe w firmie instrukcja przetwarzania z wzorcową dokumentację*, ODDK, Gdańsk 2014.

Kuck J., *Logistyka dziś i jutro*, Państwowa Wyższa Szkoła Techniczno-Ekonomiczna, Jarosław 2022.

Kutyłowski M., Strothmann W-B., *Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych*, , Read Me, Warszawa 1998.

Kuck J., *Nowoczesne technologie w logistyce,* AON, Warszawa 2013.

Kuck J., *Nowoczesność, efektywność i bezpieczeństwo współczesnej logistyki*, AON, Warszawa 2014.

Kuck J., *Nowoczesne rozwiązania do wsparcia procesu zarządzania logistyką w resorcie obrony narodowej*, w: *Innowacje w zarządzaniu procesami logistycznymi sił zbrojnych*, Jałowiec T., Nyszk W. (red. nauk.), AON, Warszawa 2012.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych,* PWN, Warszawa 2008.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*. Wyd. Adam Marszałek, Toruń 2006.

Lissowski G., hasło *Informacja*, w: *Wielka Encyklopedia Powszechna*, wyd. PWE, Warszawa 2002.

Maik R., Gołoś A., Szczerbacz K., Walkiewicz P. *Strategiczne źródła informacji w działalności przedsiębiorstw*, PARP, Warszawa 2010.

Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, w: *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, Terlikowski M. (red.), Wydawnictwo PISM, Warszawa 2009.

Nabrdalik S., *Bezpieczeństwo systemów i sieci teleinformatycznych w świetle ustawy o ochronie informacji niejawnych*, w: *Współczesne zagrożenia w zarządzaniu i bezpieczeństwie*, Kuck J. (red.), Tom I. Wyd. UKiP J&D Gębka, Katowice 2014.

Niedziejko P., Krysowaty I., *Biometria. Charakterystyka danych człowieka i ich wykorzystanie w bezpieczeństwie*, „Zabezpieczenia" 2006, nr 4; 2007, nr 1.

Nowak A., *Zarządzanie bezpieczeństwem informacyjnym,* AON, Warszawa 2010.

Stallings W., *Kryptografia i bezpieczeństwo sieci komputerowych*, Wyd. Helion, Gliwice 2012.

Madej M., Terlikowski M., *Bezpieczeństwo Teleinformatyczne*, Podlaska Spółka Produkcyjno-Handlowo-Usługowa, Warszawa 2009.

Nowak A., Schefers W., *Zarządzanie bezpieczeństwem informacyjnym*, AON, Warszawa 2010.

O'Brien J.A., *Management Information Systems. A Managerial End User Perspective*, Irwin, Homewood Ill, Boston 1990.

Linebarger P.M.A., *Wojna psychologiczna*, Warszawa 1954.

Potejko P., *Bezpieczeństwo informacyjne*, w: *Bezpieczeństwo państwa*, K. A. Wojtaszczyk, A. Materska-Sosnowska (red.), Oficyna Wydawnicza ASPRA-JR, Warszawa 2009.

Pomykała M., *Instytucjonalno-prawne podstawy przeciwdziałania cyberterroryzmowi*, w: *Cyberterroryzm – nowe wyzwania XXI wieku*, T.Jemioła, J. Kisielnicki, K. Rajchel (red.), WSIZiA, Warszawa 2009.

Społeczeństwo informacyjne, praca zbiorowa pod red. S. J. Nowak, G. Bliźniuk, PTI-Oddział Górnośląski, Katowice 2005.

Ross J.W., Weill R., Robertson D.C., *Architektura korporacyjna jako strategia*, wyd. Studio Emka, Warszawa 2010.

Samól D., Kuck J,. *Współczesne metody wsparcia informatycznego dla logistyki, kadr i finansów*, w: *Perspektywy informatyzacji logistyki wojska polskiego*, „Logis. Wewn." 2006, nr 4.

Strzoda M., *Zarządzanie informacją w organizacji,* AON, Warszawa 2004.

Sienkiewicz P., *25 wykładów*, AON, Warszawa 2013.

Siwicki M., *Cyberprzestępczość*, Wyd. C.H. Beck, Warszawa 2013.

Shinder D.L, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Helion, Gliwice 2004.

Studium Realizowalności Zintegrowanego Systemu Informatycznego Resortu Obrony Narodowej (ZSI ON), t. 1. *Model ogólny systemu* (STD-01), SG WP, Warszawa 2005.

Szaniawski K., *Informacja*, w: *Filozofia a nauka*, *wyd. PWE, Warszawa* 1987.

Schneier B., *Kryptografia dla praktyków*. wyd. WNT, Warszawa 1996.

Szpyra R., *Militarne operacje informacyjne*, AON, Warszawa 2003.

Stinson D., *Kryptografia w teorii i praktyce*, wyd. PWN, Warszawa 2021.

Stallings W., *Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji*, wyd. Helion, Gliwice 2012.

Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem,* wyd. Oficyna a Wolters Kluwer business, Warszawa 2010.

Sopińska A., *Rola systemu informacyjnego w procesie zarządzania strategicznego*, w: *System Informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*, M. Romanowska, R. Borowiecki (red.), Difin, Warszawa 2001.

Strzoda M., *Zarządzanie informacją w organizacji,* AON, Warszawa 2004.

Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe" Akademii Marynarki Wojennej 2005, rok XLVI, nr 1 (160).

Świątkowska J., Bunsch I., *Cyberterroryzm – nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI*, http://ik.org.pl/pl/.

Trejderowski T., *Kradzież tożsamości. Terroryzm informatyczny. Cyberprzestępstwa. Internet. Telefon. Facebook,* Eneteia, Wydawnictwo Psychologii i Kultury, Warszawa 2013.

Wrzosek M., *Procesy informacyjne w zarządzaniu organizacją zhierarchizowaną*, AON, Warszawa 2010.

Strony internetowe:

https://www.komputerswiat.pl/recenzje/sprzet/komponenty-pc/zarys-historii-nosnikow-informacji-czesc-pierwsza-wczoraj/w4peyq2

https://www.bing.com/search?q=informacja&form=ANSPH1&refig=792fd7d423674e7e9be7cb9d9936f537&pc=U531

https://www.scribd.com/document/49766365/wstep-do-teorii-informacji

https://mfiles.pl/pl/index.php/Warunki_efektywnej_komunikacji

http://www.silesia.org.pl/upload/Nowak_Jerzy__Spoleczenstwo_informacyjnegeneza__i_definicje. pdf

https://www.bing.com/search?q=10+inicjatyw+w+celu+rozwoju+nowoczesnych+technik+teleinformacyjnych+w+zakresie%3A+&form=ANSPH1&refig=1A43EA29F02C44B9AC243173D4AC582A&pc=U531

http://www.uci.agh.edu.pl/uczelnia/tad/PSI11/art/Dane_informacje_wiedza.pdf

https://mfiles.pl/pl/index.php/Dane

https://czakalaka.pl/informacja-definicja-charakterystyka-rodzaje/

http://pl.wikipedia.org/wiki/Strategia_organizacji

http://mfiles.pl/pl/index.php/System_informacji_strategicznej

http://tvn24bis.pl/wiadomosci-gospodarcze,71/oto-22-strategicznych-spolek-rzad--poznal-ich-liste,456522.html
http://www.parp.gov.pl/index/more/14837
https://pl.psichiatria.org/wp-content/uploads/2018/09/piramida-maslowa2-300x225.png
http://rocznikikae.sgh.waw.pl/p/roczniki_kae_z29_30.pdf
https://ochrona-bezpieczenstwo.pl/ochrona-informacji/prawo/846-bezpieczenstwo-informacyjne-panstwa-pozyskiwanie-informacji-i-kontroling-w-systemie-zarzadzania-kryzysowego-w-panstwie.
https://magazynprzedsiebiorcy.pl/audyty-it
https://pl.wikipedia.org/wiki/Infrastruktura_informatyczna
http://www.awronka.nazwa.pl/bazya/wojnainfor.htm
http://pl.wikipedia.org/wiki/Manipulacja_(psychologia)
http://pl.wikipedia.org/wiki/Propaganda
http://pl.wikipedia.org/wiki/Wywiad_(instytucja)
http://pl.wikipedia.org/wiki/Haker_(slang_komputerowy)
http://pl.wikipedia.org/wiki/Z%C5%82o%C5%9Bliwe_oprogramowanie
http://www.bankier.pl/wiadomosc/Strony-GPW-i-prezydenta-zaatakowane-przez-CyberBerkut-7217306.html
http://tech.wp.pl/kat,130068,title,Panstwo-Islamskie-zaatakowalo Newsweeka, wid,17251140,wiadomosc.html?ticaid=114bea
https://sobieski.org.pl/cybernetyczny-wymiar-wojny-rosyjsko-ukrainskiej/
https://www.dw.com/pl/ukrai%C5%84ska-partyzantka-w-cyberprzestrzeni-jak-hakerzy-atakuj%C4%85-rosj%C4%99/a-61273452
https://www.gov.pl/web/sluzby-specjalne/wzrasta-liczba-cyberatakow
https://www.iso.org.pl/uslugi-zarzadzania/wdrazanie-systemow/systemy-bezpieczenstwa-informacji/iso-27001/
http://www.wywiad-gospodarczy.pl/2.html
http://pl.wikipedia.org/wiki/Analiza_ryzyka
http://pl.wikipedia.org/wiki/Test_penetracyjny
http://www.wywiad-gospodarczy.pl/3.html
http://www.wywiad-gospodarczy.pl/2_1.html
http://www.wywiad-gospodarczy.pl/2_2.html
http://www.wywiad-gospodarczy.pl/2_3.html
http://www.stosunkimiedzynarodowe.info/artykul,393,Zagrozenie_cyberterrory-zmem_a_polska_strategia_obrony_przed_tym_zjawiskiem,

https://www.gov.pl/static/mi_arch/media/3510/Slownik_pojec_SRT.pdf *Słownik pojęć strategii rozwoju transportu do 2020 roku*, Ministerstwo Transportu, Budownictwa i Gospodarki Morskiej, s. 26.
http://www.instalacje-instalacje.com.pl/teleinformatyczna.php
https://pl.wikipedia.org/wiki/
https://pl.wikipedia.org/wiki/Sie%C4%87_komputerowa
http://www.sieci.u2.pl/
https://pl.wikipedia.org/wiki/Oprogramowanie
http://pl.wikipedia.org/wiki/Informacja
http://pldocs.docdat.com/docs/index-117214.html
https://www.gov.pl/web/rcb/infrastruktura-krytyczna
https://www.computerworld.pl/news/7-cech-ktore-kazdy-specjalista-IT-posiadac-powinien,348062.html
https://ena.lpnu.ua:8443/server/api/core/bitstreams/d4941166-d688-45ba-b999-47074d966d07/content
https://www.bing.com/search?q=The+Internenational+Partnership+Against+Cyber+Threats+%28IMPACT%29+z+siedzib%C4%85+w+Malezji&qs=ds&form=QBRE
http://europa.eu/rapid/press-release_IP-13-13_pl.htm
https://www.cybsecurity.org/pl/9-faktow-o-dyrektywie-nis-ktore-powinienes-znac/
https://www.cybsecurity.org/wp-content/uploads/2016/08/DyrektywaNISodc3. png
http://e- terroryzm.pl/archiwum/, nr 8/2012, s. 38.
https://pl.wikipedia.org/wiki/Zabezpieczenie_biometryczne
https://www.bing.com/search?q=linie+papilarne+identyfikacja&form=ANSPH1&refig=3b0a4e2dbf2a4fda92a71e6e13a9a8de&pc=U531
https://pl.wikipedia.org/wiki/Linie_papilarne
https://www.bing.com/
https://www.bing.com/images/search?q=%c5%bby%c5%82y+R%c4%99ki&form=RESTAB&first=1
https://biosys.pl/media/images/twarz-kobiety-biometria.width-1170.jpges
https://ichef.bbci.co.uk/news/466/amz/worldservice/live/assets/images/2010/03/02/100302093657_1.jpg
https://www.researchgate.net/figure/a-The-truncated-cone-body-model-b-Joint-positions-c-Kinematic-tree_fig1_220866810
https://zabezpieczenia.com.pl/images/old/stories/zdjecia_artykuly/biometria/2/9_biometria_ucho.jpgs
https://kurs-na-funta.pl/informacje/wp-content/uploads/2021/04/biometrics-eye--1024x683.jpg

https://i0.wp.com/www.info24service.com/wp-content/uploads/Fremde--Gene_2019-065-0000.png?ssl=1
http://www.kamery.pl/storage/arty/zasada_biometria.jpg
https://www.bing.com/search?q=skaner+linii+papilarnych&form=ANSPH1&refig=dbb 595696ccc419e87501ac08ef29a74&pc=U531
https://www.bing.com/images/search?q=Paszport+Polski&form=RESTAB&first=1
https://economic-historian.com/wp-content/uploads/2021/03/20131011082040 telegraph-470.jpg
https://www.slideserve.com/stella/maszyny-szyfruj-ce
https://i.pinimg.com/originals/40/16/22/401622b5813bb403710fb797298949d2.jpg, https://www.bing.com/search?q=znakikanji&form=ANNTH1&refig=b5bce915ab1543e9849dda05933f5bd4
https://image2.slideserve.com/ 4562172/ko-o-szyfrowe-n.jpg https://pl.abcdef.wiki/wiki/Alberti_cipher
https://www.bing.com/search?q=Dysk+szyfrowy+Albertiego&form=ANSPH1&refig=b0ae363f56b44c5cba8af8adb30062bd&pc=U531
http://pl.wikipedia.org/wiki/Strona_g%C5%82%C3%B3wna
https://www.szkolneblogi.pl/static/media/users/private/JASIENICA/szyfr-czekolada_sko_thumb.jpg
https://pl.wikipedia.org/wiki/Szachownica_Polibiusza
Źródło:https://www.bing.com/images/search?q=Szyfr+Vigen%c3%a8re%e2%80%99A&form=RESTAB&first=1
https://pl.wikipedia.org/wiki/Szyfr_Cezara
https://www.lo69.pl/liceum/strony/obraz/album/rot13.png
https://bi.im-g.pl/im/da/fd/18/z26 202842 AMP,Przewozna-radiostacja-Marconi-YB1--podstawowe-wypo.jpg
https://www.slideserve.com/stella/maszyny-szyfruj-ce
https://www.bing.com/images/search?q=enigma&qpvt=Enigma&form=IQFRML&first=1
https://www.slideserve.com/stella/maszyny-szyfruj-ce
https://www.slideserve.com/stella/maszyny-szyfruj-ce
http://pl.wikipedia.org/wiki/Strona_g%C5%82%C3%B3wna
http://pl.wikipedia.org/wiki/Strona_g%C5%82%C3%B3wna
https://www.slideserve.com/stella/maszyny-szyfruj-ce https://pl.wikipedia.org/wiki/Enigma
https://wazniak.mimuw.edu.pl/images/0/0f/Bsi_04_wykl.pdf https://pl.wikipedia.org/wiki/Kryptologia#Historia_kryptografii_i_kryptoanalizy
https://wazniak.mimuw.edu.pl/images/0/0f/Bsi_04_wykl.pdf

https://pl.wikipedia.org/wiki/Steganografiaeganografia
https://www.soczko.pl/iod-soczko-partnerzy/blog-ochrona-danych/integralnosc-poufnosc/
https://i0.wp.com/www.diwebsity.com/wp-content/uploads/2019/11/15.Symetryczne.png ?resize=768%2C420&ssl=1
https://pl.wikipedia.org/wiki/Alternatywa_roz%C5%82%C4%85czna
https://wykop.pl/cdn/c3201142/comment_eaL5OHTHsNLzgYztL3HrcvnbmJjsHfoV.jpg https://www.bing.com/search?q=firmware&form=ANSPH1&refig=21f78294364c4711b60eced3f1a4c370&pc=U531&sp=1&qs=AS&pq=firmware&sc=10-8&cvid=21f78294364c4711b60eced3f1a4c370
https://www.epuzzle.info/es/rompecabezas/jugar/tecnolog%C3%ADa/115468-tarjeta-de-cr%C3%A9dito#16x10
https://pl.wikipedia.org/wiki/CrypTool
https://medium.com/@markmuskardin/not-your-keys-not-your-crypto-373945c8d46d
https://odo24.pl/blog-post.obowiazki-administratora-systemow-informatycznych
https://odo24.pl/blog-post.obow
Wszechobecna kryptografia Serwis Akademii GórniczoHutniczej (agh.edu.pl).

ISBN 978-83-65823-64-9