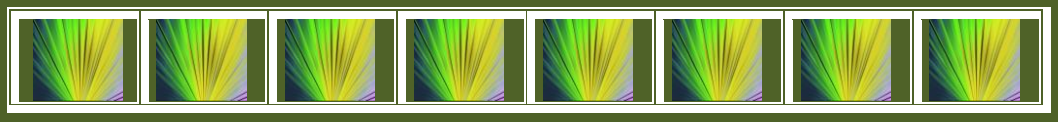
Władysław Wornalkiewicz

Wstęp do zagadnienia

„BEZPIECZEŃSTWO TELEINFORMATYCZNE I CYBERBEZPIECZEŃSTWO”



2024

Władysław Wornalkiewicz

Wstęp do zagadnienia

„BEZPIECZEŃSTWO TELEINFORMATYCZNE I CYBERBEZPIECZEŃSTWO”

Dnipro 2024

ISBN 978-617-627-177-2

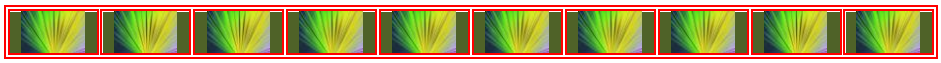
Zatwierdzone na posiedzeniu Rady Naukowej
Wydziału Humanistyczno-Ekonomicznego
Państwowego Uniwersytetu Pedagogicznego w Berdiańsku (Zaporoże)
protokół nr 6 (26.02.2024 r.)

Władysław Wornalkiewicz. *Wstęp do zagadnienia „Bezpieczeństwo teleinformatyczne i cyberbezpieczeństwo”***.** Monografia. Dnipro: Wydawca «Svidler A.L.», 2024. 145 s.

Autor ponosi pełną odpowiedzialność za tekst, cytaty i ilustracje.

Wydawca
Wydawca «Svidler A.L.»
zaświadczenie o wpisie do Państwowego Rejestru Podmiotów Wydawniczych:
Seria DK № 3876 z dnia 10.09.2010 r.
a/s 2493, Dnipro, 49041, tel. +38 (067) 635-78-83

Spis treści



Słowo wstępne 6

1. Wprowadzenie do zagadnienia „*Bezpieczeństwo teleinformatyczne i cyberbezpieczeństwo*” 8

1.1. Rewolucja informacyjna i informatyczna 8

1.2. Zmianki publikacyjne w Internecie dotyczące bezpieczeństwa teleinformatycznego 9

1.3. Istotność bezpieczeństwa informatycznego 12

1.4. Dostępność usług w zakresie pracy zdalnej i cyberbezpieczeństwa 17

1.5. Czuwanie i monitorowanie możliwości ataków na zasoby 18

1.6. System teleinformatyczny a informatyczny 19

2. Rodzaje i struktura budowy sieci teleinformatycznych stacjonarnych i mobilnych 22

2.1. Wstęp 22

2.2. Standardy sieci bezprzewodowych 23

2.3. Karty sieciowe i punkty dostępowe 25

2.4. Przykłady struktur sieci bezprzewodowych 26

2.5. Ochrona informacji w sieciach 28

2.6. Oferta budowy sieci bezprzewodowych i telefonii VoIP 29

2.7. Przykłady platform korzystających z sieci teleinformatycznych 31

3. Cyberprzestrzeń oraz zagrożenie ze strony sieci globalnych 35

3.1. Błędy we wdrażaniu systemów jako „*furtki*” do złośliwej interakcji 25

3.2. Bieżące czuwanie nad możliwością wystąpienia cyberzagrożenia infrastruktury krytycznej 37

3.3. Konieczność dokształcania służb w zakresie cyberbezpieczeństwa 38

4. Wytyczne przeciwdziałania atakom hakerskim w zakresie dostępu do baz danych 40
4.1. Budowa aplikacji z myślą o cyberbezpieczeństwie 40
4.2. Akty prawne regulujące bezpieczeństwo teleinformatyczne 41
4.3. Dyrektywa instytutu NIST i inne 43

5. Zakres działalności administratorów sieci i systemów w obszarze ochrony przed dostępem do zasobów oraz usług informatycznych 46
5.1. Szkolenia doskonalające umiejętności administratorów systemów 46
5.2. Odpowiedzialność firmy/instytucji za stan zabezpieczenia baz danych 48
5.3. Stosowane bazy danych 49
5.4. Narzędzia programistyczne logowania do usług komputerowych 51
5.5. Wspomaganie ochrony zasobów informatycznych poprzez instalowanie programów antywirusowych 52

6. Analiza przestrzeni programowej i działania sprzętu teleinformatycznego 55
6.1. Pojęcie „*złośliwe oprogramowanie*” 55
6.2. Kategorie *malware* 59

7. Metody i programy ochrony przed cyberprzestępczością 61
7.1. Strategie zabezpieczenia systemów 61
7.2. Zagadnienia bezpieczeństwa teleleinformatycznego 63
7.3. Tworzenie programu cyberbezpieczeństwa 63
7.4. Ślady literaturowe dotyczące ochrony przed cyberatakiem 64
7.5. Przykłady środków i programów zabezpieczenia przed włamaniem cyberprzestępców 67

8. Studium przykładów wystąpień hakerskich 72
8.1. Prace nad *Programowalnym Układem Scalonym* 72
8.2. Przykłady wykorzystania złośliwego oprogramowania do spowodowania zakłóceń w ruchu kolejowym 73
8.3. Rodzaje ataków hakerskich 74
8.4. Skutki dużych włamań do systemów 75
8.5. Ataki na systemy domowe 76

9. Słownik pojęć podstawowych z zakresu „*Bezpieczeństwa telekomunikacyjnego i cyberbezpieczeństwa*” 78

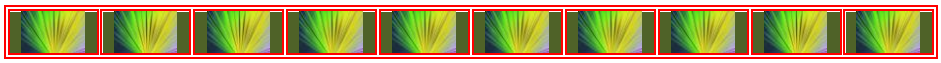
10. Prezentacja wykładów z przedmiotu: „*Bezpieczeństwa telekomunikacyjnego* 97

11. Moje wcześniejsze publikacje w latach 2008-2023 119

Bibliografia 145

Załącznik: Komplet prezentacji wykładów z przedmiotu „*Bezpieczeństwo teleinformatyczne i cyberbezpieczeństwo*” (dotyczy wersji elektronicznej)

Słowo wstępne



Analiza literaturowa i publikacji internetowych i nie tylko wykazała, że nieliczne są jeszcze opracowania dotyczące bezpieczeństwa teleinformacyjnego i cyberbezpieczeństwa. Podkreśla się zwłaszcza zagrożenia dla infrastruktury sieciowej i aplikacji jakie niesie za sobą dość szybkie zaangażowanie niektórych programistów w tworzenie złośliwego oprogramowania, zwanego *malware*. Przenika ono do struktur kodów pakietów programowych, rozwiązań hardwarowych i zarządzających sieciami komputerowymi oraz bazami danych. Wywołuje duże straty spowodowane zakłóceniami, a nawet występują niekiedy przerwania w pracy sieci lokalnych, jak też o szerszym zasięgu.

W takiej sytuacji, jak opracować w miarę syntetyczny podręcznik dla studentów kierunków *Zarządzanie*, *Logistyka*, czy też *Administracja dotyczący Bezpieczeństwa telekomumikacyjnego i cyberbezpieczeństwa*? Powinni oni nie tylko znać jak posługiwać się określonym programem „*antyhakerowym*", ale także jako przyszli managerowie procesu produkcji, czy usług z zastosowaniem techniki IT, znać podstawową terminologię wynikającą z zagrożenia w szeroko rozumianej Sieci. Istotna jest także znajomość aktów prawnych, które na niwie krajowej - polskiej, wzorowane są na wytycznych Unii Europejskiej, które traktowane są jako zalecenia dla państw stowarzyszonych. Ponadto, ci studenci studiów, zwłaszcza podyplomowych, którzy już pracują jako administratorzy sieci, baz danych obiektów powinni znać oczekiwania w tym zakresie, aby uchronić zgromadzone informacje elektroniczne i sprzęt komputerowy przed złośliwymi programistami (hakerami), którzy jeszcze niedawno pracowali w danej jednostce gospodarczej, usługowej czy administracyjnej.

Celem przewodnim tej pracy jest udostępnienie, przede wszystkim na podstawie zgromadzonej i wyselekcjonowanej wiedzy z publikacji sieci globalnej Internet, mojej wstępnej jeszcze nie opublikowanej, propozycji wykładów dotyczących przedmiotu „*Bezpieczeństwo teleinformatyczne i cyberbezpieczeństwo*". Opracowanie ma dwie wersje papierową i elektroniczną. W części tekstowej zaprezentowano tylko slajdy pierwszego wykładu „*Wprowadzenie*", natomiast do wersji elektronicznej dołączono załącznik z kompletem wykładów. Wykładem początkowym - zerowym jest „*Słownik pojęć*

podstawowych". Dalsze wykłady zasygnalizowane w prezentacji stanowią wypunktowanie zakresu problematyki objętej tą pracą i są następujące:

- *Rodzaje i struktura budowy sieci teleinformatycznych stacjonarnych i mobilnych,*

- *Cyberprzestrzeń oraz zagrożenia ze strony sieci globalnych,*

- *Wytyczne w zakresie przeciwdziałania atakom hakerskim w celu dostępu do bazy danych,*

- *Zakres działalności administratorów sieci i systemów w obszarze ochrony przed dostępem do zasobów oraz usług informatycznych,*

- *Analiza przestrzeni programowej i konfiguracji sprzętowej w celu zablokowania przed wejściem złośliwego oprogramowania,*

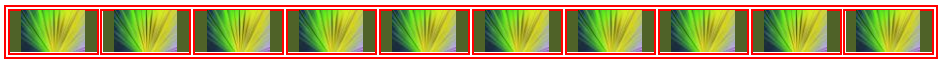
- *Metody i programy ochrony przed cyberprzestępczością,*

- *Studium przykładów wystąpień hakerskich i sposoby ich neutralizacji na przyszłość*.

Zdaję sobie sprawę, że przedstawione ramowo zagadnienie spotka się z ostrą oceną znawców szczegółów podjętej tematyki, ale proszę wziąć pod uwagę zaadresowanie tego opracowania jako pomocniczego podręcznika dla studiów zaocznych na kierunkach ekonomicznych. Jednak cenne uwagi oraz rozwinięcia merytoryczne podjęte przez Czytelników mogą być pomocne do dalszego udoskonalenia sugerowanego podręcznika i szerszego jego drugiego wydania.

Autor

1. Wprowadzenie do zagadnienia „*Bezpieczeństwo teleinformatyczne i cyberbezpieczeństwo*”



1.1. Rewolucja informacyjna i informatyczna

Rewolucja informacyjna (RI) to proces rozwoju społecznego, który zachodzi w rozwiniętych ekonomicznie i technologicznie państwach od II połowy XX wieku[1]. Jest on skutkiem szybkiego postępu w telekomunikacji, mikroelektronice, jak również w informatyce. W ramach rewolucji informacyjnej wyodrębnia się pojęcie rewolucji informatycznej. W obecnych czasach dostępu do aplikacji sztucznej inteligencji możemy skorzystać bezpłatnie z programu *ChatGPT* w wersji GPT-3.5. Zwróćmy uwagę jak elektroniczny asystent tej aplikacji formułuje pojęcie „*rewolucja informatyczna*”.

Rewolucja informatyczna to określenie, które odnosi się do dynamicznych zmian i rozwiązań rozwoju technologii oraz jej rozpowszechniania[2]*. Powodują istotny wpływ na życie społeczeństwa. Jest to proces, który rozpoczął się w drugiej połowie XX wieku i nadal trwa nieprzerwanie, przy czym wyróżnia się dwa podstawowe rozwiązania informatyczne:*

1. *Rozwój komputerów (ewolucja od dużych, kosztownych maszyn po komputery przenośne typu laptopy i urządzenia mobilne; umożliwiło to powszechne korzystanie z technologii IT).*

2. *Utworzenie sieci globalnej Internet i powszechność dostępu do zgromadzonej wiedzy w postaci zasobów elektronicznych.*

Rewolucja informacyjna charakteryzuje się komputeryzacją, rozbudową Internetu i łatwiejszym dostępem do informacji. Komputery, Internet i cyfrowe urządzenia komunikacyjne stały się integralną częścią życia ludzi i działalności różnych instytucji. Rewolucja informacyjna zmienia społeczeństwo, powodując powstanie nowych podziałów, zmiany w pracy i życiu człowieka. Informacja staje się głównym towarem rynkowym, a komputery zastępują rutynowe czynności intelektualne. Rewolucja informacyjna tworzy współczesną gospodarkę opartą na wiedzy i formułuje nowe społeczeństwo informacyjne.

[1] https://mfiles.pl/pl/index.php/Rewolucja_informacyjna
[2] Według zredagowanej edycyjnie przez autora odpowiedzi uzyskanej z programu *ChatGPT* - wersja GPT-3.5 (*chat.openai.com*) .

Wykorzystywanie Internetu pozwala na upowszechnianie pozyskiwania, przetwarzania i przesyłania informacji, która jest dostępna oraz ekspansji komunikacyjnej. Obserwujemy również jak przyspieszeniu i ułatwieniu ulega obieg wiedzy oraz idei[3].

Komputery, Internet, a także cyfrowe urządzenia komunikacyjne stały się integralnym elementem działalności firm, instytucji naukowych, urzędów, placówek oświatowych i opieki zdrowotnej, instytucji upowszechniania kultury, środków masowego przekazu. Technika komputerowa oraz technologia informacyjna przyczyniły się do usprawnienia, jak również poszerzenia możliwości działań we wszystkich niemalże aspektach ludzkiej aktywności. Impulsem do ekspansji rewolucji informatycznej jest cyfryzacja niemalże wszystkich obszarów działalności społeczności.

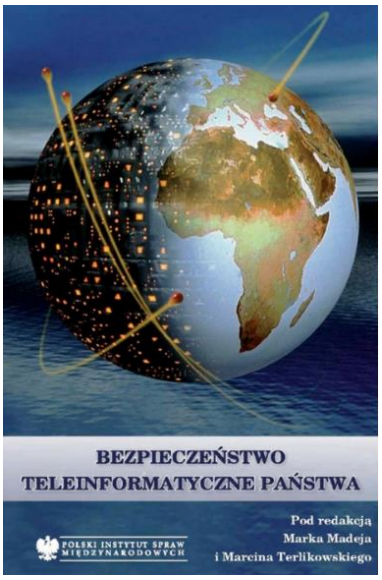
Rewolucja cyfrowa (informatyczna), zwana również *czwartą rewolucją przemysłową*, to kolejna epoka przemian spowodowanych rozwojem informatyzacji i nowoczesnych technologii[4]. Charakteryzują ją szybki postęp technologiczny, powszechna cyfryzacja i jej wpływ na wszystkie dziedziny życia. W związku z przemianami, jakie niesie za sobą rewolucja cyfrowa, wykształciła się, wspomniana już, nowa formacja społeczna, zwana społeczeństwem informacyjnym, dla którego strategicznym zasobem, zamiast kapitału i pracy, stała się wiedza. Rewolucja informatyczna prowadzi do bezprecedensowego przekształcenia globalnych rynków pracy, a świat stoi u progu zjawiska określanego przez niektórych jako "*gospodarka współużytkowania*"[5]. Nowe tryby pracy łączą pracowników z korporacjami na całym świecie w oparciu o wyrafinowane platformy informatyczne. Otwiera to nowe możliwości przede wszystkim przed programistami o wysokich kwalifikacjach w zakresie oprogramowania urządzeń mobilnych.

1.2. Wzmianki publikacyjne w zakresie bezpieczeństwa teleinformatycznego

Penetrując informacje internetowe dotyczące bezpieczeństwa teleinformatycznego Polski warto zwrócić uwagę na monografię zbiorową pod redakcją Marka Madeja i Marcina Terlikowskiego pt. „*Bezpieczeństwo teleinformatyczne państwa*", wydaną przez Instytut Spraw Międzynarodowych (zob. rysunek 1.1[6]. Monografię tę można potraktować jako wprowadzenie do zagadnień poprzedzających występujące coraz częściej zagrożenia z

[3] Zacher L. (1997), *Rewolucja informacyjna i społeczeństwo: niektóre trendy, zjawiska i kontrowersje*, „*Transformacje*", Warszawa.
[4] https://cyberpolicy.nask.pl/spoleczenstwo-informacyjne-w-czasach-cyfrowej-rewolucji-o-zjawisku-banki-informacyjnej-i-jego-nastepstwach/.
[5] https://www.worldbank.org/pl/news/feature/2014/11/06/poland-and-the-ict-revolution-are-we-there-yet.
[6] https://www.pism.pl/publikacje/bezpieczenstwo-teleinformatyczne-panstwa.

cyberprzestrzeni, niepokojące przede wszystkim administratorów sieci, jak też baz danych. Podkreślono w niej istotę, przejawy oraz wpływ rewolucji informatycznej na postrzeganie bezpieczeństwa państwa i systemu międzynarodowego. Ponadto zaznaczono znaczenie dla nowoczesnego państwa dominującej roli Internetu jako sieci globalnej. Specjalną uwagę poświęcono systemom teleinformatycznym, które służą systemowi płatniczemu Polski oraz roli jaką pełnią w walce informacyjnej.



Rys. 1.1. Strona tytułowa monografii „*Bezpieczeństwo teleinformatyczne państwa*”

Ze zjawiskiem bezpieczeństwa teleinformatycznego związanych jest szereg pojęć takich jak haking, haktywizm i cyberterroryzm. Ich określenia znalazły się we wspomnianej wcześniej monografii. Oprócz wymienionych na wstępie zagadnień w monografii „*Bezpieczeństwo teleinformatyczne państwa*” podjęto tematykę:

- monitoringu stanu bezpieczeństwa teleinformatycznego;
- kodowanie, szyfrowanie i integralność informacji elektronicznej;
- społeczeństwo informacyjne a problemy rozwoju *e-governmentu* w Polsce;
- inicjatywy Unii Europejskiej w zakresie bezpieczeństwa teleinformatycznego.

Rozwinięciem problematyki jest przedstawienie:

- konwencji o cyberprzestępczości,
- protokołu dodatkowy do *Konwencji o cyberprzestępczości* dotyczącego penalizacji czynów o charakterze rasistowskim, ksenofobicznym popełnionych przy użyciu systemów komputerowych.

Dążenie do zachowania bezpieczeństwa sieci, jak i zasobów cyfrowych obowiązuje szerokie gremium osób. Jednak np. polityk, decydując o przyjęciu strategii zapewnienia bezpieczeństwa narodowego w wymiarze teleinformatycznym, musi brać pod uwagę także techniczne możliwości wdrożenia proponowanych rozwiązań. Podobnie administrator sieci, dbający o stabilność nadzorowanego systemu, powinien pamiętać o szerszym kontekście wymogów bezpieczeństwa teleinformatycznego, np. konieczności ich pogodzenia z innymi priorytetami państwa w dziedzinie bezpieczeństwa narodowego.

Wspomniano tylko o jednej szerszej publikacji dotyczącej telebezpieczeństwa. Jednak w odniesieniu do cyberbezpieczeństw funkcjonujących systemów branżowych jak i lokalnych są także inne publikacje. Opracowania dotyczące problemów bezpieczeństwa teleinformatycznego nierzadko otwierają sugestywne opisy ataków na sieci komputerowe, prowadzących do poważnych zakłóceń sfer życia gospodarczego. Cyberterroryści bowiem mogą ingerować w eksploatowane systemy, uniemożliwić odbiór telewizji, a także zablokować funkcjonowanie Internetu. W tym obszarze niektórzy publikatorzy wysuwają katastroficzne scenariusze np. krachy giełdowe, blokowanie funkcjonowania banków.

Przypomnienia w środkach masowego przekazu o zagrożeniach ze strony hakerów nasilają się od czasu do czasu, zwłaszcza wtedy, gdy występują niepokojące wydarzenia, a przykładem może być Estonia. W ostatnich dniach kwietnia, już w roku 2007 roku, doszło do zaskakujących zakłóceń ruchu internetowego. Lawinowo wzrosła ilość danych przesyłanych pod określone adresy, głównie rządowe serwery z informacyjnymi witrynami WWW. Dość szybko doprowadziło to do ich przeciążenia, a w konsekwencji niedostępności portali estońskich instytucji rządowych dla użytkowników Internetu. W ciągu następnych kilku dni podobne ataki powtórzyły się, a ich siła gwałtownie wzrosła. W wyniku zalewu danymi w ilości kilkakrotnie większej niż maksymalna przepustowość estońskiej infrastruktury internetowej została ona praktycznie sparaliżowana.

W kilka miesięcy po tym wydarzeniu media na całym świecie donosiły o aktach cyberszpiegostwa – bezprecedensowej w swej skali kradzieży danych z komputerów wielu najważniejszych instytucji rządowych USA, włącznie z Pentagonem, zorganizowanej przez nieznaną grupę sprawców. Zainfekowanie komputerów złośliwym oprogramowaniem umożliwia bowiem przejęcie nad nimi kontroli i wykorzystanie ich zasobów do celów przestępczych. Temat aktów szpiegostwa wymierzonych przeciwko rządowym sieciom USA i innych państw, głównie sojuszników z NATO, powrócił w mediach światowych także na początku 2009 roku. Eksperci z Kanady zaprezentowali raport na temat grupy określającej

siebie nazwą GhostNet, która rzekomo zajmuje się „*zawodowo*" szpiegostwem komputerowym.

O narastających problemach w sferze bezpieczeństwa teleinformatycznego w mówi się także w Polsce. Media coraz częściej podejmowały choćby temat oszustw dotykających posiadaczy kont bankowych online. W kontekście wymienionych wydarzeń mówi się o bezpieczeństwie teleinformatycznym, a niekiedy informatycznym. Podejmowano próby klasyfikowania tych zdarzeń jako zagrożeń związanych z wykorzystywaniem technologii teleinformatycznych.

1.3. Istotność bezpieczeństwa teleinformatycznego

Wieloaspektowość i wielopłaszczyznowość zagadnienia *bezpieczeństwo teleinformatyczne* wynika z różnorodności i dużej liczby poziomów, na których należy je rozpatrywać. Może się ono bowiem odnosić do bardzo różnych podmiotów, począwszy od użytkownika indywidualnego – przez przedsiębiorstwa i instytucje, wykorzystujące w swej codziennej działalności całe sieci teleinformatyczne, aż po państwo, o rozległych sieciach spinających jego struktury administracyjne, organy i służby, a nawet całą gospodarkę.

Najbardziej rozpowszechnione określenia, często używane w odniesieniu do zagadnień bezpieczeństwa teleinformatycznego wykorzystywane wymiennie to bezpieczeństwo informacyjne (*information security*) i cyberbezpieczeństwo (*cybersecurity*).

Identyfikacja zagrożeń jest skomplikowanym wyzwaniem, towarzyszącym analizie problemów teleinformatycznych. Niektóre polegają na groźbie zniszczenia materialnych narzędzi służących do przechowywania, przetwarzania lub przesyłania cyfrowej informacji. Tego rodzaju niebezpieczeństwo może też być spowodowane klęskami żywiołowymi lub katastrofami technicznymi. Większość z zagrożeń bezpieczeństwa teleinformatycznego wiąże się jednak z działaniami prowadzonymi w cyberprzestrzeni, przy wykorzystaniu odpowiedniego sprzętu i oprogramowania. Wówczas negatywnemu oddziaływaniu poddawana jest sama informacja utrwalona w formie elektronicznej, a nie urządzenia służące do jej przechowywania i przetwarzania.

Złożoność problematyki bezpieczeństwa informatycznego utrudnia znalezienie cech wspólnych wszystkim zagadnieniom uznawanym za przynależne do tej dziedziny. Mimo to można przyjąć, że istotą bezpieczeństwa teleinformatycznego jest *zdolność określonego podmiotu do pozyskania i zachowania, w formie niezmienionej bez jego zgody i wiedzy, wszelkiego rodzaju informacji utrwalonej w postaci cyfrowej oraz możliwość jej bezpiecznego*

przetwarzania, przesyłania i upowszechniania. Bezpieczeństwo teleinformatyczne państwa w pewnej mierze zależy również od stanu ochrony komputerów i tym podobnych urządzeń znajdujących się w posiadaniu użytkowników indywidualnych. Bezpieczeństwo danych przechowywanych lub przesyłanych przez poszczególne jednostki z wykorzystaniem ich własnego sprzętu jest uzależnione także od poziomu odporności na rozmaite potencjalne ataki na infrastrukturę teleinformatyczną na szczeblu narodowym.

Wielowymiarowość zagadnień bezpieczeństwa teleinformatycznego oznacza też możliwość odmiennych interpretacji samej istoty tego wymiaru bezpieczeństwa. Inaczej mianowicie na kwestie bezpieczeństwa teleinformatycznego zareaguje administrator systemu przedsiębiorstwa, a inaczej wojskowy specjalista, koncentrujący się na zapewnieniu jednostkom wojskowym nieprzerwanej łączności. Warto w tym miejscu przytoczyć „*triadę*" warunków utrzymania bezpieczeństwa:

1. *Integralność* (spójność, nienaruszona struktura i treści informacji).
2. *Poufność* (zabezpieczenie informacji przed nieuprawnionym dostępem).
3. *Dostępność* (możliwości niezakłóconego skorzystania uprawnionych podmiotów do informacji)z perspektywy własnej specjalności).

Rozważając temat bezpieczeństwa teleinformatycznego zwróćmy jeszcze uwagę na przybliżenie oraz rozwinięcie tego pojęcia przez źródła internetowe.

Bezpieczeństwo teleinformatyczne to zbiór zagadnień z dziedziny telekomunikacji i informatyki związany z szacowaniem i kontrolą ryzyka wynikającego z korzystania z komputerów, sieci komputerowych i przesyłania danych do zdalnych lokalizacji, rozpatrywany z perspektywy poufności, integralności i dostępności[7]. Budowanie bezpiecznych systemów teleinformatycznych i aplikacji jest celem starań projektantów sieciowych i programistów. Konieczne jest opracowanie metod oceny bezpieczeństwa i kontrolowania zagrożeń. Mimo tych starań, ze względu na złożoność i czasochłonność wielu spośród proponowanych procesów, luki zabezpieczeń stanowią jednak poważny i wymierny problem dla użytkowników sieci teleinformatycznych.

Bezpieczeństwo teleinformatyczne nazywane również cyberbezpieczeństwem (*cybersecurity*) to zagadnienia związane z telekomunikacją oraz informatyką, które odnoszą się do ryzyk związanych z użytkowaniem komputerów, sieci komputerowych, czy Internetu. Dbając o bezpieczeństwo teleinformatyczne nie tylko chronimy gromadzone i przetwarzane dane, ale również zapewniamy bezpieczeństwo i ciągłość procesów biznesowych

[7] https://pl.wikipedia.org/wiki/Bezpiecze%C5%84stwo_teleinformatyczne.

wykonywanych w firmie[8]. Na cyberbezpieczeństwo należy patrzeć z perspektywy zapewnienia poufności, integralności oraz ograniczonej dostępności[9].

Cyberbezpieczeństwo dotyczy zabezpieczenia gromadzonych, przetwarzanych i udostępnianych informacji w formie elektronicznej przy użyciu różnych technik cyfrowych i wszelkich dostępnych narzędzi komunikacji elektronicznej[10]. Polega na zapewnieniu bezpieczeństwa systemów technologo informatycznej (IT) przedsiębiorstw w zakresie:

- danych;
- aplikacji i programów (systemy IT);
- systemów sieciowych IT;
- infrastruktury IT (komputery, serwery, sieć IT, komputery przemysłowe, smartfony);
- osób mających dostęp do elementów systemów teleinformatycznych przedsiębiorstwa.

Przytoczmy jeszcze fragment preambuły z Konwencjia Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie dnia 23 listopada 2001 roku[11].

„Państwa członkowskie Rady Europy i inne Państwa Sygnatariusze niniejszej konwencji,

- biorąc pod uwagę, że celem Rady Europy jest osiągnięcie większej jedności między jej członkami;

- uznając wartość wspierania współpracy z innymi Państwami Sygnatariuszami niniejszej konwencji;

- przekonane o potrzebie prowadzenia, jako kwestii priorytetowej, wspólnej polityki kryminalnej mającej na celu ochronę społeczeństwa przed cyberprzestępczością, między innymi poprzez przyjęcie właściwych przepisów prawnych i wspieranie międzynarodowej współpracy;

- świadome głębokich zmian dokonanych na skutek digitalizacji, konwergencji i trwającej globalizacji sieci informatycznych;

- zaniepokojone ryzykiem, że sieci informatyczne i informacje elektroniczne mogą być także wykorzystywane w celu popełniania przestępstw oraz że dowód w sprawie takich przestępstw może być przechowywany i przekazywany za pomocą tych sieci;

[8] https://twojepc.pl/news42344/Jak-zadbac-o-bezpieczenstwo-teleinformatyczne-w-firmie.html.
[9] (https://mindworkers.pl/bezpieczenstwo-teleinformatyczne-cybersecurity-czym-jest-oraz-jakie-sa-najwieksze-zagrozenia-w-2021-roku-dla-twojego-przedsiebiorstwa/).
[10] https://ccit.pl/bezpieczenstwo-informacji/.
[11] https://www.prawo.pl/akty/dz-u-2015-728,18197508.html.

- uznając potrzebę współpracy między państwami i przemysłem prywatnym w zwalczaniu cyberprzestępczości oraz potrzebę ochrony prawnie uzasadnionych interesów w stosowaniu i rozwoju technologii informatycznych;

- zdając sobie sprawę, że skuteczna walka z cyberprzestępczością wymaga zwiększonej, szybkiej i dobrze funkcjonującej współpracy międzynarodowej w sprawach karnych;

- przekonane, że niniejsza konwencja jest niezbędna dla powstrzymania działań skierowanych przeciwko poufności, integralności i dostępności systemów informatycznych, sieci i danych informatycznych, jak również nieprawidłowemu wykorzystywaniu tych systemów, sieci i danych, poprzez uznanie takiego postępowania za przestępstwo, zgodnie z niniejszą konwencją, oraz przyjęcia środków, które będą przydatne w skutecznym zwalczaniu takich przestępstw, poprzez ułatwienie ich wykrywania, prowadzenia dochodzenia i ścigania zarówno na szczeblu krajowym, jak i międzynarodowym, oraz poprzez przyjęcie rozwiązań sprzyjających szybkiej i rzetelnej współpracy międzynarodowej;

- pamiętając o konieczności zagwarantowania równowagi pomiędzy egzekwowania prawa a poszanowaniem podstawowych praw człowieka, zgodnie z Konwencją Rady Europy z 1950 roku o Ochronie Praw Człowieka i Podstawowych Wolności oraz Międzynarodowym Paktem Praw Obywatelskich i Politycznych z 1966 roku, jak również innymi traktatami odnoszącymi się do praw człowieka, które - potwierdzają prawo każdej jednostki do swobodnego wyrażania opinii, jak również prawo do wolności wypowiedzi, łącznie z wolnością poszukiwania, uzyskiwania i dzielenia się wszelkiego rodzaju informacjami i ideami, bez względu na granice, oraz prawo do poszanowania prywatności;

- pamiętając także o prawie do ochrony danych osobowych, przewidzianym np. w Konwencji Rady Europy z 1981 roku o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych;

- mając na uwadze Konwencję Narodów Zjednoczonych z 1989 roku o prawach dziecka oraz Konwencję Międzynarodowej Organizacji Pracy z 1999 roku o dotyczącą zakazu i natychmiastowych działań na rzecz eliminowania najgorszych form pracy dzieci; ..."

Wśród specjalistów jest opinia, że odmienne określenia bezpieczeństwa teleinformatycznego powodują utrudnienia we współpracy i koordynacji działań prowadzonych z myślą o poprawie stanu bezpieczeństwa teleinformatycznego, zwłaszcza w skali ogólnopaństwowej. Zagwarantowanie dostępu społeczeństwu do zasobów sieci

internetowych odgrywa w obecnych czasach kluczowe znaczenie. Trzeba jednak w tym miejscu podać rozumienie technologii informatycznej[12].

Technologia informatyczna, określana także wymiennie jako IT, technologia informacyjna, ICT (*Information and Communication Technology*) jest bardzo szerokim pojęciem. Kryje się pod nim wiele dziedzin wiedzy takich jak informatyka, a w ramach niej wszystkie jej znane działy np. *informatyka w zarządzaniu*, telekomunikacja, matematyka oraz inne dziedziny, w których występują narzędzia i technologie związane z przetwarzaniem informacji. Jednak IT jest zaangażowana w pozyskiwanie, gromadzenie, przetwarzanie i dystrybuowanie informacji przez sprzęty elektroniczne, takie jak komputer, telefon, radio czy też telewizja. Na bieżąco obserwujemy, że nowe i coraz bardziej zaawansowane techniki przekazywania informacji wkraczają w praktycznie każdą dziedzinę ludzkiego życia, przy czym podstawowe technologie informatyczne są następujące :

- gromadzenie danych,
- przetwarzanie danych,
- przesyłanie danych,
- magazynowanie danych,
- udostępnianie danych i zastosowania marketingowe w biznesie.

IT jako narzędzie rozwoju strategii to wspomaganie biznesowej strategii, wspieranie strategicznego rozwoju, ukierunkowanie na wirtualizację, tj.: zarządzanie wiedzą, sieci biznesowe oraz interakcje z klientami. Trzeba wyraźnie zaznaczyć, że technologia informatyczna jako narzędzie uzyskiwania przewagi konkurencyjnej zmierza również do

- powiększanie relacji z klientami,
- tworzenia wartości wirtualnej,
- indywidualizacji usług i produktów,
- tworzenia nowych struktur rynkowych oraz ról organizacyjnych,
- zwiększania kapitału intelektualnego.

Natomiast IT jako narzędzie transformacji prowadzi do*:* ulepszenia koordynacji, przeprojektowania procesów, efektywniejszego wykorzystanie zasobów informacyjnych, poprawy współdziałania, poprawy procesów rozwoju oraz uczenia się, innowacji w zakresie usług i produktów. Biorąc pod uwagę rolę IT jako narzędzia organizacji i funkcjonowania systemu informacyjnego to technologia informatyczna umożliwia*:*

- definiowanie procesów w systemie informacyjnym,

[12] https://mfiles.pl/pl/index.php/Technologia_informatyczna.

- kształtowanie architektury systemu informacyjnego,
- zwiększenie efektywności systemu informacyjnego,
- rozwój umiejętności personelu IT,
- poprawę elastyczności systemu informacyjnego.

Obserwujemy szybki rozwój zarówno sprzętu jak i aplikacji w zakresie IT. Obecnie najważniejsze trendy w informatyce to sztuczna inteligencja i uczenie maszynowe, *Big Data*, bioinformatyka i technologia medyczna, doskonalenie platform usług zdalnych, a także przetwarzanie w chmurze.

1.4. Dostępność usług w zakresie pracy zdalnej i cyberbezpieczeństwa

Rozwój techniki informatycznej wprowadził szereg udogodnień w zakresie nauki zdalnej jak i prowadzenia różnorodnych spotkań w świecie wirtualnym[13]. Powstało też wiele rozwiązań techniki IT, a jednym z przykładów jest *wielofunkcyjny zestaw do wideokonferecji* o nazwie *All In One od Huawei*, który obejmuje:

- urządzenie integrujące w sobie ekran dotykowy, kamerę wideo ze śledzeniem mówcy oraz mikrofon;
- dwa systemy operacyjne, tj. *Windows 10* oraz *Android*, dzięki czemu można go traktować jako pełnowartościowy komputer.

Wbudowany system operacyjny *Windows* pozwala na wykorzystanie wszystkich aplikacji komputerowych, w tym aplikacji do obsługi wideokonferencji, takich jak *Zoom*, *Skype* czy *ClickMeeting*. Wspomniany zestaw dzięki ekranowi dotykowemu IdeaHub może służyć jako tablica z możliwością kreślenia. Dysponuje także funkcją rozpoznawania pisma ręcznego, przy czym IdeaHub występuje w dwóch wielkościach ekranu o przekątnej 65 oraz 86 cali. Ponadto obejmuje system do wideokonferencji *MS Teams* lub *Webex*, a w ramach niego są:

- zestaw głośnomówiący do telekonferencji,
- mikrofon do telekonferencji,
- telefon konferencyjny,
- kamery do wideokonferencji,
- dedykowane kamery do *MS Teams*.

Wspomnieć trzeba jeszcze o telefonii IP, która jest nowoczesnym sposobem komunikacji głosowej w sieciach teleinformatycznych i dzięki której pracownicy firmy w łatwy sposób

[13] https://networkexpert.pl/cyberbezpieczenstwo/.

mogą się komunikować się między sobą. Telefon może być w formie tradycyjnej na biurko, aplikacji na komputer lub jako telefon komórkowy.

Firma ICT oferuje:

- wsparcie konsultingowe i wdrożeniowe w opracowaniu bezpiecznej struktury systemów ICS/OT,

- opracowanie strategii podwyższenia cyberbezpieczeństwa,

- przegląd i wsparcie w opracowaniu polityk i procedur związanych z cyberbezpieczeństwem,

- opracowanie bezpiecznej architektury systemów ICS/OT uwzględniających najnowsze rozwiązania sprzętowe i programowe renomowanych dostawców,

- monitorowanie sieci przemysłowych,

- SOC (*Security Operation Center*) – świadczenie usług związanych z zorganizowaniem centrum operacyjnego.

Oferowany jest także audyt bezpieczeństwa, który jest sprawdzeniem zabezpieczeń infrastruktury systemów teleinformatycznych. Jest to kontrolowanie i nieinwazyjne testowanie konkretnych zasobów w infrastrukturze, tak aby sprawdzić ich podatność na dane zagrożenia. Ataki wykonywane są przez certyfikowanego specjalistę od cyberbezpieczeństwa. Audyt zakończony jest raportem na podstawie którego, dzięki dokładnym wskazówkom, można rozpocząć wdrażanie zmian w zakresie cyberbezpieczeństwa. Przeprowadzenie audytów następuje pod kątem zgodności z wymogami standardów występujących w środowiskach przemysłowych (np. IEC 62443 /wybrane sekcje/, ISO 27001, wymagania KSC, specyficzne standardy kolejowe i motoryzacyjne).

1.5. Czuwanie i monitorowanie możliwości ataków na zasoby

Atak na zasoby teleinfromatyczne danej firmy/organizacji składa się z wielu kroków przygotowań. Istotne jest to, że cyberprzestępcy pozostawiają ślady swojej działalności zanim wykonają konkretny atak fizyczny, jednak nie spodziewają się, że oni również mogą być obserwowani[14]. Konieczny jest zatem audyt podatności systemów na zagrożenia zewnętrzne ze strony cyberprzestępców. Pozwala on bowiem dostosować zabezpieczenia zanim dojdzie do niebezpiecznej sytuacji, pozwala lepiej zarządzać podatnościami, co sprawia, że zagrożenia można wyeliminować możliwie wcześniej. Audyt pozwala danej

[14] Ibidem.

organizacji dostosować się do zgodności z normami i regulacjami GDPR RODO, ISO 27000. Występuje też konieczność bieżącego ujawniania informacji o zaistniałych incydentach bezpieczeństwa. Trzeba jeszcze dodać, że poprzez wydatki związane z przeprowadzeniem audytu zabezpieczenia systemu przed cyberprzestępcami określona firma/instytucja otrzymuje:

- wsparcie konsultingowe i wdrożeniowe w opracowaniu bezpiecznej struktury systemów ICS/OT,
- opracowanie strategii podwyższenia cyberbezpieczeństwa,
- przegląd i wsparcie w opracowaniu polityk i procedur związanych z cyberbezpieczeństwem,
- opracowanie bezpiecznej architektury systemów ICS/OT uwzględniających najnowsze rozwiązania sprzętowe i programowe renomowanych dostawców,
- monitorowanie sieci przemysłowych.

1.6. System teleinformatyczny a informatyczny

Po tych rozważaniach wprowadzających przybliżmy jeszcze rozróżnienie miedzy systemem teleinformatycznym a informatycznym, oraz określenie sieci teleinformatycznej, co może być pomocne w poznaniu dalszych zagadnień, w tym budowy sieci teleinformatycznych w określonym obiekcie.

System teleinformatyczny – oznacza każdy system umożliwiający przetwarzanie informacji w formie elektronicznej, w tym wszystkie zasoby niezbędne do jego działania, a także infrastrukturę, organizację, pracowników i zasoby informatyczne[15]. Definicja ta obejmuje aplikacje biznesowe, wspólne usługi IT, systemy obsługiwane na zewnątrz oraz urządzenia użytkownika końcowego . W prawie polskim system teleinformatyczny to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego.

System informatyczny (*information processing system*) – urządzenie lub grupa wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych[16]. W Polsce, termin ten jest używany w kontekście przede wszystkim systemów informacyjnych (*information*

[15] https://pl.wikipedia.org/wiki/System_teleinformatyczny.
[16] https://pl.wikipedia.org/wiki/System_informatyczny.

systems). W kontekście nauki o zarządzaniu, systemy informacyjne obejmują nie tylko warstwę techniczną, ale także np. ludzi z nich korzystających. Marian Kuraś uważa, że określenie system informatyczny powinno być zarezerwowane dla systemów obliczeniowych (*computer system*, *computing system*, *computational system*) . Systemy informatyczne jako części systemów informacyjnych składają się z następujących elementów:

a) Sprzęt komputerowy (*hardware*), w tym urządzenia wejścia/wyjścia:

- urządzenia służące do przechowywania danych;
- urządzenia służące do zbierania danych (kamery, sensory);
- urządzenia służące do komunikacji między sprzętowymi elementami systemu;
- urządzenia służące do komunikacji między ludźmi a komputerami;
- urządzenia służące do odbierania danych ze świata zewnętrznego (czujniki elektroniczne, kamery, skanery);
- urządzenia służące do wywierania wpływu przez systemy informatyczne na świat zewnętrzny – elementy wykonawcze.

b) Oprogramowanie (*software*):

- oprogramowanie wbudowane (*firmware*) np. sterownik urządzenia IoT (*internet rzeczy*);
- oprogramowanie systemowe (system software) np. system operacyjny, silnik gry komputerowej;
- *oprogramowanie aplikacyjne (application* software) np. gra komputerowa, aplikacja bankowa, system zarządzania bazą danych.

Natomiast *system informacyjny* obejmuje także:

- zasoby osobowe;
- elementy organizacyjne (procedury organizacyjne, instrukcje robocze);
- elementy informacyjne (bazy wiedzy, np. podręczniki).

Sieci teleinformatyczne są fundamentem nowoczesnego środowiska informatycznego[17]. Wysokowydajna, bezawaryjna oraz bezpieczna sieć ma bezpośredni wpływ na procesy biznesowe w firmie, gwarantując tym samym ich efektywną realizację. Poprawne zaprojektowanie infrastruktury LAN, WiFi, WAN, SAN czy SD-WAN ma kluczowe znaczenie dla zapewnienia ciągłości pracy w firmie. Dzięki zaawansowanej informatyce, funkcjonujących sieciach teleinformatycznych i istotnej możliwości analizy

[17] https://vernity.pl/oferta/sieci-teleinformatyczne/.

rozproszonych danych jest możliwość uzyskania nowej wiedzy z eksploatacji dużej bazy danych.

Pojęcie dużego zbioru danych „*Big data*" jest względne i oznacza sytuację, gdy zbioru nie da się przetwarzać przy użyciu tradycyjnych, powszechnie dostępnych metod[18]. Jego wartość dla biznesu polega na tym, że dane te są od lat dostępne w przedsiębiorstwach, ale dotychczas nie były analizowane. Analizując je mamy pełniejszy obraz swojego biznesu i możemy przykładowo:

- łatwiej identyfikować potencjalnych klientów,
- lepiej dobierać ofertę dla klienta,
- lepiej rozumieć reakcję rynku na nasz produkt,
- lepiej wyceniać produkt,
- z łatwością wykrywać zagrożenia dla biznesu.

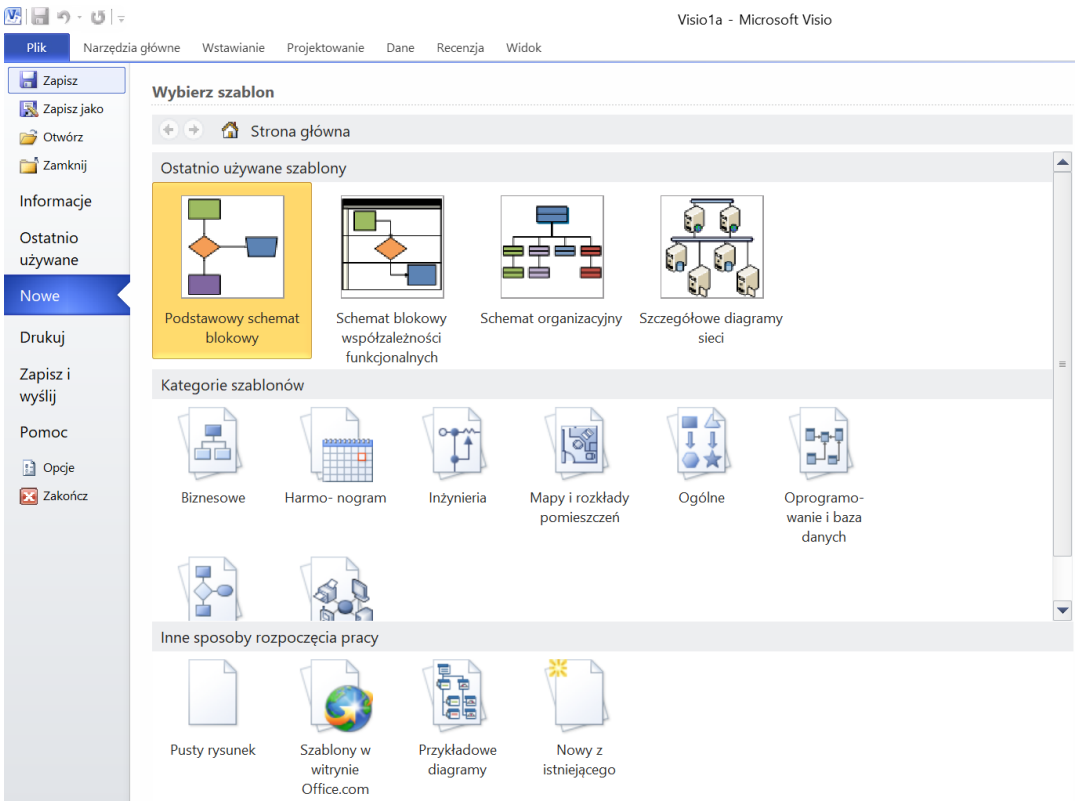
W zależności od branży i stopnia złożoności algorytmu *Big data* może oznaczać bazę o rozmiarze kilku terabajtów lub petabajtów (np. w analizie zderzeń cząstek elementarnych w fizyce wysokich energii)[19]. Jednak w innych zastosowaniach będą to już megabajty bądź gigabajty. *Big data* ma zastosowanie wszędzie tam, gdzie dużej ilości danych cyfrowych towarzyszy potrzeba zdobywania nowych informacji lub wiedzy. Szczególne znaczenie odgrywa wzrost dostępności Internetu oraz usług świadczonych drogą elektroniczną, które w naturalny sposób są przystosowane do wykorzystywania baz danych. Wykorzystanie do analiz dużych zbiorów danych oznacza jednocześnie, że nie trzeba ograniczać się do mniejszych zbiorów określanych za pomocą różnych sposobów doboru próby, co eliminuje związane z tym błędy[20].

[18] Płaszczak P., *Co to jest Big Data*, konferencja „*Big Data & Business Intelligence*", Warszawa 2013.
[19] Heath N., *Cern:* w https://cyberpolicy.nask.pl/category/obowiazujace/dyrektywa-nis/ here *the Big Bang meets Big Data*, https://www.techrepublic.com/topic/big-data/, 2023.
[20] Stępnik A., *Big data w perspektywie memetycznej*, Zeszyt memetyczny 16, 2015.

2. Rodzaje i struktura budowy sieci teleinformatycznych stacjonarnych i mobilnych

2.1. Wstęp

Mówiąc o bezpieczeństwie teleinformatycznym powinniśmy być przede wszystkim zorientowani co do budowy sieci zarówno lokalnych, branżowych jak i obsługujących określone resorty państwa. Sieci takie przedstawia się graficznie, a posłużyć się możemy w tym względzie, jeśli to będzie sieć lokalna np. programem *Microsoft Visio*. Strukturę menu głównego tej aplikacji zaprezentowano na rysunku 2.1. Wymieniony program oferuje różnego rodzaju standardowe szablony do tworzenia schematów, a w tym do opracowania szczegółowych diagramów połączeń komponentów sieci komputerowej oraz dodatkowo na nich opisu charakterystyki poszczególnych urządzeń.



Źródło: Opracowanie własne na podstawie programu *Microsoft Visio*.

Rys. 2.1. Zakładki menu głównego programu *Microsoft Visio*

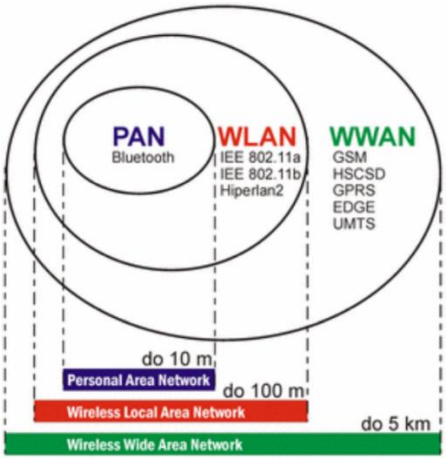
Sieci mogą być np. światłowodowe oraz przy niedużych odległościach bezprzewodowe. Skupmy teraz uwagę na standardach sieci bezprzewodowej mające różne skrócone nazwy i formy połączeń elementów tworzących daną sieć. W tym względzie skorzystajmy z publikacji internetowej prezentującej typowe rodzaje sieci bezprzewodowych[21].

2.2. Standardy sieci bezprzewodowych

Jako przykłady standardowych sieci bezprzewodowych, w tym materiale, przedstawione zostaną sieci określane skrótami: WPAN, WLAN, WWAN.

WPAN (*Wireless Personal Area Network*) - sieć o zasięgu kilku metrów służąca do wymiany informacji pomiędzy urządzeniami przenośnymi typu notebook, palmtop, telefon gsm z wykorzystaniem technologii przenoszenia o nazwie *Bluetooth*.

WLAN (*Wireless Local Area Network*) to sieć bezprzewodowa lokalna, która używa fal radiowych lub podczerwonych do przesyłania informacji z jednego punktu do drugiego. Są one projektowane z użyciem standardu IEEE 802.11. Do komunikacji za pomocą fal radiowych wykorzystuje się pasmo 2,4 GHz lub rzadziej 5 GHz, przy czym jest 14 kanałów. Każdy kanał ma swoją częstotliwość nośną, która jest modulowana przy przesyłaniu informacji. Szybkość przesyłania danych zależna jest od użytego standardu i odległości pomiędzy użytymi urządzeniami. Instalatorzy sieci bezprzewodowych mają duży wybór rozmaitych technologii przy projektowaniu rozwiązań bezprzewodowych, a podział technologii pod kątem zasięgu zaprezentowano na rysunku 2.2.



Źródło: https://qcg.home.amu.edu.pl/pliki/Sieci%20bezprzewodowe.pdf.

Rys. 2.2. Poglądowe przedstawienie zasięgu różnych sieci bezprzewodowych

[21] https://qcg.home.amu.edu.pl/pliki/Sieci%20bezprzewodowe.pdf.

Sieć WLAN zlokalizowana jest na stosunkowo niewielkim obszarze i obejmuje kilka komputerów mających łączność bezprzewodową z serwerami (zob. rysunek 2.3). Dla nawiązania łączności stosuje się małe anteny o nazwie *Access Point*, czyli punkt dostępowy.

Źródło: https://qcg.home.amu.edu.pl/pliki/Sieci%20bezprzewodowe.pdf.

Rys. 2.3. Poglądowe przedstawienie lokalnej sieci bezprzewodowej

WWAN (*Wireless Wide Area Network*) to już rozległa sieć komputerowa oparta o technologię bezprzewodową, która obejmuje dużą liczbę komputerów na dużej przestrzeni i o dużym zasięgu. Do łączności bezprzewodowej potrzebna jest duża antena umieszczona na terenie pracy komputerów.

Jak już nadmieniono, w każdym paśmie (2,4-2,5 GHz) komunikacji bezprzewodowej zgodnej ze standardem Wi-Fi - 802.11b/g - wyodrębniono 14 niezależnych kanałów (co 5 MHz od 2412 do 2477 MHz). Szybkość przesyłania danych zależna jest od użytego standardu i odległości pomiędzy użytymi urządzeniami i wynosi najczęściej:11, 22, 44, 54 lub 108 Mbps. Stosowane są metody zabezpieczeń zgodne ze standardem 801.11 dotyczące[22]:

- *uwierzytelniania* (identyfikacja i weryfikacja autentyczności informacji przesyłanych przez użytkownika, który łączy się z siecią);

- *protokół* WEP (*Wired Equivalent Privacy*), który działa na zasadzie współdzielonego klucza szyfrującego o długości 40 do 104 bitów i 24 bitowym wektorze inicjującym;

- *autoryzacja* (zgoda lub brak zgody na żądaną usługę przez uwierzytelnionego użytkownika);

[22] Ibidem.

- *rejestracja raportów* (to rejestr akcji użytkownika związanych z dostępem do sieci). Śledzenie raportów pozwala na szybką reakcję administratorów na niepokojące zdarzenia w sieci.

2.3. Karty sieciowe i punkty dostępowe

Stosowane są karty sieciowe typu PCI, USB lub PCMCIA. Karty PCI są zgodne ze standardem *Plug&Play*. Jest to popularny typ kart ponieważ praktycznie wszystkie komputery stacjonarne posiadają złącza PCI. Karty na złączach USB wymagają bardziej skomplikowanej instalacji oraz zużywają więcej zasobów komputera. W komputerach przenośnych wykorzystywane są karty PCMCIA i często odznaczają się one większą wydajnością. Widoki różnych kart sieciowych pokazano na rysunku 2.4. Przy wyborze kart sieciowych należy zwrócić uwagę również na prędkość adaptera. Do wyboru mamy: wersję 802.11B - 11Mbit/s lub wersję 802.11G - 54Mbit/s.

Źródło: https://qcg.home.amu.edu.pl/pliki/Sieci%20bezprzewodowe.pdf.

Rys. 2.4. Przykłady różnych kart sieciowych

Pokazane już wcześniej na rysunku 2.3. punkty dostępowe (*Access Point)* posiadają wbudowane różne typy pracy i stanowią łączniki z już istniejącą siecią komputerową. Umożliwia to rozwiązywanie nawet skomplikowanych topologii sieciowych. Zwróćmy teraz uwagę na funkcjonalność poszczególnych trybów pracy punktów dostępowych.

Access Point (AP) - tryb umożliwiający podłączanie abonentów do już istniejącej sieci typu LAN. Tryb ten stosują dostawcy usług internetowych podłączający swoich klientów poprzez bezprzewodowe karty sieciowe. Ponadto domowi użytkownicy Internetu dostarczanego drogą kablową.

AP Bridge Point To Point - tryb w którym punkt docelowy pracuje jako bezprzewodowy most łączący dwie oddalone od siebie sieci lokalne LAN w sąsiednich obiektach tworząc jedną strukturę sieciową.

AP Bridge Point To Multipoint - tryb ten umożliwia zwiększenie liczby połączonych sieci by stworzyć np. sieć o topologii gwiazdy.

AP Bridge WDS, gdzie *WDS* (*Wireless Distribution System*) - tryb ten charakteryzuje się możliwością jednoczesnej pracy punktu dostępowego jako *Acces Point* oraz mostu bezprzewodowego, co umożliwia to zbudowanie różnych szkieletów sieci.

2.4. Przykłady struktur sieci bezprzewodowych

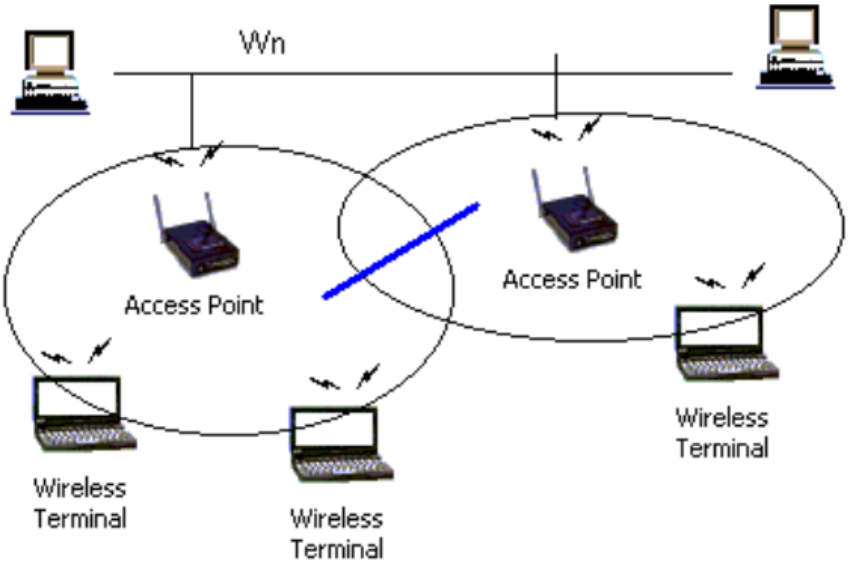
Sieci bezprzewodowe mogą być proste lub złożone. W najprostszej wersji, dwa komputery wyposażone w karty radiowe tworzą niezależną sieć, gdy tylko znajdą się w swoim zasięgu. Nazywamy to siecią *peer-to-peer*. W takim przypadku każdy użytkownik może mieć dostęp do zasobów drugiego użytkownika, lecz nie do centralnego serwera. Zainstalowanie punktu dostępowego może zwiększyć zasięg takiej sieci, efektywnie podwajając zasięg w jakim urządzenia mogą się komunikować (zob. rysunek 2.5).

Źródło: https://qcg.home.amu.edu.pl/pliki/Sieci%20bezprzewodowe.pdf.

Rys. 2.5. Bezprzewodowa sieć z punktem dostępowym włączonym do szkieletu sieci

Ponieważ punkt dostępowy jest podłączony do sieci kablowej, każdy użytkownik ma dostęp zarówno do serwera jak i do innych użytkowników. Każdy punkt dostępowy może obsłużyć wielu użytkowników, przy czym ich dokładna liczba zależy od ilości i rodzaju transmitowanych danych. Należy dodać, że wiele pracujących aplikacji działa w konfiguracjach, gdzie jeden punkt dostępowy obsługuje od 15 do 50 użytkowników.

Punkty dostępowe mają ograniczony zasięg: 300 metrów w pomieszczeniach i 30 000 metrów na otwartej przestrzeni. Natomiast w rozległych infrastrukturach, takich jak magazyny, hurtownie, czy osiedla mieszkaniowe, trzeba zainstalować więcej niż jeden punkt dostępowy. Celem jest pokrycie obszaru z zachowaniem nakładania się zasięgu poszczególnych komórek tak by użytkownik mógł poruszać się po danym obszarze bez utraty dostępu do sieci. Taką możliwość poruszania się w zasięgu zespołu punktów dostępowych nazywamy *roamingiem*[23] (zob. rysunek 2.6).



Źródło: https://qcg.home.amu.edu.pl/pliki/Sieci%20bezprzewodowe.pdf.

Rys. 2.6. Kilka punktów dostępowych i *roaming*

Możemy doprowadzić łącza Internetowe do użytkowników indywidualnych na osiedlu domków jednorodzinnych. Na punkcie dostępowym stosujemy antenę (lub anteny) dookólne, a abonenci korzystają z anten kierunkowych. Niezbędnym warunkiem dla zestawienia takich połączeń jest widzialność optyczna kierunkowych anten nadawczo-odbiorczych abonentów i anteny na punkcie dostępowym.

[23] Ibidem.

2.5. Ochrona informacji w sieciach

Szyfrowanie to najczęściej stosowany sposób implementacji zabezpieczeń i ochrony informacji przekazywanych w sieciach. W procesie szyfrowania wysyłane informacje zostają przetworzone przez zestaw instrukcji zwanych *algorytmem szyfrowania*. Instrukcje te łączą jawny tekst informacji z sekwencją liczb szesnastkowych zwanych kluczem szyfrującym. Informacje, które mają być transmitowane drogą bezprzewodową, zostają wcześniej zaszyfrowane przez klienta bezprzewodowego lub punkt dostępowy. Podczas odbierania informacji punkt dostępowy lub klient bezprzewodowy używają tego samego klucza do odszyfrowania informacji. Informacje te mogą być odczytane tylko przez urządzenia sieci WLAN, które dysponują odpowiednim kluczem szyfrującym. Im dłuższy klucz, tym mocniejsze szyfrowanie.

Połączenia do sieci korporacyjnych za pomocą sieci bezprzewodowych mogą odbywać się także przy pomocy tuneli VPN. W sieciach bezprzewodowych zgodnych ze standardem 802.11a/b/g wykorzystuje się w tym celu technologię WEP (*Wired Equivalent Privacy*).

IPsec (*IP Security*) to zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy kodowych pomiędzy komputerami. Protokoły tej grupy mogą być wykorzystywane do tworzenia *Wirtualnej Sieci Prywatnej* (VPN), przy czym sieć ta składa się z dwóch rodzajów kanałów komunikacyjnych pomiędzy połączonymi komputerami:

1. *Kanał wymiany kluczy* za pośrednictwem którego przekazywane są dane związane z autentykacją oraz kodowaniem.

2. *Kanał (jeden lub więcej), który niesie pakiety transmitowane* poprzeć sieć prywatną.

WPA (*WiFi Protected Access*) to standard szyfrowania stosowany w sieciach bezprzewodowych typu IEEE 802.11.

Hotspot (*hot spot*). Otwarty publicznie punkt umożliwiający dostęp do Internetu za pomocą sieci bezprzewodowej (WiFi). *Hotspoty* są instalowane najczęściej w hotelach, restauracjach, lotniskach, dworcach, uczelniach, centrach miast i innych miejscach publicznych. Umożliwiają one posiadaczom laptopów i palmtopów wyposażonych w bezprzewodową kartę sieciową standardu 802.11 podłączenie się i dostęp do Internetu. Usługa czasami jest bezpłatna lub też płatność następuje za pomocą karty kredytowej lub zakupienia odpowiedniej zdrapki, a do zabezpieczenia *hotspotów* służą:

- klucz WE,

- klucz WPA,
- WPA II,
- Serwer Radius,
- ukrywanie SSID,
- wirtualne prywatne sieci VPN (*Virtual Privacy Network VPN*)[24].

2.6. Oferta budowy sieci bezprzewodowej i telefonii VoIP

Jak już nadmieniono, wertując strony internetowe spotykamy różnorodne oferty instytucji programowania w zakresie projektowania, instalowania oraz serwisowania sieci bezprzewodowych. Na uwagę zasługuje między innymi szersza oferta zaproponowana przez firmę „Network Expert"[25]. Na jej stronie internetowej spotykamy ofertę różnych usług, cenną informację o budowie sieci oraz telefonii VoIP, a ponadto szczególnie interesującą nas zakładkę „*Cyberbezpieczeństwo*". Proponowane są usługi kompleksowe obejmujące między innymi:

- budowę i zabezpieczenie sieci komputerowych klasy *Lan & Wan, Security, Unified Communication, Wireless,*
- projektowanie i wdrażanie sieci

Firma „Network Expert" podejmuje się projektowania i budowy profesjonalnych sieci w obiektach różnego typu, między innymi w biurach, magazynach, hotelach, obiektach przemysłowych, a ponadto: planowania radiowego i *site survey*, audytu sieci, audytu bezpieczeństwa sieci, modernizacje istniejącej sieci.

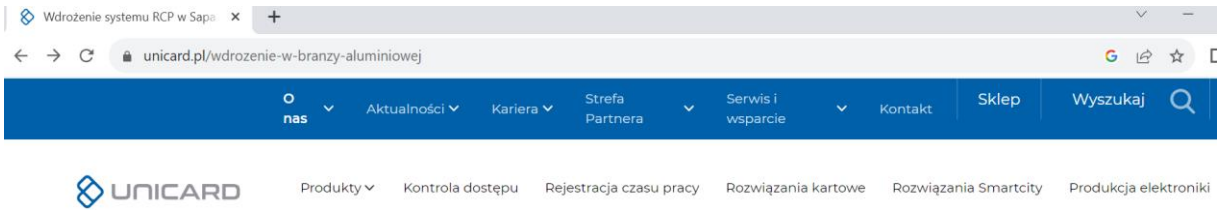
Przykładem wdrożenia jest budowa sieci radiowej dla SAPA Aluminium**,** jednego z największych producentów form aluminiowych na świecie. Głównym celem całościowym tego rozwiązania było pokrycie siecią Wi-Fi obszaru wszystkich hal produkcyjnych w jednym z oddziałów firmy na terenie województwa wielkopolskiego. Wymagało to przygotowania planu radiowego nowej sieci oraz planu nowej infrastruktury kablowej. Po zakończeniu wszystkich prac instalacyjno-montażowych oraz rekonfiguracyjnych sieci, firma Network Expert wykonała całościową dokumentację podwykonawczą zawierającą pomiary sieci radiowej. Na rysunku 2.7 widzimy front jednej z hal firmy SAPA Aluminium.

[24] Wyszukiwarka hotspotów w Polsce (*http://hot.spots.pl*).
[25] https://networkexpert.pl/cyberbezpieczenstwo/.

Źródło: https://qcg.home.amu.edu.pl/pliki/Sieci%20bezprzewodowe.pdf.

Rys. 2.7. Widok jednej z hal firmy SAPA Aluminium

Warto jeszcze zaglądnąć na stronę WWW firmy SAPA Aluminium i dowiedzieć się więcej o realizowanym rozwiązaniu informatycznym (rys. 2.8). W procesie projektowo-wdrożeniowym korzystano z rozwiązań UNICARD do rejestracji czasu pracy w 3 lokalizacjach: Trzcianka, Łódź, Chrzanów. Rozwiązania zainstalowane w Trzciance i Łodzi korzystały z kart w systemie INDALA, przy czym Chrzanów od już samego początku (2014) pracuje w standardzie kart MIFARE.

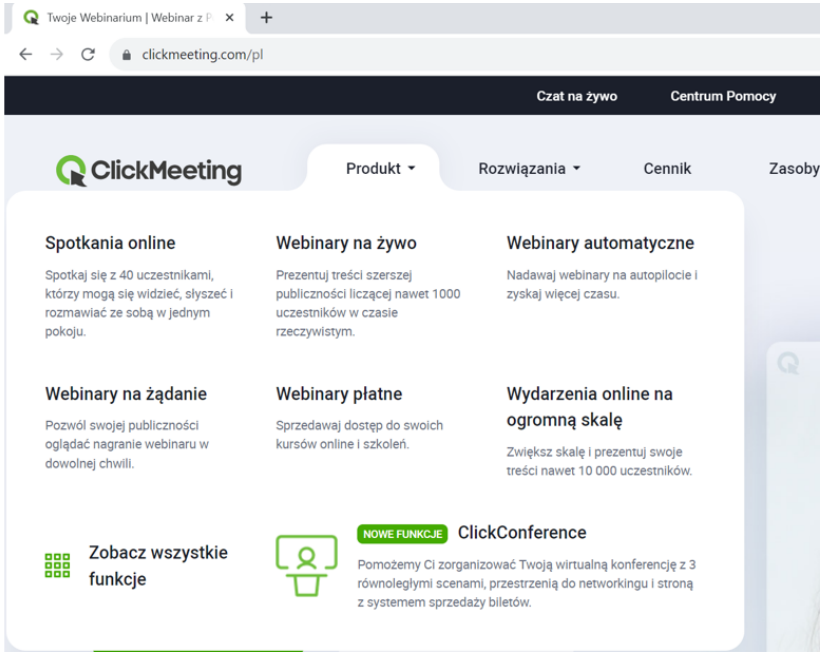


Źródło: unicard.pl/wdrożenie-w-branzy-aluminiowej

Rys. 2.8. Fragment strony WWW firmy SAPA Aluminium

2.7. Przykłady platform korzystających z sieci teleinformatycznych

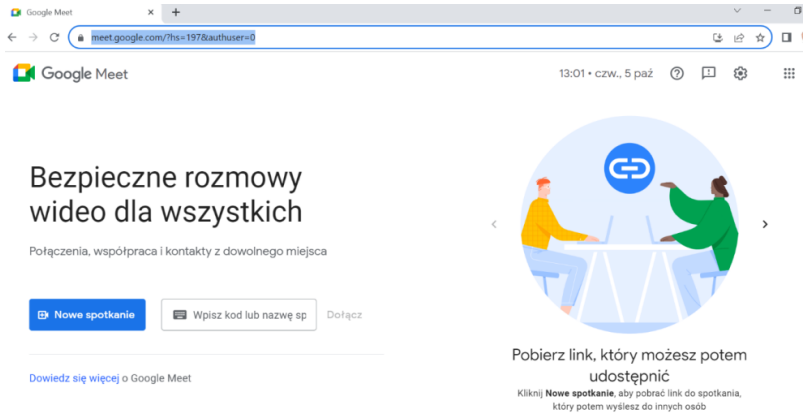
Platforma *ClickMeeting* to szeroka gama możliwości współpracy oraz spotkań *online*[26]. Stronę WWW tej platformy zaprezentowano na rysunku 2.9.



Źródło: https://clickmeeting.com/pl.

Rys. 2.9. Zakres usług w ramach platformy *ClickMeeting*

Platforma *Google Meet* jest wykorzystywana w szczególności do prowadzenia wykładów na studiach między innymi na kierunkach *Zarządzanie*, *Logistyka*, *Administracja* oraz *Pedagogika*[27]. Stronę wstępną zarejestrowania się na spotkanie *online* pokazano na rys. 2.10.

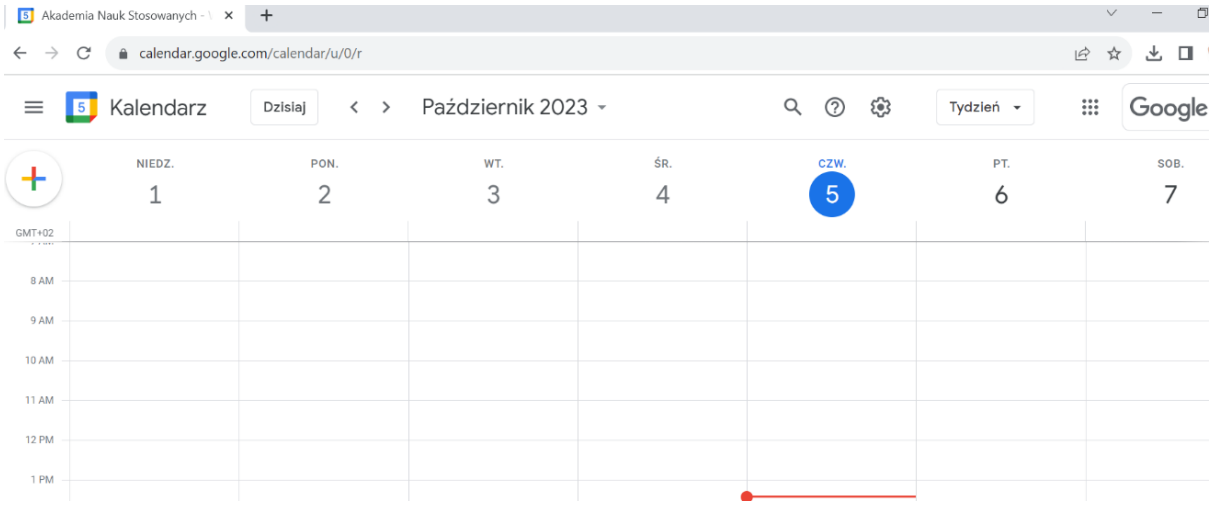


Źródło: https://meet.google.com.

Rys. 2.10. Strona platformy *Google Meet* umożliwiająca dostęp do spotkania

[26] https://clickmeeting.com/pl.
[27] https://meet.google.com/?hs=197&authuser=0.

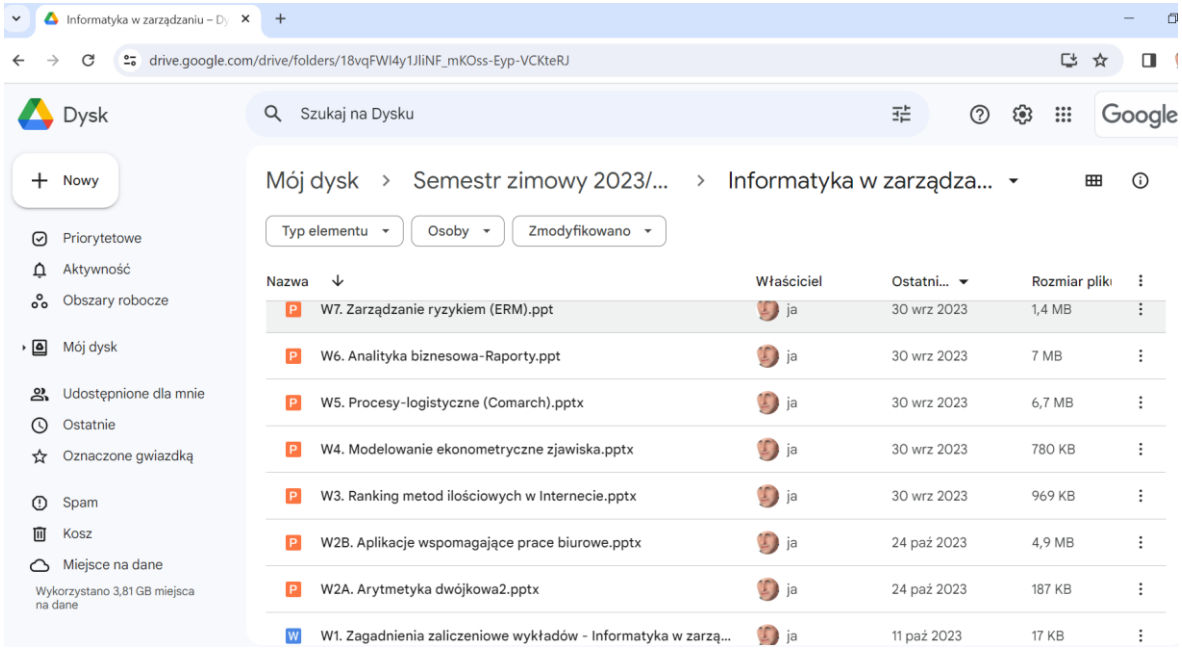
Przykładowo, w uczelni Akademia Nauk Stosowanych WSZiA w Opolu poszczególne spotkania online są odnotowane w zakładce *Kalendarz* (zob. rysunek 2.11).



Źródło: https://meet.google.com.

Rys. 2.11. Możliwości wprowadzenia wydarzenia w *Kalendarzu*

Prezentacje wykładów i ćwiczeń z określonych przedmiotów zgromadzone są na dysku platformy *Google Meet*. Przykład plików z zakresu wykładów przedmiotu „*Informatyka w zarządzaniu*" widzimy na rysunku 2.12.



Źródło: Opracowanie własne w *Google Meet*.

Rys. 2.12. Pliki do wykładów z przedmiotu „*Informatyka w zarządzaniu*"

Platforma *Google Hangouts* to komunikator internetowy amerykańskiej firmy Google[28]. Służył do wysyłania wiadomości oraz telefonowania za pośrednictwem technologii VoIP. Komunikator zastąpił trzy inne aplikacje Google'a służące do komunikacji: *Google Talk, Google+ Messenger* oraz *Hangouts* (wideo chat wbudowany w Google+). Do korzystania z aplikacji wymagane jest aktywne konto Google[29] .

Google Chat to inteligentne i bezpieczne narzędzie do komunikacji w zespołach[30]. Stanowi zintegrowaną platformę ułatwiającą komunikację dzięki zastosowaniu różnorodnych usług, od czatów indywidualnych po pokoje do rozmowy dla całych zespołów. Obecna wersja jest przeznaczona wyłącznie dla klientów korzystających z *Google Workspace*.

Usługa sieciowa (*Web Service*) stanowi właściwość systemu teleinformatycznego polegająca na powtarzalnym wykonywaniu przez ten system z góry określonych funkcji po otrzymaniu, za pomocą sieci teleinformatycznej, danych uporządkowanych w określonej strukturze[31] [32]. Usługa sieciowa jest w istocie składnikiem oprogramowania, niezależnym od platformy sprzętowej oraz implementacji, dostarczającym określonej funkcjonalności. Zgodnie z zaleceniami *Słowniczka Usług Sieciowych* (W3C), dane przekazywane są zazwyczaj za pomocą protokołu HTTP i z wykorzystaniem XML[33].

Join.me jest uproszczonym oprogramowaniem do spotkań *online* z zabezpieczeniami klasy korporacyjnej, które jest częścią rodziny *GoTo,* która zawiera produkty do wirtualnych spotkań, w tym *GoTo Connect* i *GoTo Meeting*[34].

WhatsApp firmy Meta to bezpłatna aplikacja do komunikacji i połączeń wideo[35]. Używa jej ponad 2 miliardy osób w ponad 180 krajach. Aplikacja *WhatsApp* jest prosta w obsłudze, niezawodna i prywatna, więc można z łatwością utrzymywać kontakt ze znajomymi i rodziną. *WhatsApp* działa bez opłat subskrypcyjnych na urządzeniach mobilnych i komputerach stacjonarnych nawet przy niskiej szybkości połączenia.

---

[28] https://pl.wikipedia.org/wiki/Google_Hangouts.
[29] *Making calls from Hangouts — in Gmail and across the web, „Official Gmail Blog"* (https://pl.wikipedia.org/wiki/Google_Hangouts).
[30] https://play.google.com/store/apps/details?id=com.google.android.apps.dynamite&hl=pl&gl=US.
[31] https://pl.wikipedia.org/wiki/Us%C5%82uga_sieciowa.
[32] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247).
[33] *Web Services Glossary*. www.w3.org.
[34] https://www.goto.com/meeting?utm_source=joinme.com&utm_medium=referral&utm_campaign=jm_eos_2022&campaignid=7014P000001vnMyQAI.
[35] https://play.google.com/store/apps/details?id=com.whatsapp&hl=pl&gl=US.

Aplikacja *Skype* jest to wysokiej jakości połączenia wideo ułatwiające kontakt z innymi osobami[36]. Menu główne tej platformy firmy Microsoft pokazano na rysunku 2.13.

Źródło: Opracowanie własne w *Skype*.

Rys. 2.13. Zakładki menu aplikacji *Skype*

Platforma *Zoom* pomaga konsolidować komunikację, łączyć uczestników spotkania i lepiej współpracować w sali konferencyjnej, klasie oraz sali operacyjnej[37]. Wersja *Zoom Docs* oparta jest na sztucznej inteligencji do obsługi dokumentów, stron encyklopedii Wikipedia i zarządzania pracą. Przewiduje się, że rozwiązanie to będzie dostępne od 2024 roku i integrować będzie się z *Zoom* oraz aplikacjami innych firm. Dzięki wbudowanej sztucznej inteligencji *Zoom Docs* umożliwia wypełnianie dokumentów treścią ze spotkań *Zoom Meetings* w celu zbierania informacji i przyspieszania tworzenia opracowań, przy czym kolejne rozwiązanie *Zoom AI Companion* pomaga podsumowywać i tworzyć informacje.

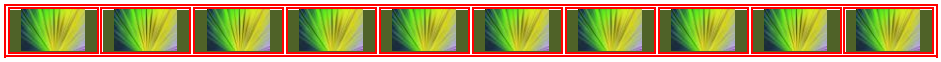
Na zakończenie przeglądu platform wirtualnych do spotkań *online* wspomniana zostanie aplikacja *Cisco Webex* (zob. rysunek 2.14). Platforma *Cisco Webex* umożliwia pracę zespołów zdalnie, korzystając z przeglądarki internetowej, telefonu komórkowego lub urządzenia wideo[38]. W ramach tej platformy rozwiązanie *Webex Meetings* oferuje zintegrowane funkcje udostępniania dźwięku, wideo i treści oraz bezpieczne spotkania sieciowe w ramach chmury. Wymienione *Cisco Webex* to proste i innowacyjne rozwiązanie ułatwiające prowadzenie efektywnych spotkań wirtualnych.

Źródło: https://www.cisco.com/c/pl_pl/products/conferencing/webex-meetings/index.html.

Rys. 2.14. Menu główne platformy *Cisco Webex*

[36] https://www.skype.com/pl/.
[37] https://zoom.us/pl.
[38] https://www.cisco.com/c/pl_pl/products/conferencing/webex-meetings/index.html.

3. Cyberprzestrzeń oraz zagrożenie ze strony sieci globalnych



3.1. Błędy we wdrażaniu systemów jako „*furtki*" do złośliwej interakcji

Po tych wstępnych rozważaniach, wprowadzających nas w świat wirtualnych publikacji dotyczących cyberbezpieczeństwa, wniknijmy w cyberprzestrzeń, która coraz częściej stanowi zagrożenie dla niezawodności eksploatowanych sieci teleinformatycznych, pakietów oprogramowania oraz komunikatorów umożliwiających spotkania, naukę *online* i pracę zdalną. W opracowaniu niniejszym, traktowanym jako materiał pomocniczy do specjalizacji w zakresie cyberbezpieczeństwa, zabazowano przede wszystkim na publikacji internetowej firmy Network Expert[39] oraz informacjach z encyklopedii Wikipedia.

Wymarzony bezpieczny system teleinformatyczny jest urządzeniem, które poprawnie i w całości realizuje tylko i wyłącznie cele zgodne z intencjami użytkownika[40]. W praktyce jednak budowa skomplikowanego systemu teleinformatycznego spełniającego te intencje jest z reguły niemożliwa i dlatego zapewnianie bezpieczeństwa sprowadza się do kompleksowego zarządzania ryzykiem poprzez:

- określenie potencjalnego zagrożenia,
- szacowanie prawdopodobieństwo ich wystąpienia,
- ocenianie potencjalnych strat,
- podejmowanie kroków zapobiegawczych.

Według pozyskanej publikacji pod linkiem: *https://networkexpert.pl/cyberbezpieczenstwo/* informacji zarządzanie dostępem do sieci teleinformatycznej obiektu odbywa się z zastosowaniem *Cisco ISE*, który jest zaawansowanym systemem zarządzania dostępem. Stosowany serwer *Network Admision Control* (NAC) to urządzenie, który wspiera sprzęt sieciowy w udzielaniu dostępu do danej sieci, czyli dokonuje uwierzytelniania. Ten centralny serwer może być powiązany z bazą danych użytkowników, np. *Microsoft AD* i możemy na takim serwerze tworzyć polityki dostępu do sieci. Występuje możliwość uruchomienia *Cisco*

[39] https://networkexpert.pl/cyberbezpieczenstwo/.
[40] https://pl.wikipedia.org/wiki/Bezpiecze%C5%84stwo_teleinformatyczne.

ISE na jednym serwerze wirtualnym lub kilkunastu serwerach dedykowanych. Aplikacja ta ma bardzo dogodny interfejs systemu GUI, co pozwala wykonywać wiele operacji dostępowych do sieci.

Zewnętrzne wnikanie w działające oprogramowanie jest konieczne, gdyż na etapach pospiesznego projektowania, programowania jak i wdrażania mogą wystąpić początkowo niedostrzeżone błędy tworzenia kodu źródłowego lub inne określonej aplikacji. Skorzystajmy zatem z publikacji pod linkiem: *https://networkexpert.pl/cyberbezpieczenstwo/* , gdzie spotykamy wymienienie i omówienie potencjalnych możliwych wystąpień błędów.

Błędy zabezpieczeń. W dobie łączności modemowej, sieci rozległych i Internetu, problemem stały się sytuacje, w których chociaż oprogramowanie działa zgodnie z oczekiwaniami projektanta, pozwala oprócz tego osobom trzecim na złośliwą interakcję z systemem. Scenariusze, które mogą prowadzić do nieautoryzowanego wykorzystania systemu, są dzielone na kilka grup, w zależności od swego pochodzenia.

Błędy projektowe. Występują wtedy, gdy założenia dla oprogramowania oparte są na nieprawidłowych przesłankach w utworzonym schemacie blokowym. Może to być nie w pełni poprawne rozumienie procedury użytkownika, zasad funkcjonowania sieci komputerowych, budowy wykorzystywanych protokołów komunikacyjnych, a do takich błędów można zaliczyć:

- wykorzystanie szyfrów podatnych na ataki,
- nieodpowiedni dobór mechanizmów uwierzytelniania,
- zaufanie informacjom przesyłanym przez klienta w architekturze klient-serwer.

Ich skutkiem może być sytuacja, w której nie można ufać wynikom pracy aplikacji i integralności przetwarzanych przez nią danych.

Błędy implementacyjne. W tej grupie błędów występują pomyłki techniczne popełniane przez programistów na skutek ich wywołań systemowych. Częstym efektem błędów implementacyjnych jest możliwość przejęcia pełnej kontroli nad procesem przez osoby niepowołane oraz możliwość bezpośredniej interakcji z systemem operacyjnym.

Błędy konfiguracyjne. Są to pomyłki popełniane przez administratorów, którzy przygotowują oprogramowanie do wykorzystania przez użytkowników. Przykładem może być ustawienie typowych haseł dla uprzywilejowanych kont.

Błędy operatora. Przykładem może być uruchamianie przez użytkowników załączników od niepewnych nadawców przysłanych w poczcie elektronicznej, ignorowanie komunikatów ostrzegawczych, a także przypadkowa zmiana opcji programu.

3.2. Bieżące czuwanie nad możliwością wystąpienia cyberzagrożenia infrastruktury krytycznej

Z punktu widzenia zagrożenia infrastruktury krytycznej w ramach organów państwa istotne jest prowadzenie na bieżąco monitorowania tego obszaru. Konieczny jest podział obiektów z uwagi na ich poziom ochrony, przy czym istotne są plany ochrony dla obiektów[41]:

- podlegających obowiązkowej ochronie,
- szczególnie ważnych dla bezpieczeństwa i obronności państwa,
- stanowiących infrastrukturę krytyczną.

Ważna jest znajomość aspektów prawnych ochrony infrastruktury krytycznej oraz faz zarządzania kryzysowego. Na uwagę zasługuje też ochrona informacji niejawnych. W szkoleniach należy podać zasady ewakuacji obiektów lub/i obszarów należących do infrastruktury krytycznej.

Zgodnie z art. 41 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa dla sektora transportu oraz sektora zaopatrzenia w wodę pitną i jej dystrybucji organem właściwym do spraw cyberbezpieczeństwa jest Minister Infrastruktury[42]. Za realizację obowiązków organu właściwego do spraw cyberbezpieczeństwa wynikających z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa odpowiada Wydział Bezpieczeństwa Teleinformatycznego w Biurze Zarządzania Kryzysowego w Ministerstwie Infrastruktury. Na podstawie art. 42 ust. 1 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa organ właściwy do spraw cyberbezpieczeństwa realizuje między innymi następujące prace:

- prowadzi bieżącą analizę podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej;
- wydaje decyzje o uznaniu podmiotu za operatora usługi kluczowej albo decyzje stwierdzające wygaśnięcie decyzji o uznaniu podmiotu za operatora usługi kluczowej;
- niezwłocznie po wydaniu decyzji o uznaniu za operatora usługi kluczowej, albo decyzji stwierdzającej wygaśnięcie decyzji o uznaniu za operatora usługi kluczowej, przekazuje wnioski do ministra właściwego do spraw informatyzacji o wpisanie do wykazu operatorów usług kluczowych albo wykreślenie z tego wykazu;

[41] https://bip.skw.gov.pl/skw/bezpieczenstwo-teleinfo/zalecenia-w-zakresie-be/5109,Zalecenia-w-zakresie-bezpieczenstwa-teleinformatycznego.html.
[42] https://www.gov.pl/web/infrastruktura/wydzial-bezpieczenstwa-teleinformatycznego.

- składa wnioski o zmianę danych w wykazie operatorów usług kluczowych, nie później niż w terminie 6 miesięcy od zmiany tych danych;

- przygotowuje we współpracy z CSIRT NASK, CSIRT GOV, CSIRT MON i sektorowymi zespołami cyberbezpieczeństwa rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów;

- monitoruje stosowanie przepisów Ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych.

- uczestniczy w ćwiczeniach w zakresie cyberbezpieczeństwa organizowanych w Rzeczypospolitej Polskiej lub w Unii Europejskiej.

3.3. Konieczność dokształcania służb w zakresie cyberbezpieczeństwa

Wykorzystywanie atutów cyfrowego otoczenia dla realizowania celów w obszarze bezpieczeństwa, a także realizowanie efektywnej strategii komunikacyjnej w cyfrowym otoczeniu informacyjnym to ważne obszary wsparcia – ale też potencjalnych zagrożeń dla współczesnych państw[43]. Zagadnienie cyberbezpieczeństwa to nowy obszar bezpieczeństwa. Nowe problemy i wyzwania stoją przed informatyką, analizą informacji oraz danych przy wykorzystaniu narzędzi *Business Intelligence* (BI) i *Big Data*. Dochodzą do tego jeszcze kwestie związane z ochroną danych osobowych. Cyberbepieczeństwo obejmuje bowiem następujące obszary zagadnień: bezpieczeństwo teleinformatyczne, informatyka śledcza, walka informacyjna, analiza informacji, zarządzanie ryzykiem i bezpieczeństwem, zwalczanie międzynarodowego terroryzmu, prawo.

Na szeregu szkoleniach oraz studiach podyplomowych, w tym na kierunku *Zarządzanie*, podejmowane są wykłady wskazujące na przypadki zagrożenia bezpieczeństwa teleinformatycznego. Trzeba tu dodać, że zarządzanie cyberbezpieczeństwem obejmuje szerokie spektrum zagadnień, a mianowicie:

- strategie i regulacje prawne;
- zapewnienie bezpieczeństwa w procesie projektowania i wdrażania oprogramowania;
- narzędzia i standardy w obszarze cyberbezpieczeństwa;
- ISO 27000 / 24762 / 22301, NIST;

[43] https://civitas.edu.pl/pl/oferta-edukacyjna/cyberbezpieczenstwo-podyplomowe/opis-cyberbezpieczenstwo-podyplomowe.

- CISA, CISSP, RESILIA, CEH;

- CoBIT Risk Framework, ISO 27005.

Firmami zajmującymi się cyberbezpieczeństwem są między innymi: Resilia, One Trust, Bird&Bird. Program szkoleń opiera się na rozwiązaniach i metodach stosowanych w edukacji na rzecz cyberbezpieczeństwa w Wielkiej Brytanii i USA i obejmuje:

- pracowników jednostek administracji publicznej;

- pracowników sektora prywatnego, zwłaszcza działów odpowiedzialnych za bezpieczeństwo informacyjne i teleinformatyczne organizacji;

- analityków zagrożeń dla bezpieczeństwa organizacji.

Wiedza oraz umiejętności uzyskane w ramach szkolenia umożliwiają jego uczestnikom branie czynnego udziału w procesach związanych z szeroko pojętym bezpieczeństwem informacji, związanym między innymi z audytowaniem systemów, sieci i magazynów danych pod kątem bezpieczeństwa oraz monitorowaniem, detekcją i analizą zagrożeń oraz naruszeń w systemach informatycznych[44]. Wykształcenie w obszarze bezpieczeństwa sieci oraz systemów informatycznych i telekomunikacyjnych, a także ochrony danych pozwala przede wszystkim na:

- wykorzystanie nowoczesnych narzędzi teleinformatycznych (biblioteki programistyczne, sprzęt sieciowy, protokoły komunikacyjne) w projektowaniu i integracji systemów bezpieczeństwa;

- praktyczne stosowanie narzędzi i technologii związanych z bezpieczeństwem oraz audytowaniem sieci teleinformatycznych w celu zabezpieczania podmiotów gospodarczych i instytucji publicznych;

- obsługę i działanie aplikacji oraz usług elektronicznych w Internecie oraz sieciach lokalnych, rozwiązań zabezpieczających sieci teleinformatyczne (w tym sieci bezprzewodowe);

- projektowanie inteligentnych systemów teleinformatycznych zabezpieczających przez atakami hakerów;

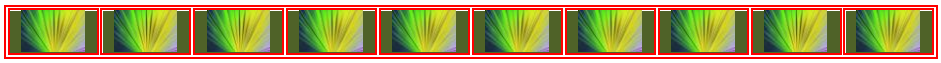
- stosowanie zasad działania podstawowych narzędzi kryptograficznych;

- bezpieczne wirtualizowanie funkcji sieciowych;

- zarządzanie systemami operacyjnymi i uodparniania ich na cyberataki.

[44] https://ktt.pwr.edu.pl/ksztalcenie/cyberbezpieczenstwo.

4. Wytyczne przeciwdziałania atakom hakerskim w zakresie dostępu do baz danych



4.1. Budowa aplikacji z myślą o cyberbezpieczeństwie

Hakerzy to przeważnie pasjonaci języków programowania. Ich doskonała znajomość systemów operacyjnych i różnorodnych języków zwłaszcza ze sfery oprogramowania pracującego mobilnie ”*korci*” do popisywania się przed kolegami z „*fachu*”. Dokonują wtrąceń zdalnych do systemów funkcjonujących, aby one pracowały pod ich dyktando. Powodować to może nawet ogromne zakłócenia w działaniach systemów teleinformatycznych, jak i spowodować wyciek danych z zorganizowanych przeważnie relacyjnych baz danych. Zwłaszcza groźne staje się organizowanie hakerów w różne grupy, które mogą być wykorzystywane do działań terrorystycznych.

Z tego względu budując i administrując systemy informatyczne i korzystając z sieci teleinformatycznych trzeba już na etapie tworzenia lub implementacji, zwłaszcza systemów zintegrowanych klasy ERP, przestrzegać wytycznych w tym zakresie. Ciekawe informacje – w formie wytycznych, z tej tematyki znajdujemy we wcześniej już cytowanej publikacji: *https://networkexpert.pl/cyberbezpieczenstwo/*. Wytyczne te dotyczą projektowania systemów, protokołów, budowy interfejsu oraz doboru metod programistycznych, więc skupmy nieco więcej im uwagi.

Projektowanie z myślą o bezpieczeństwie. Istnieją dwa podstawowe nurty w walce z zagrożeniami bezpieczeństwa. Pierwszym z nich jest możliwie skuteczne zapobieganie powstawaniu takich usterek. Chociaż wyeliminowanie błędów zabezpieczeń w skomplikowanych systemach teleinformatycznych jest w praktyce niemożliwe, zaproponowano szereg metod, które pozwalają na zredukowanie ryzyka pomyłek przy tworzeniu oprogramowania. Wychodząc tej potrzebie opracowane zostało wiele międzynarodowych standardów opisujących metody oceny bezpieczeństwa architektury systemów teleinformatycznych, a przykładem są normy Common Criteria ISO/IEC 15408[5], ITSEC czy FIPS.

Odpowiednia budowa protokołów i interfejsów. W odróżnieniu od drobnych błędów programistycznych, wybór prawidłowej i podatnej na ataki architektury rozwiązania często jest problemem. Typowym przykładem są współczesne kłopoty ze *spamem*, które w dużej mierze wynikają z budowy protokołu SMTP. Ze względu na popularność i znaczenie tego protokołu, znacząca modyfikacja SMTP jest dziś w praktyce niewykonalna. Podobne zasady dotyczą interfejsów użytkownika, tj. ekranów WE/WY, gdy zaprojektowane w nieintuicyjny i niekonsekwentny sposób sprzyjają popełnianiu błędów przez operatora.

Wybór metod programistycznych. Na skutek zmęczenia lub pośpiechu, nawet najlepiej wyszkoleni i doświadczeni programiści mogą popełniać oczywiste dla innych błędy w doborze metody programistycznej, jak również w sekwencji tworzonego przez nich kodu źródłowego, stanowiącego „*komponenty*" połączeń sekwencji różnych języków maszynowych.

4.2. Akty prawne regulujące bezpieczeństwo teleinformatyczne

Wróćmy jednak do tematu podjętego w tym rozdziale, a więc wytycznych formalnych w zakresie bezpieczeństwa teleinformatycznego. Wyszczególnione zostaną teraz podstawowe akty prawne stanowiące zalecenia Służby Kontrwywiadu Wojskowego (SKW), które są następujące[45]:

DBBT-801B – Zalecenia w zakresie bezpieczeństwa teleinformatycznego.

DBBT-803 – Zalecenia w zakresie bezpieczeństwa autonomicznych stacji roboczych oraz sieci lokalnych przetwarzających informacje niejawne.

DBBT-811.1 – Organizacja zarządzania bezpieczeństwem teleinformatycznym. Wprowadzenie i podstawy teoretyczne.

DBBT-811.2 – Metodologia szacowania ryzyka dla systemów teleinformatycznych przetwarzających informacje niejawne.

DBBT-811.3 – Przykład dokumentacji wstępnego szacowania ryzyka prowadzonego zgodnie z zalecaną metodologią dla typowego systemu teleinformatycznego przetwarzającego informacje niejawne.

[45] https://bip.skw.gov.pl/skw/bezpieczenstwo-teleinfo/zalecenia-w-zakresie-be/5109,Zalecenia-w-zakresie-bezpieczenstwa-teleinformatycznego.html.

ZIBT-818A – Zalecenia w zakresie zawartości dokumentacji bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne. Szczególne Wymagania Bezpieczeństwa.

ZIBT-818B – Zalecenia w zakresie zawartości dokumentacji bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne. Procedury Bezpiecznej Eksploatacji.

ZIBT-142 – Zalecenia w zakresie ustawienia zabezpieczeń systemu operacyjnego *Windows 10* w systemach przetwarzających informacje niejawne.

ZBT-101 - Zalecenia w zakresie ustawień zabezpieczeń w środowisku domenowym opartym o system operacyjny *Windows Server 2016* w systemach przetwarzających informacje niejawne.

DBBT-830A – Zalecenia w zakresie stosowania przełączników KVM.

ZIBT-810 – Zalecenia w zakresie sanityzacji informatycznych nośników danych.

DBBT-901A – Zalecenia w zakresie certyfikacji urządzeń i narzędzi kryptograficznych będących rozwiązaniem sprzętowym (elektronicznym), programowym lub sprzętowo-programowym oraz urządzeń służących do składania i weryfikacji podpisu elektronicznego. Obowiązują w zakresie dotyczącym wymagań na dokumentację do certyfikacji.

ZBT-401 – Zalecenia w zakresie urządzeń i narzędzi kryptograficznych przeznaczonych do ochrony informacji niejawnych.

ZBT-402 - Zalecenia dotyczące certyfikacji urządzeń, narzędzi oraz środków służących do ochrony informacji niejawnych.

ZIBT-950B – Zalecenia w zakresie zasad, warunków i zakresu uznawania oraz sprawowania nadzoru nad laboratoriami podmiotów zewnętrznych.

ZOBT-500A – Zalecenia ogólne w zakresie zapewnienia ochrony elektromagnetycznej systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych.

ZBT-601 - Zalecenia w zakresie zarządzania materiałami kryptograficznymi.

ZBT-602 - Zalecenia w zakresie powoływania i odwoływania kancelarii kryptograficznej

ZBIT-690 Zalecenia w zakresie postępowania z materiałami kryptograficznymi zabezpieczającymi pracę urządzeń ochrony kryptograficznej typu GUU-3.

ZIBT-693 – Zalecenia w zakresie postępowania z bezpiecznymi kopertami.

Szeroki jest zakres różnorodnych zaleceń i dlatego na stronie SKW zaproponowano ciąg szkoleń, który obejmuje miedzy innymi zagadnienia[46]:

- podstawowe zasady bezpieczeństwa pracy na komputerze;
- OSINT – *biały wywiad*, czyli jak i gdzie szukać informacji w sieci;
- symptomy zainfekowania komputera (przykłady ataków);
- bezpieczeństwo haseł (budowa, przechowywanie oraz inne bezpieczniejsze metody logowania);
- podstawowe informacje o atakach na użytkowników (socjotechnika, *phishing*, *spearphishing*, *malware*, *pharming*, *spoofing*, *spam*, *spim*, *scam*.

4.3. Dyrektywa NIST i inne

Podane wcześniej zalecenia wynikają z dyrektyw instytucji zagranicznych. Istotną rolę odgrywa tu amerykański NIST (Narodowy Instytut Standardu i Technologii) – zob. obiekt tego Instytutu na rysunku 4.1[47].

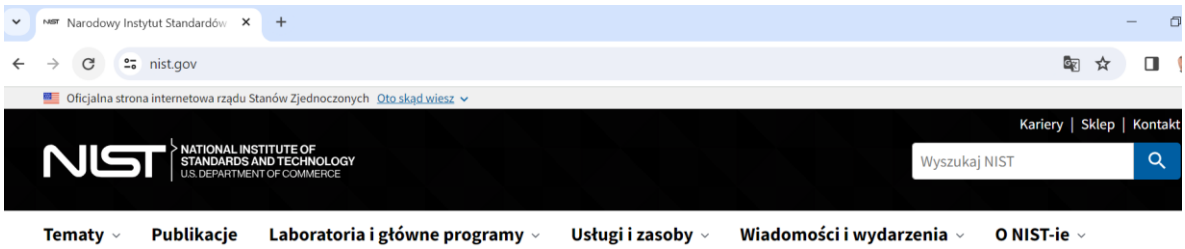
Źródło: https://pl.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology#/media/Plik:NIST_AML_building.jpg.

Rys. 4.1. Budynek NIST

Natomiast fragment strony internetowej wspomnianego Instytutu pokazano na rysunku 4.2. Tematami badawczymi instytutu NIST są zagadnienia dotyczące: sztucznej inteligencji, klimatu, komunikacji, bezpieczeństwa cybernetycznego, zdrowia i biologii, infrastruktury, produkcji oraz nauki kwantowej.

[46] https://bip.skw.gov.pl/skw/bezpieczenstwo-teleinfo/zalecenia-w-zakresie-be/5109,Zalecenia-w-zakresie-bezpieczenstwa-teleinformatycznego.html.

[47] https://pl.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology#/media/Plik:NIST_AML_building.jpg.



Źródło: https://www.nist.gov/.

Rys. 4.2. Fragment strony www instytutu NIST

Trzeba jeszcze wspomnieć o dyrektywie NIS, która została przyjęta 6 lipca 2016 roku[48]. Jest ona pierwszym europejskim prawem w zakresie cyberbezpieczeństwa. Dyrektywa nakłada na państwa członkowskie szereg obowiązków, obliguje je do powołania konkretnych instytucji oraz wprowadzenia mechanizmów współpracy. W Polsce jej zapisy realizuje ustawa o krajowym systemie cyberbezpieczeństwa z 28 sierpnia 2018 roku. Dostęp do obowiązującej dyrektywy NIIS i NIS2 w zakresie cyberbezpieczeństwa następuje poprzez link: *https://cyberpolicy.nask.pl/category/obowiazujace/dyrektywa-nis/* (zob. rysunek 4.3).

Źródło: https://cyberpolicy.nask.pl/category/obowiazujace/dyrektywa-nis/.

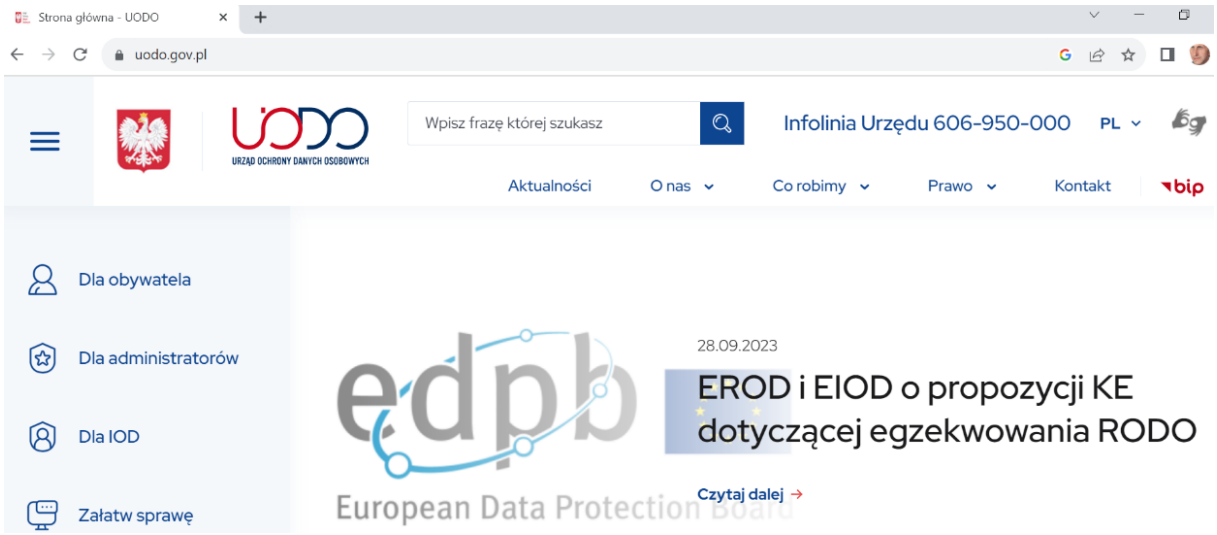
Rys. 4.3. Menu główne strony: cyberpolicy.nask.pl

W styczniu 2023 roku w Brukseli po raz pierwszy odbyło się wydarzenie ENISA EU *Cybersecurity Policy Conference*. Uczestnikami konferencji byli zarówno kluczowi interesariusze, jak i przedstawiciele sektora publicznego i przemysłu. Wśród poruszanych tematów, oprócz kwestii związanych z rozwojem i wyzwaniami w *cyberpolicy*, poruszono

[48] https://cyberpolicy.nask.pl/category/obowiazujace/dyrektywa-nis/.

także tematy związane z wdrażaniem regulacji prawnych z obszaru cyberbezpieczeństwa, aktualnym statusem Dyrektywy NIS 2, wprowadzeniem CVD (skoordynowanego ujawniania podatności), a także *Aktu o cyberodporności* (*Cyber Resilience Act*) i DORA. Podczas panelu zaprezentowano ciekawe spostrzeżenia z poszczególnych krajów w przedmiocie aktualnego statusu adaptacji Dyrektywy NIS 2, a także wyzwań związanych z CVD (takich jak zróżnicowane prawo karne dotyczące działalności etycznych hakerów.

Ogólne rozporządzenie o ochronie danych, inaczej rozporządzenie o ochronie danych osobowych GDPR (*General Data Protection Regulation*) lub w polskiej wersji RODO to rozporządzenie unijne, zawierające przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych[49]. Celem rozporządzenia jest doprowadzenie do pełnej harmonizacji prawa w ramach UE i swobodnego przepływu danych osobowych. Warto też sięgnąć do strony: *https://www.uodo.gov.pl/*, gdzie możemy znaleźć aktualne informacje publikowane przez Urząd Ochrony Danych Osobowych (UDO) – zob. rysunek 4.4[50].



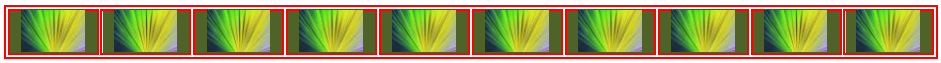
Źródło: https://www.uodo.gov.pl/.

Rys. 4.4. Strona tytułowa Urzędu Ochrony Danych Osobowych

Z wcześniejszego wyszczególnienia zaleceń dotyczących bezpieczeństwa teleinformatycznego wynika, że część z nich reguluje postępowanie z informacjami niejawnymi. Zatem w ochronie zasobów cyfrowych przed atakami cyberprzestępców należy też przestrzegać szczegółowe uregulowania GDPR/RODO dotyczące danych osobowych.

[49] https://pl.wikipedia.org/wiki/Og%C3%B3lne_rozporz%C4%85dzenie_o_ochronie_danych.
[50] https://www.uodo.gov.pl/.

5. Zakres działalności administratorów sieci i systemów w obszarze ochrony przed dostępem do zasobów oraz usług informatycznych



5.1. Szkolenia doskonalające umiejętności administratorów systemów

Rozwiązania informatyczne stają się coraz bardziej skomplikowane. Dotyczy to zarówno *hardware* jak i *software*. Dla utrzymania ciągłości i niezawodności ich działania administratorzy sieci oraz systemów obiektowych muszą stale doskonalić swoje umiejętności. W tym rozdziale zwrócono uwagę na zakres prowadzonych szkoleń dla wymienionej grupy informatyków. Szkolenia prowadzone są przez wyspecjalizowane instytucje i przybierają np. formę warsztatów nabrania wprawy w ochronie informacji niejawnych oraz zabezpieczeń w zakresie niepożądanych dostępów, w tym z cyberprzestrzeni. *Warsztaty* skierowane są zwłaszcza do administratorów systemu i inspektorów bezpieczeństwa teleinformatycznego[51]. Ponadto w ograniczonym zakresie do dyrektorów i kierowników działów IT, pełnomocników ochrony, a w szczególności tych, którzy zamierzają ubiegać się o akredytację oraz stoją przed problemem stworzenia dokumentacji bezpieczeństwa stosowanej technologii informatycznej. Podczas zajęć omówione zostają wprowadzone zmiany w ustawie o ochronie informacji niejawnych dotyczące oznakowania i rejestracji środków ochrony elektromagnetycznej oraz szacowanie ryzyka dla bezpieczeństwa przetwarzanych informacji niejawnych i zarządzanie tym ryzykiem.

Osobnym zakresem jest przekazywanie wiedzy dotyczącej *bezpieczeństwa teleinformatycznego* (BTI). Uczestnicy szkolenia dowiadują się o zasadach wynikających z rozporządzenia PRM z 20 lipca 2011 w sprawie wymagań BTI. Ponadto uczestnicy szkolenia nabierają umiejętności w szacowaniu ryzyka w świetle ustawy z dnia 5 sierpnia 2010 o ochronie informacji niejawnych – podstawowe wymagania. Normy ISO 27001 oraz 27005. Na szczególną uwagę zasługuje poznanie zabezpieczeń systemowych w sytuacji korzystania z outsourcingu IT. Określona firma softwarowa świadcząca usługi informatyczne przeważnie realizuje działania wymienione w tabeli 5.1.

[51] https://www.ksoin.pl/szkolenia/bezpieczenstwo-teleinformatyczne/.

Tab. 5.1. Działania firmy świadczącej usługi informatyczne w zakresie cyberbezpieczeństwa

Działania	Efekty działań
Audyt bezpieczeństwa IT	Pełna ocena zabezpieczeń stosowanych przez firmę w tym analiza używanych programów antywirusowych, infrastruktury sieciowej, bezpieczeństwa danych, aplikacji i sprzętu IT. Wykonanie testów penetracyjnych, analiza procedur stosowanych przez firmę wraz z ewentualnym planem naprawczym oraz wskazówkami czy można zoptymalizować koszty bezpieczeństwa informatycznego.
Interwencja w przypadku awarii	Ekspercka pomoc doświadczonych inżynierów IT, którzy pomogą usunąć awarię oraz wprowadzą rozwiązania minimalizujące ryzyko przyszłych incydentów w obszarze IT przedsiębiorstwa. Uszczelnienie zabezpieczeń, regularne tworzenie *backupów* – kopii bezpieczeństwa, bieżący nadzór nad infrastrukturą IT, odzyskiwanie i naprawa danych utraconych lub uszkodzonych po awarii systemu/ataku hakerskim/wirusie komputerowym.
Przeglądy konfiguracyjne	Ocena czy zakupione oprogramowanie antywirusowe jest prawidłowo skonfigurowane. Konfiguracja używanych w firmie programów pod kątem określonych zagrożeń.
Wdrażanie systemów bezpieczeństwa	*Kompleksowe działanie zabezpieczające przed atakami:* *- analiza potrzeb, projektowanie, wdrażanie i ocena funkcjonowania systemów bezpieczeństwa w firmie;* *- wdrożenie systemów ochrony baz danych DAM;* *- systemów zarządzania kontami uprzywilejowanymi oraz kontroli dostępu do sieci firmowej;* *- systemów ochrony aplikacji, SIEM, czyli zbierających informacje o bezpieczeństwie i ułatwiających zarządzanie zdarzeniami;* *- systemów obsługi incydentów;* *- systemów poprawiających bezpieczeństwo pracy zdalnej,* *- zestawienie bezpiecznych łączy VPN;* *- projektowanie bezpiecznych sieci firmowych;* *- pełnej ochrony danych zgodnie z RODO;* *- zabezpieczeń antimalware, antiphishing, antyspam oraz antyransomware.*
Szkolenia dla pracowników z cyberbezpieczeństwa	Praktyczna wiedza jak działają hakerzy, jak uniknąć ryzyka utraty danych w codziennej pracy w środowisku IT, jak zadbać o bezpieczeństwo w Internecie.

https://twojepc.pl/news42344/Jak-zadbac-o-bezpieczenstwo-teleinformatyczne-w-firmie.html.

5.2. Odpowiedzialność firmy/instytucji za stan zabezpieczenia baz danych

Zapewnienie odpowiedniego poziomu bezpieczeństwa teleinformatycznego jest obowiązkiem każdej firmy produkującej, czy też świadczącej usługi[52]. Wynika to przede wszystkim z faktu, że przedsiębiorstwo odpowiada za właściwe zabezpieczenie gromadzonych i przetwarzanych danych. Niedopilnowanie tego obowiązku może skutkować wyciekiem danych, za co mogą zostać nałożone surowe kary finansowe (zgodnie z RODO). W sytuacji ataku cyberprzestępców może chodzić również o wyłącznie używanych systemów, czy wprowadzenie w nich zmian, co będzie skutkowało pojawianiem się błędów w pracy systemów operacyjnych, czy też aplikacji branżowych. W związku z tym każde oprogramowanie musi posiadać odpowiednie zabezpieczenia, a jego działanie powinno być stale monitorowane.

Wobec nadmiaru obowiązków administratorów systemów stosowanych obszarów informatyki, niektóre duże firmy powołują jeszcze specjalistów ds. cyberbezpieczeństwa[53]. Zakres zadań zawodowych tego specjalisty obejmuje przede wszystkim:

- utrzymywanie i rozwój systemów bezpieczeństwa teleinformatycznego;

- formułowanie wymagań bezpieczeństwa dla projektów i rozwiązań wdrażanych w organizacji w zakresie bezpieczeństwa teleinformatycznego;

- planowanie i wdrażanie rozwiązań z zakresu cyberbezpieczeństwa;

- opracowywanie procedur awaryjnych, scenariuszy reakcji na ataki cybernetyczne;

- obsługiwanie incydentów oraz prowadzenie analizy powłamaniowej do systemów teleinformatycznych;

- tworzenie polityk, standardów i procedur bezpieczeństwa teleinformatycznego, w tym sprawowanie nadzoru nad aktualnością procedur "*Disaster Recovery/Business Continuity*" oraz ścisła współpraca z Pełnomocnikiem ds. Ochrony Informacji Niejawnych w zakresie aktualizacji polityki bezpieczeństwa wdrożonej w organizacji;

- programowanie systemów w językach skryptowych: *perl*, *bash*, *python* lub innych językach wysokiego poziomu bezpieczeństwa teleinformatycznego;

- konfigurowanie i zarządzanie bezpieczeństwem aktywnych urządzeń sieciowych, systemu pocztowego oraz stacjami roboczymi poprzez *Active Directory*;

[52] https://twojepc.pl/news42344/Jak-zadbac-o-bezpieczenstwo-teleinformatyczne-w-firmie.html.
[53] https://psz.praca.gov.pl/rynek-pracy/bazy-danych/klasyfikacja-zawodow-i-specjalnosci/wyszukiwarka-opisow-zawodow/-/klasyfikacja_zawodow/zawod/252902?p_p_state=pop_up&_jobclassificationportlet_WAR_nnkportlet_viewMode=print.

- obsługa systemów bezpieczeństwa, tj.: IDS/IPS, FW, AV, SIEM, LM, NAC, FDE, DLP, protokołów sieciowych ISO1-7, serwerów Unix/Linux, Microsoft oraz tworzenie zapytań SQL.

Specjalista ds. cyberbezpieczeństwa powinien znać organizację eksploatowanych systemów zarzadzania bazami danych. Z tego względu, zwłaszcza dla przyszłych początkujących adeptów sztuki ochrony sieci teleinformatycznych i cyberbezpieczeństwa, warto teraz przedstawić rodzaje baz danych.

5.3. Stosowane bazy danych

Model bazy danych to zbiór zasad (specyfikacji), opisujących strukturę danych w tej bazie, przy czym określane są również dozwolone operacje[54]. Definiuje się strukturę danych poprzez specyfikację reprezentacji dozwolonych w modelu obiektów (encji) oraz ich związków. Trzeba dodać, że w informatyce głównymi modelami baz danych są:

- hierarchiczny model danych,
- relacyjny model danych,
- sieciowy model danych,
- obiektowy model danych,
- sieci semantyczne,
- logiczny model danych,
- temporalny model danych.

Hierarchiczny model danych przypomina strukturę organizacyjną przedsiębiorstwa. Natomiast w relacyjnym modelu danych dane grupowane są w relacje, które reprezentowane są przez tabele[55]. Relacje są pewnym zbiorem rekordów o identycznej strukturze wewnętrznie powiązanych za pomocą związków zachodzących pomiędzy danymi. Relacje zgrupowane są w tzw. schematy bazy danych. Relacją może być tabela zawierająca dane teleadresowe pracowników, zaś schemat może zawierać wszystkie dane dotyczące firmy. Jak już wspomniano, dane w modelu relacyjnym przechowywane są w tabelach, z których każda ma stałą liczbę kolumn i dowolną liczbę wierszy. Każda tabela (relacja) ma zdefiniowany klucz danych (*key*) – wyróżniony atrybut lub kilka takich atrybutów, którego wartość jednoznacznie

[54] https://pl.wikipedia.org/wiki/Model_bazy_danych.
[55] https://pl.wikipedia.org/wiki/Model_relacyjny.

identyfikuje dany wiersz. Wyszukiwanie danych odbywa się za pomocą odwołania się programu do danego klucza i identyfikacji danego wiersza za jego pomocą.

Model sieciowej bazy danych stanowi zmodyfikowana wersja modelu hierarchicznego, pozwalająca na definiowanie relacji wiele-wiele w postaci struktury drzewiastej bez powtarzania poszczególnych wartości w ramach obiektu danych[56]. Model sieciowy korzysta z rekordów i zbiorów, przy czym:

- rekordy zawierają pola przechowujące dane;

- zbiory określają relację jeden-do-wielu między rekordami, gdzie jeden rekord jest „*właścicielem*" zbioru zawierającego „*członków*" zbioru,

- jeden rekord może być zarówno „*właścicielem*", jak i „*członkiem*" wielu zbiorów.

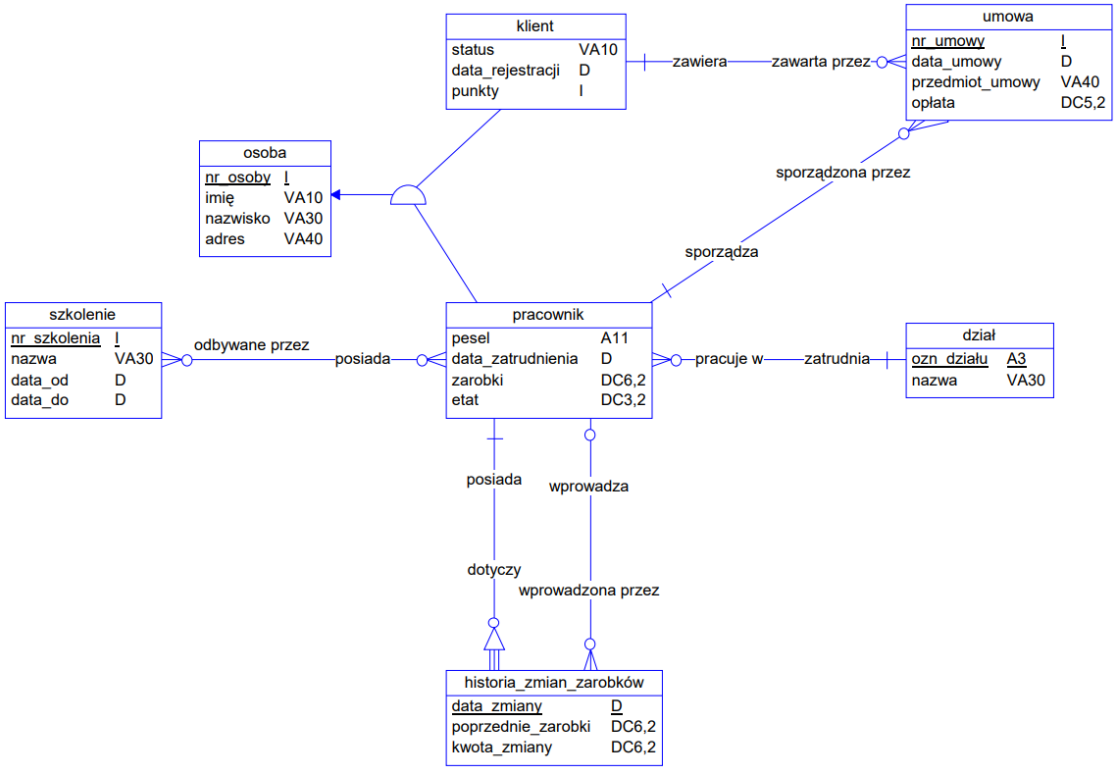
Obiektowa baza danych obejmuje zbiór obiektów, których zachowanie się, stan oraz związki są określone zgodnie z obiektowym modelem danych[57]. Obiektowy system zarządzania bazą danych jest systemem wspomagającym definiowanie, zarządzanie, utrzymywanie, zabezpieczanie i udostępnianie obiektowej bazy danych.

Sieci semantyczne (*Semantic Web*) stanowią rozwiązanie, które ma przyczynić się do utworzenia i rozpowszechnienia standardów opisywania treści w Internecie w sposób, który umożliwi maszynom i programom (tzw. agentom) przetwarzanie informacji w sposób odpowiedni do ich znaczenia[58]. Wśród standardów sieci semantycznych znajdują się m.in. OWL, RDF, *RDF Schema* (inaczej RDFS). Znaczenia zasobów informacyjnych określa się za pomocą tzw. *ontologii*.

Logiczny model danych. W celu utworzenia tego modelu wykorzystamy jest program *Data Architect*, wchodzący w skład pakietu narzędzi *CASE Power Designer*, który pozwala utworzyć logiczny - konceptualny model danych (CDM), fizyczny model danych (PDM) oraz wygenerować skrypt SQL tworzący bazę danych[59]. Na wstępie określa się zbiory encji oraz ich atrybuty (wraz z określeniem typu danych, wymagalności, ograniczeń) i klucze główne. Pomiędzy tak zdefiniowanymi zbiorami encji kreśli się relacje o określonych własnościach. Wszystko to odbywa się w trybie graficznym. Przykładowy model logiczny bazy danych do rejestracji danych klientów i pracowników, z wyszczególnieniem atrybutów poszczególnych

[56] https://pl.wikipedia.org/wiki/Sieciowa_baza_danych.
[57] https://pl.wikipedia.org/wiki/Obiektowa_baza_danych.
[58] https://pl.wikipedia.org/wiki/Semantic_Web.
[59] http://staff.uz.zgora.pl/afiedoro/pliki/modelowanie1.pdf.

encji (wraz z ich dziedzinami), kluczy głównych (podkreślone atrybuty) oraz związków pomiędzy encjami pokazano na rysunku 5.1[60].



Źródło: http://staff.uz.zgora.pl/afiedoro/pliki/modelowanie1.pdf.

5.1. Schemat przykładowego modelu logicznego utworzony za pomocą programu *Data Architect* z *pakietu Power Designer*

Temporalna baza danych posiada informację o czasie wprowadzenia lub czasie ważności zawartych w niej danych[61]. Temporalne bazy danych są często administrowane automatycznie, poprzez usuwanie nieaktualnych danych lub ich archiwizowanie.

5.4. Narzędzia programistyczne logowania do usług komputerowych

Są różne aplikacje chroniące dostępu nieupoważnionych osób do zasobów i funkcji systemów komputerowych. Wspomnieć należy chociażby o dwóch z nich, a mianowicie: *token kryptograficzny*, *smart card*. *Tokeny kryptograficzne* są urządzeniami, które umożliwiają zdalne uwierzytelnienie użytkownika, przy użyciu jedynie sprzętów

[60] Ibidem.
[61] https://pl.wikipedia.org/wiki/Temporalna_baza_danych.

elektronicznych lub programów komputerowych[62]. Są zwykle używane jako dodatkowe sposoby autoryzacji, zwykle razem z normalnymi hasłami. Tokeny mogą być zarówno urządzeniami elektronicznymi jak i programami działającymi na komputerach lub urządzeniach mobilnych. W zależności od implementacji, *tokeny kryptograficzne* są również nazywane tokenami uwierzytelniającymi, tokenami sprzętowymi lub programowymi, ewentualnie tokenami USB. Niezależnie od typu, wszystkie tokeny kryptograficzne służą realizowaniu jednego zadania: dostarczania kodu uwierzytelniającego użytkownika. Zazwyczaj *token kryptograficzny* wymaga podania hasła, które umożliwia odczytanie wewnętrznego kodu autoryzacyjnego. Hasło przyjmuje zwykle formę krótkiego numeru *PIN*. Popularną metodą jest wyświetlanie kodu na wyświetlaczu urządzenia, tak aby użytkownik mógł przedstawić go na żądanie we właściwym momencie.

Dwuetapowa weryfikacja logowania do usług komputerowych to najbardziej zalecana praktyka bezpieczeństwa, przy czym taka autoryzacja przybiera różną formę. Może być to dodatkowe hasło, kod *PIN*, losowy ciąg znaków z aplikacji lub rozpoznawanie twarzy. Wciąż stosowaną formą dwuetapowej autoryzacji logowania jest wykorzystanie karty inteligentnej i czytnika *Smart Card*[63]. Takie rozwiązanie wymaga jednak od użytkownika potwierdzenia jego tożsamości.

5.5. Wspomaganie ochrony zasobów informatycznych poprzez instalowanie programów antywirusowych

Występuje duża różnorodność aplikacji chroniących system użytkownika przed zagnieżdżeniem się wirusa. Nowe złośliwe programy wirusowe stale powstają. Po rozpoznaniu otrzymują one nazwy i biura oprogramowania starają się je neutralizować poprzez opracowanie i testowanie programów antywirusowych. Wybór najlepszego oprogramowania antywirusowego dla komputera może być jednak trudnym zadaniem ze względu na wszystkie kryteria, które należy wziąć pod uwagę[64]. Potrzebne jest bowiem proste rozwiązanie zabezpieczającego np. komputer PC lub laptop użytkownika albo najbardziej zaawansowany system ochrony dla całej rodziny, który zapewnia ochronę nie tylko przed wirusami, ale również przed atakami hakerów i wyłudzeniami.

[62] http://www.crypto-it.net/pl/narzedzia/token-kryptograficzny.html.
[63] https://www.onexstore.pl/blog/malo-popularna-metoda-logowania-omawiamy-czym-jest-smart-card/.
[64] https://www.antivirusguide.com/pl/najlepszy-antywirus/?

Światowym liderem w dziedzinie bezpieczeństwa IT jest Norton, znana marka oprogramowania antywirusowego. Firma ta zdobyła wiele nagród za najlepsze programy antywirusowe od wiodących laboratoriów testujących *online*, takich jak *AV Comparatives, AV Test, PcMag* i *The Anti-Malware Testing Standard Organization*. Przykładem skutecznego produktu jest *Norton AntiVirus Plus*[65]. Spośród innych programów antywirusowych na uwagę zasługują: *Norton 360 Deluxe, Total AV, Avast, Bitdefender, panda, PCPROTECT, MCAfee*.

Oprogramowanie antywirusowe dzięki ochronie przed złośliwym oprogramowaniem (*malware*) w czasie rzeczywistym może przede wszystkim zapobiec zainfekowaniu systemu przez program tej kategorii. Jednak nowoczesne antywirusy to znacznie więcej niż tylko skanery złośliwego oprogramowania. Oferowane są z szeroką gamą dodatkowych narzędzi, które chronią podczas korzystania z Internetu. Najlepsze marki udostępniają funkcje bezpieczeństwa, takie jak zabezpieczenia sieciowe do ochrony podczas przeglądania Internetu, zapory sieciowe do monitorowania ruchu przychodzącego i wychodzącego, wirtualne sieci prywatne (VPN) zapewniające prywatność sesji *online*, kontrolę rodzicielską, która pomaga zapewnić bezpieczeństwo dzieciom w Internecie oraz menedżery haseł, zapewniające ochronę haseł przed ich złamaniem. Zainstalowanie dobrego programu antywirusowego renomowanej, godnej zaufania firmy jest niezbędne do ochrony danych i urządzeń przed znanym i pojawiającym się złośliwym oprogramowaniem.

W uzupełnieniu tego materiału, dotyczącego programów antywirusowych, wspomnę o aplikacji *Endpoint Antivirus*, która zainstalowana jest na moim laptopie DELL (zob. rysunek 5.2).

Źródło: https://shorter.me/6sVqH.

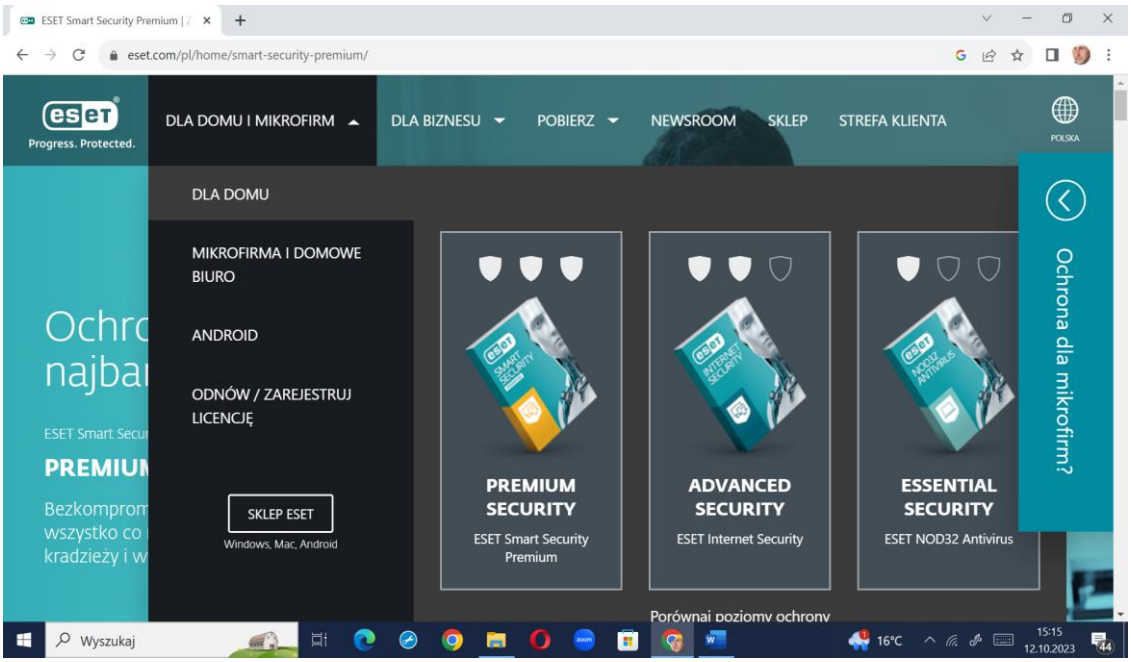
5.2. Strona tytułowa programu antywirusowego *Endpoint Antivirus* firmy eset

[65] https://pl.norton.com/products/norton-360-antivirus-plus?API1=100&API2=8848779&cjid=8848779&cjevent=b84eaf4768dd11ee80f4004a0a18b8fb.

Według producenta wspomnianego programu antywirusowego wskazany jest on dla użytkowników, którzy troszczą się o swoją prywatność podczas korzystania z Internetu do zakupów, bankowości elektronicznej, pracy i komunikacji. Wymieniony program zabezpiecza nawet do 9. urządzeń z systemem *Windows*, *macOS* i *Android*.

Proponuję jeszcze zmiankę o firmie eset[66]. Jest to słowackie przedsiębiorstwo informatyczne z siedzibą w Bratysławie, założone w roku 1992. Zajmuje się tworzeniem oprogramowania antywirusowego. Produkty firmy eset zabezpieczają urządzenia z systemem *Windows*, *MacOS*, *Linux*, *Android*, *iOS*, *Microsoft Azure*, *Microsoft Windows Server*, *Microsoft Exchange Server*, *VMware*, BSD, *Lotus Domino*. Wymieniona firma oferuje różne rodzaje pakietów antywirusowych z podziałem dla domu i mikrofirm oraz dla większego biznesu[67]. W wariancie dla domu i mikrofirm występują następujące rozwiązania (zob. rysunek 5.3)[68]:

- *Premium Security*,
- *Advanced Security*,
- *Essential Security*.

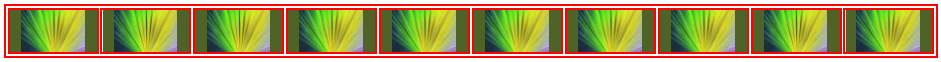


Źródło: https://www.eset.com/pl/home/smart-security-premium/.

Rys. 5.3. Propozycje pakietów programu antywirusowych dla instalacji komputerowych domowych

[66] https://pl.wikipedia.org/wiki/Eset.
[67] https://pl.wikipedia.org/wiki/Eset.
[68] https://www.eset.com/pl/home/smart-security-premium/.

6. Analiza przestrzeni programowej w celu zablokowania przed wejściem złośliwego oprogramowania



6.1. Pojęcie „*złośliwe oprogramowanie*”

Zalecane procedury testowania oprogramowania, pod kątem otwartości aplikacji na niepożądane „*wstawki*” programowe, w postaci sekwencji złośliwego oprogramowania (*malware*) spotykamy w już cytowanej publikacji internetowej: *https://networkexpert.pl/cyberbezpieczenstwo/*. Aby zapobiegać temu zjawisku, stworzono języki, które w odróżnieniu np. od *C++* lub *Javy* wymagają od programistów przestrzegania ścisłego rygoru pracy, zmierzającego do wyeliminowania niepewnych struktur tworzonych programów, przykładem takiego języka jest Ada.

W budowie aplikacji sugeruje się różne bezpieczne metody programistyczne oraz stosowanie niewielkich, przejrzystych i łatwych do weryfikacji bloków funkcjonalnych. Metody te wymagają jednak dodatkowego przeszkolenia programistów. Z tego względu stosowane powinny być operacje weryfikujące opracowany program źródłowy, które dalej zostaną przedstawione[69].

Testowanie aplikacji, ponieważ zapewnianie jakości oprogramowania powinno uwzględniać także weryfikację bezpieczeństwa zaimplementowanych rozwiązań technologicznych.

Przegląd kodu źródłowego, polegający na kontroli kodu w poszukiwaniu potencjalnie niebezpiecznych konstrukcji lub oczywistych pomyłek. Może być dokonane ze wsparciem narzędzi automatycznych typu *Flawfinder, Splint, Cqual*.

Testy typu czarna skrzynka, mające na celu badanie zachowania się programu, bez dodatkowej wiedzy o sposobie wewnętrznej konstrukcji programu. Może być przeprowadzona ręcznie, często przy wykorzystaniu *debuggerów* lub za pomocą

[69] W opracowaniu tego fragmentu bazowano na tekście zamieszczonym w publikacji internetowej pod linkiem: *https://networkexpert.pl/cyberbezpieczenstwo/*.

specjalizowanych skanerów zabezpieczeń takich jak *Nmap, Nessus, WebInspect*. Wadą tej procedury jest trudność w diagnozowaniu szczegółowych problemów implementacyjnych.

Testy siłowe, przeprowadzane są za pomocą narzędzi zautomatyzowanego losowego testowania (*fuzzing*). Polegają na generacji przypadkowych danych wejściowych i obserwowaniu zachowania programu. Zaletą jest pełna automatyzacja procesu i możliwość ujawnienia bardzo złożonych błędów wynikających z interakcji z systemem operacyjnym.

Formalne dowodzenie poprawności, które zakłada, że istnieje potencjalna możliwość wykorzystania systemów automatycznego dowodzenia twierdzeń do zbadania, czy napisana sekwencja kod programu spełnia oczekiwania jego twórcy. Powstały też pewne inne rozwiązania, a do przykładów zaliczyć można *proste mikrojądro systemu Coyotos*, czy *Extremely Reliable Operating System*. W praktyce jednak sprowadzają się one realizacji do następujących operacji[70]:

a) *Pomiar bezpieczeństwa*, a przykładem działań mających na celu ocenę stanu ochrony teleinformatycznej jest audyt informatyczny. Trzeba tu jeszcze przytoczyć definicję bezpieczeństwa teleinformatycznego zaproponowaną przez Krzysztofa Lidermana:

Bezpieczeństwo teleinformatyczne oznacza poziom uzasadnionego (np. analizą ryzyka) zaufania, że potencjalne straty wynikające z niepożądanego (przypadkowego lub świadomego) ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej i przesyłanej za pomocą systemów teleinformatycznych nie zostaną poniesione.

b) *Pomiar błędów w systemach*, przy czym w tym zakresie stosowane są różne miary, a szczególne wątpliwości budzą porównania opierające się na zliczaniu błędów bez uwzględnienia ich faktycznej wagi i ryzyka, które się z nim wiąże. Ponadto zliczanie wyłącznie błędów potwierdzonych i poprawionych przez producenta. Przykładem takiego kontrowersyjnego porównania była sponsorowana przez firmę Microsoft analiza, która wykazała, że system operacyjny *Linux* jest bardziej podatny na ataki niż *Windows*.

W celu ujednolicenia metodyki pomiaru wagi błędów stworzono miarę podstawową CVSS (*Common Vulnerability Scoring System*), która jest formułą pozwalającą na wyliczenie bezwzględnej wagi błędu na podstawie jego cech systematycznych. CVSS stosowany jest między innymi w katalogach błędów (CVE) oraz przez producentów komercyjnych skanerów podatności (np. Qualys).

[70] Ibidem.

Zakłada się, że cyberbezpieczeństwo może być zapewnione tylko systemowo, tzn. bez pozostawiania wrót do ataków cybernetycznych[71]. Są one obecnie coraz powszechniejszym zjawiskiem, a ich celem są nie tylko komputery i całe systemy teleinformatyczne, ale również telefony komórkowe. Wiele z tych wrót zwanych *backdoorami* znajduje się w sprzęcie i jego oprogramowaniu, które jest w ten sprzęt wbudowane. Polska od lat nie produkuje układów scalonych, które są podstawowymi elementami wszystkich urządzeń teleinformatycznych i w związku z tym zmuszona jest akceptować ryzyka związane z ich stosowaniem. Tak więc nie możemy do końca panować nad własnym bezpieczeństwem teleinformatycznym, a koszty ponoszone już dziś w związku z zapewnieniem minimalnych gwarancji tego bezpieczeństwa są znaczne.

Coraz w szerszym zakresie uczelnie polskie wychodzą naprzeciw pojawiającemu się zagrożeniu w sieci oraz w systemach teleinformatycznych[72]. W ofertach szkoleniowych proponowane są kursy dla nowych specjalności w obszarze „*Bezpieczeństwo systemów informatycznych*", a także „*Cyberbezpieczeństwo*", odniesione przede wszystkim do pakietów informatycznych. Praca przyszłego specjalisty będzie miała na celu rozpoznanie i analizę śladów niebezpieczeństwa w cyberprzestrzeni. Stąd też wymagane jest od specjalistów poznanie między innymi języków programowania obiektowego i skryptowego, zagadnień bezpieczeństwa sieci LAN/WAN/WiFi. Ponadto konieczne jest orientowanie się na czym polega bezpieczeństwo wirtualizacji systemów operacyjnych, bezpieczeństwo *cloud,* bezpieczeństwo IoT. Mam nadzieję, że niniejsze opracowanie będzie też małym kroczkiem w poznaniu rozległej problematyki cyberbezpieczeństwa.

Odnieśmy jednak teraz poznanie cyberzabezpieczenia do obszaru konkretnego przedsiębiorstwa, czy też instytucji, gdyż zapewnienie odpowiedniego poziomu bezpieczeństwa w firmie to kwestia kluczowa[73]. Oczywiście nie jest to proste, ponieważ cyberprzestępcy nieustannie pracują nad nowymi formami cyberataków, które mają na celu ominięcie istniejących zabezpieczeń. W związku z tym należy szacować potencjalne ryzyko oraz diagnozować rodzaj ewentualnych zagrożeń. Tak więc, firma powinna mieć opracowany program bezpieczeństwa, w którym należy zawrzeć definicje potencjalnych zagrożeń, a także instrukcje postępowania w przypadku ich wystąpienia.

[71] http://www2.ite.waw.pl/docs/pl/inne/20161130_POLPUS_prasa.pdf.
[72] https://www.wsb.pl/gdansk/studia-i-szkolenia/studia-ii-stopnia/kierunki-i-specjalnosci/informatyka/bezpieczenstwo-systemow-teleinformatycznych.
[73] https://twojepc.pl/news42344/Jak-zadbac-o-bezpieczenstwo-teleinformatyczne-w-firmie.html.

Jak już podkreślano, rozpatrując temat zagrożeń z cyberprzestrzeni, już na początku trzeba sobie określić rozumienie pojęcia „*złośliwe oprogramowanie*" (*malware*)[74]. Termin ten obejmuje fragmenty kodu i programy, które szkodzą systemom operacyjnym, jak i użytkowym, a także systemom sterującym pracą sieci teleinformatycznych. Wrogie, inwazyjne i celowo dokuczliwe złośliwe oprogramowanie ma na celu inwazję, uszkodzenie lub dezaktywację komputerów, systemów komputerowych, sieci, tabletów i urządzeń przenośnych, często przez częściowe przejęcie kontroli nad działaniem urządzenia. *Malware* może ukraść, zaszyfrować lub usunąć dane, zmienić lub przechwycić podstawowe funkcje komputera i szpiegować działania na komputerze bez wiedzy i akceptacji użytkownika. Obecność *malware* może się przejawiać na wiele różnych sposobów, a mianowicie[75]:

a) *Komputer działa wolniej,* co skutkuje znacznym oczekiwaniem w pracy systemu operacyjnego, bez względu na to, czy nawiguje się po Internecie czy uruchamia aplikacje lokalne.

b) *Natłok denerwujących reklam*, objawiający się nieoczekiwanym pojawianiem się wyskakujące reklam. Zwykle są one powiązane z rodzajem złośliwego oprogramowania znanego pod nazwą *adware*.

c) *System często się zawiesza,* przy czym pojawia się niebieski ekran (BSOD, *Blue Screen of Death*), który może wystąpić w systemach *Windows* po wystąpieniu błędu fatalnego.

d) *Tajemnicza utrata miejsca na dysku,* a spowodowane to może być działaniem złośliwego oprogramowania, które ukrywa się na dysku twardym.

e) *Nadmierny wzrost aktywności internetowej*.

f) *Wykorzystanie zasobów systemowych jest nienormalnie wysokie,* przy czym wentylator komputera zaczyna działać z pełną prędkością, bowiem aktywność złośliwego oprogramowania pochłania zasoby systemowe w tle.

g) *Strona startowa przeglądarki zmienia się bez pozwolenia operatora,* a odsyłacze, które klikamy, wysyłają do miejsc innych niż oczekiwane. Przeglądarka może działać bardzo wolno.

h) *W przeglądarce nieoczekiwanie pojawiają się paski narzędzi,* rozszerzenia lub wtyczki.

[74] https://pl.malwarebytes.com/malware/.
[75] Ibidem.

i) *Program antywirusowy przestaje działać*, przy czym tak zachowuje się słynne oprogramowanie *ransomware*, które oznajmia, że jest zainstalowane, informuje, że przejął dane i żąda okupu za zwrot plików.

6.2. Kategorie *malware*

Pomysły hakerów nie mają granic, bowiem pojawiają się wciąż nowe rozwiązania programistyczne. Według dotychczasowego rozpoznania „*złośliwe oprogramowanie*" (*malware*) można podzielić na następujące kategorie[76]:

Adware jest niechcianym oprogramowaniem służącym do wyświetlania reklam na ekranie użytkownika, najczęściej w oknie przeglądarki internetowej. Zazwyczaj programy te wykorzystują różne metody podszywania się pod żądane aplikacje lub podczepiają się do nich, aby skłonić nas do zainstalowania ich na eksploatowanym komputerze, tablecie lub urządzeniu mobilnym.

Oprogramowanie szpiegujące to złośliwe oprogramowanie, które potajemnie obserwuje działania użytkownika komputera bez jego zgody.

Wirus to wspomniane już złośliwe oprogramowanie, które dołącza się do innego programu, a po uruchomieniu powiela się, modyfikując inne programy komputerowe i zarażając je własnymi bitami kodu.

Robaki to oprogramowanie podobne do wirusów, samopowielające się i infekujące inne komputery przez sieć, które powoduje szkody, niszcząc dane i pliki.

Trojan lub *koń trojański* to jeden z najniebezpieczniejszych typów złośliwego oprogramowania. Zazwyczaj podszywa się pod coś pożytecznego. *Koń trojański* może być wykorzystywany do kradzieży informacji finansowych lub instalowania zagrożeń, takich jak wirusy i oprogramowanie *ransomware*.

Ransomware to wspomiane już złośliwe oprogramowanie, które blokuje urządzenie i pliki, a następnie zmusza użytkownika do zapłacenia okupu, aby je odzyskać. Oprogramowanie *ransomware* czasem jest nazywane bronią cyberprzestępców, ponieważ żąda szybkiego, wysokiego haraczu.

Rootkit to rodzaj złośliwego oprogramowania, który nadaje atakującemu uprawnienia administratora w zainfekowanym systemie.

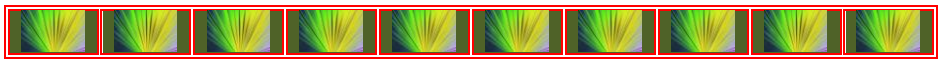
[76] https://pl.malwarebytes.com/malware/.

Keylogger to złośliwe oprogramowanie, które zapisuje wszystkie naciśnięcia klawiszy użytkownika na klawiaturze, zazwyczaj przechowuje zebrane informacje i wysyła je do atakującego.

Złośliwy cryptomining, określany czasem jako *drive-by mining* lub *cryptojacking*, to coraz bardziej rozpowszechnione *malware* instalowane zazwyczaj przez *konia trojańskiego*. Umożliwia ono atakującemu wykorzystywanie komputera do zdobywania kryptowalut, takich jak *bitcoin* lub *monero.*

Exploity to rodzaj złośliwego oprogramowania, które wykorzystuje błędy i słabe punkty w systemie, aby umożliwić przejęcie kontroli.

7. Metody i programy ochrony przed cyberprzestępczością



7.1. Strategie zabezpieczenia systemów

Pewne elementy zapobiegania cyberprzestępczości wystąpiły już we wcześniejszych rozdziałach tej pracy. Jednak w tym miejscu zamieszczono zbiorcze działania jakie należy podejmować, aby przeciwdziałać zagrożeniom. Skorzystajmy zatem z wybranych i zaimplementowanych fragmentów szerszej publikacji internetowej dotyczącej cyberbezpieczeństwa[77].

Strategią zapewnienia bezpieczeństwa systemów teleinformatycznych jest budowanie ich w sposób, który ogranicza ewentualne problemy wynikające z naruszenia zabezpieczeń lub niepożądanej aktywności uprawnionego użytkownika. Takie podejście staje się szczególnie istotne w przypadku utrzymywania dużej infrastruktury o zastosowaniu komercyjnym, a także w firmach i organizacjach rządowych. Popularnym przykładem standardu jest dwuczęściowa brytyjska norma BS 7799, *Information technology – Code of practice for information security management oraz Information Security Management Systems – Specification with guidance for use.* Norma ta została później zaadaptowana jako ISO/IEC 17799:2003 oraz ISO/IEC 27001:2005. Polskimi odpowiednikami są PN-ISO/IEC 17799:2007 oraz PN-ISO/IEC 27001:2007.

W celu ograniczenia interakcji *malware* instalowany i eksploatowany jest system zwany *zaporą sieciową*. Oprogramowanie to stanowi narzędzie w zarządzaniu bezpieczeństwem, a jego rola ogranicza się do niezbędnego minimum zakresu możliwej interakcji między użytkownikami i systemami, oraz pomiędzy poszczególnymi komponentami platformy. Wyróżnia się cztery podstawowe metody ograniczenia zakresu interakcji:

1. Dobrane do zastosowania minimalistyczne projektowanie protokołów, unikanie łączenia diametralnie różnych funkcjonalności w ramach jednego rozwiązania.

[77] https://networkexpert.pl/cyberbezpieczenstwo/.

2. Separacja komponentów logicznych platformy tak, by zdobycie uprawnień administratora na jednym komputerze nie oznaczało całkowitej utraty kontroli nad systemami.

3. Wyłączanie zbędnych usług sieciowych na platformach.

4. Stosowanie zapór sieciowych do segmentacji sieci.

W analizie potencjalnych zagrożeń cyberprzestępczością istotne jest ograniczenie uprawnień nadawanych użytkownikom i systemom do najniższego, uzasadnionego realizowanymi celami poziomu, oraz taki podział kompetencji, by sfinalizowanie istotnych procesów biznesowych wymagało współpracy kilku osób. Cel ten można osiągnąć między innymi za pomocą mechanizmów ACL. Istotny jest też odpowiedni poziom rozliczalności i logowania działań użytkowników, a także monitorowanie tworzonych rejestrów pracy i wykrywanie innych nieprawidłowości np. poprzez zastosowanie programu antywirusowego, który powinien być ważnym elementem nadzorowania bezpieczeństwa. Pozwala on na reagowanie na problemy, zanim włamywacz zdecyduje się na ujawnienie swojej obecności. Jak już nadmieniono, czuwanie nad bezpieczeństwem zasobów informatycznych wzmaga okresowy *audyt wewnętrzny.*

Tak więc ponieważ wielu użytkowników obawia się o bezpieczeństwo swoich danych i prywatność podczas korzystania z Internetu, bezpieczeństwo stało się argumentem marketingowym, często przywoływanym przez producentów oprogramowania komercyjnego, a także przedmiotem wielu analiz porównawczych. Takie postępowanie rodzi jednak wiele kontrowersji, a dotychczasowe obietnice producentów nie przekładają się na zauważalną redukcję liczby obserwowanych włamań, mimo że około 90% użytkowników komputerów używa oprogramowania mającego chronić przed atakami. Dostawcy oprogramowania stosują niekiedy różne praktyki, a mianowicie:

Niezrozumiała terminologia. Nawet w przypadku, gdy opracowana przez specjalistów terminologia używana jest prawidłowo, często okazuje się ona zbyt skomplikowana. Stosowana jest tu ikona *zamkniętej kłódki,* zaprojektowana jako intuicyjny komunikat dla użytkownika i wyświetlana przez niemal wszystkie przeglądarki internetowe.

Zrzekanie się odpowiedzialności. Kolejną praktyką budzącą znaczne kontrowersje jest zrzekanie się przez niemal wszystkich producentów oprogramowania jakiejkolwiek odpowiedzialności za straty spowodowane przez błędy zabezpieczeń, wliczając w to przypadki celowych zaniedbań ze strony autora.

Tryb informowania o błędach. Wielu badaczy uważa, że użytkownicy mają prawo wiedzieć o problemach (błędach w pracy systemów) tak szybko, jak to możliwe, i że tylko taki sposób postępowania wymusza odpowiednią reakcję na producentach.

7.2. Zagadnienia bezpieczeństwa teleinformatycznego

Specjaliści zajmujący się bezpieczeństwem zasobów informatycznych muszą posiadać coraz szerszy zakres wiedzy, stąd też wachlarz przedmiotów wykładanych na szkoleniach specjalistycznych w ramach Programu Akademii Bezpieczeństwa Informatycznego (EITCA/IS) obejmuje zagadnienia[78]:

- podstawy kryptografii,
- bezpieczeństwo informatyczne *e-Gospodarki*,
- administracja i zarządzanie bezpieczeństwem w systemach Microsoft,
- bezpieczeństwo systemów operacyjnych,
- bezpieczne sieci komputerowe,
- zaawansowane bezpieczeństwo sieci informatycznych,
- kryptografia kwantowa,
- formalne aspekty bezpieczeństwa informacji,
- teoria bezpieczeństwa informatycznego,
- informatyka kwantowa w kontekście bezpieczeństwa,
- złożoność obliczeniowa jako podstawa bezpieczeństwa informacji.

7.3. Tworzenie programu cyberbezpieczeństwa

W 2021 roku 95,3% przedsiębiorstw wykorzystywało przynajmniej jeden ze środków bezpieczeństwa ICT, czyli bezpieczeństwa teleinformatycznego – wskazywał Główny Urząd Statystyczny w raporcie "*Społeczeństwo informacyjne w Polsce w 2021 r.*" W tym czasie wiele firm korzystało z usług IT świadczonych przez specjalistów z firm outsourcingowych[79]. Tworząc program bezpieczeństwa oraz diagnozując potencjalne zagrożenia należy dobrać do

[78] https://eitca.pl/is/GISEC?gclid=CjwKCAiAuaKfBhBtEiwAht6H7-rpnAnzzJjiE55yVjnnRzx7BasqAYyAeYC-WFLFfJKe-CXcKJGNFBoCzZsQAvD_BwE.
[79] https://ccit.pl/bezpieczenstwo-informacji/.

nich odpowiednie rozwiązania zapewniające ochronę[80]. Wymienia się wśród nich różnego rodzaju programy antywirusowe, *anti-malware*, *filtry DNS*, czy nowoczesne *firewalle*. Tego typu rozwiązania pozwalają ochronić przed atakiem nie tylko fizyczne urządzenia, ale także sieci, czy dane przechowywane w chmurze. Twórcy tych zabezpieczeń nieustannie pracują nad opracowaniem nowoczesnych systemów bezpieczeństwa, których wdrożenie zapewni ochronę przed coraz nowszymi formami ataków. Chcąc wdrożyć je w swojej firmie warto skorzystać z oferty, która znajduje się na *Mindworkers.pl*.

Warto zdawać sobie sprawę z faktu, że nawet najwyższy poziom wdrożonych zabezpieczeń nie zapewni 100% ochrony, w sytuacji, gdy możliwość przeprowadzenia skutecznego cyberataku udostępni pracownik. Oczywiście w sposób nieświadomy, ponieważ z reguły następuje to poprzez otwarcie zainfekowanego maila, czy korzystanie z sieci publicznej na służbowym sprzęcie, co może mieć miejsce podczas pracy zdalnej lub delegacji. W związku z tym należy nieustannie uświadamiać pracowników o istniejących zagrożeniach, a tego typu szkolenia powinny odbywać się regularnie. Wynika to z faktu, że najlepszą ochroną są działania prewencyjne. Podsumowując należy stwierdzić, że odpowiednia dbałość o bezpieczeństwo teleinformatyczne firmy to konieczność, która umożliwia jej bezproblemowe działania.

7.4. Ślady literaturowe dotyczące ochrony przed cyberatakami

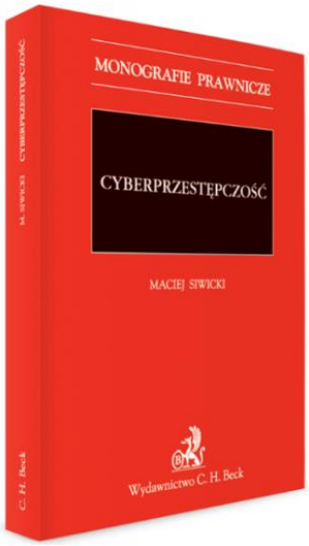
Cyberterroryzm oraz pokrewne mu formy wykorzystania technologii informatycznych przez podmioty pozapaństwowe stanowią działalności hakerów czy haktywizm[81]. Intensywne wykorzystywanie technik informatycznych w komunikacji międzyludzkiej to problem wyzwań towarzyszących szyfrowaniu i kodowaniu danych. Istotne jest zatem przybliżenie zarówno metody, jak i narzędzia kodowania danych Ponadto warto poznać sposoby oraz środki przełamywania tego rodzaju zabezpieczeń. Cenna jest także znajomość podmiotów zainteresowanych szyfrowaniem i odszyfrowywaniem informacji przechowywanych lub przesyłanych z wykorzystaniem technologii informatycznych oraz ocena poziomu współcześnie stosowanych przez państwa zabezpieczeń danych w formie elektronicznej. W wymienionej publikacji podjęto temat wykorzystania technologii informatycznych przez struktury administracji rządowej oraz tempo rozwoju i charakteru współpracy w tej sferze w

[80] https://twojepc.pl/news42344/Jak-zadbac-o-bezpieczenstwo-teleinformatyczne-w-firmie.html.
[81] https://www.pism.pl/publikacje/bezpieczenstwo-teleinformatyczne-panstwa.

ramach Unii Europejskiej[82]. Omówiono też proces budowy w Polsce tzw. *e-governmentu*, a więc wdrażania rozwiązań opartych na technologiach informatycznych do praktyki działania polskiej administracji publicznej, patrząc na to zagadnienie przez pryzmat inicjatyw proponowanych i zalecanych przez UE.

Zaprezentowano organy i instytucje odpowiedzialne w Unii Europejskiej za tego rodzaju zadania oraz omówiono dokonania w tym względzie w postaci rozmaitych ukończonych lub wciąż prowadzonych projektów. Wskazano na najpoważniejsze słabości, niedociągnięcia i braki tego aspektu unijnej współpracy. W cytowanej w wymienionym źródle internetowym monografii podjęto się analizy prawno-międzynarodowej dokumentu dotyczącego kwestii bezpieczeństwa teleinformatycznego, czyli *Konwencji o cyberprzestępczości* opracowanej pod auspicjami Rady Europy.

Sięgnijmy teraz po kolejną publikację „*Cyberprzestepczość*” [83] [84]. Wprowadza ona nas w problematykę najnowszych trendów dotyczących zagrożeń płynących z sieci i systemów komputerowych. Stanowi jednak rodzaj wiedzy specjalistycznej, niedostępnej i często niezrozumiałej terminologii dla dużej części społeczeństwa.



Źródło: https://www.ksiegarnia.beck.pl/10271-cyberprzestepczosc-maciej-siwicki.

Rys. 7.1. Widok publikacji „*Cyberprzestępczość*”

Niska jest jeszcze świadomość wśród podmiotów stosujących prawo oraz użytkowników szeroko pojętej tzw. *Sieci* na temat natury cyberprzestępczości. Powoduje to nie zgłaszanie przez pokrzywdzonych zaistniałych incydentów, a w rezultacie nie

[82] Ibidem.
[83] https://www.ksiegarnia.beck.pl/10271-cyberprzestepczosc-maciej-siwicki.
[84] Sawicki M., *Cyberprzestępczość*, Wydawnictwo C.H. Beck, *Monografie prawnicze*.

angażowanie Policji w ściganie oraz wykrywanie sprawców cyberataków na zasoby informatyczne. W rezultacie przestępczość zorganizowana skupiona wokół tzw. „*podziemia komputerowego*" przynosi znaczne zyski przy niewielkim ryzyku pociągnięcia do odpowiedzialności karnej. Przeciwdziałanie tej przestępczości wymaga jednak nie tylko zwiększenia świadomości użytkowników oraz organów ścigania i karania o zagrożeniach i kosztach powodowanych cyberprzestępczością, ale również ciągłego dostosowywania prawa do dynamicznie zmieniającej się w tym zakresie rzeczywistości. Cytowane opracowanie obejmuje cztery grupy merytorycznie powiązanych ze sobą zagadnień:

1. Charakterystyka zjawiska cyberprzestępczości uwzględniającą statystyczno-empiryczne aspekty tego zjawiska.

2. Przedstawienie międzynarodowych standardów kryminalizacji wybranych cyberprzestępstw.

3. Analiza przepisów prawnych odnoszących się do tych nadużyć przyjętych na gruncie polskiego ustawodawstwa.

4. Problematyka zapobiegania cyberprzestępczości z wykorzystaniem środków pozaprawnych.

Ocena zakresu i sposobu kryminalizacji cyberprzestępstw dokonana została m.in. z uwzględnieniem wypracowanych na gruncie prawa karnego wybranych państw instrumentów prawnych, na tle prawa unijnego oraz wybranych dokumentów międzynarodowych, w tym w szczególności:

Konwencji Rady Europy o cyberprzestępczości,

Prawa Modelowego Wspólnot Narodów dotyczącego przestępstw komputerowych i przestępstw związanych z komputerami (*Commonwealth Model Law on Computer and Computer Related Crime*).

Przygotowanego pod auspicjami ONZ przez Międzynarodowy Związek Telekomunikacyjny opracowania pt. „*ITU Cybercrime Legislation Toolkit*".

Zachęceni zawartością merytoryczną wcześniej wymienionych publikacji skorzystajmy jeszcze z pracy „*Cyberprzestępczość Jak walczyć z łamaniem prawa w Sieci*"[85] (zob. rysunek 7.2). W wymienionej książce zaprezentowano następujące zagadnienia:

- historię cyberprzestępczości,
- aspekty psychologiczne walki z cyberprzestępczością,
- podstawy działania komputerów i sieci komputerowych,

[85] https://helion.pl/ksiazki/cyberprzestepczosc-jak-walczyc-z-lamaniem-prawa-w-sieci-debra-littlejohn-shinder-ed-tittel-technica,cyber.htm#format/d.

- techniki włamań do sieci i ataków na serwery sieciowe,
- sposoby zapobiegania cyberprzestępstwom,
- metody zabezpieczania danych,
- techniki wykrywania cyberprzestępstw i zabezpieczania ich dowodów,
- podstawy prawne oskarżenia o cyberprzestępstwo.

Źródło: https://www.ksiegarnia.beck.pl/10271-cyberprzestepczosc-maciej-siwicki.

Rys. 7.2. Strona tytułowa książki „*Cyberprzestępczość Jak walczyć z łamaniem prawa w Sieci*"

Wertując dalej strony internetowe spotykamy informację o publikacji „*Zagrożenie cyberprzestrzeni i świata wirtualnego*", którą poleca się zaangażowanemu w problematykę ochrony przed cyberprzestępczością[86].

7.5. Przykłady środków i programów zabezpieczenia przed włamaniami cyberprzestępców

Instytucje finansowe, handlowe i nie tylko one stosują różnego rodzaju rozwiązania zabezpieczające przed dostępem do konta. Przykładem są karty płatnicze z *chipem*[87]. Najpopularniejszą formą przechowywania informacji na karcie płatniczej są paski magnetyczne i kody kreskowe. *Karty chipowe* powstały dzięki organizacji EMV zrzeszającej m.in. *Europay*, *MasterCard* i *Visa*. Były one odpowiedzią na niewystarczającą ochronę kart

[86] https://bonito.pl/produkt/zagrozenia-cyberprzestrzeni-i-swiata-wirtualnego-2?gclid=CjwKCAiAuaKfBhBtEiwAht6H76UnpO1SUfpPhmFJLaQcN19aSbvxrSdkNAW3kJ29mzfW1aW-Qc7cbRoCVckQAvD_BwE.
[87] https://www.cartpoland.pl/czego-wykonany-chip-karcie-chipowej/.

magnetycznych. Chip stał się narzędziem walki ze *skimmingiem*, czyli kopiowaniem zawartości paska magnetycznego i wykorzystywania go do zakupów na koszt ofiary.

Chip jest to mikroprocesor, który kontroluje dostęp do zapisanych danych. Umożliwia ochronę procesu logowania i zapewnienie niezaprzeczalności poprzez podpis cyfrowy. Dzięki niemu przechowywane informacje są dodatkowo szyfrowane, co utrudnia ich odczytanie przez osoby niepowołane. Choć *karty chipowe* wypierają karty magnetyczne, okres przejściowy sprawia, że oba te zabezpieczenia są spotykane razem, co umożliwia przeprowadzanie transakcji w starszych systemach.

Przesyłanie informacji do komputera następuje wtedy, gdy odpowiednie styki w czytniku połączą się z jego powierzchnią. Mikroprocesor, kontroluje zapis i odczyt informacji wtedy, gdy w pamięci zapisywane są dane. *Chip* wyposażony jest też w pamięć ROM (*read-only memory*), która dzieli się na trzy obszary. Pierwszy z nich to odczyt swobodny, w którym zawarte jest imię i nazwisko posiadacza karty, jej numer oraz data ważności. Drugi to obszar poufny, który zawiera poufne informacje o użytkowniku i dane producenta karty. Natomiast w trzecim obszarze zwanym roboczym przechowywane są informacje, które stale i dynamicznie się zmieniają. Są to np. saldo rachunku czy lista operacji i transakcji.

Obecnie oprócz gotówki, kart płatniczych w użyciu zaczynają być tzw. *waluty cyfrowe*[88]. Podobnie jak Internet opanował świat, tak i nieuchronnie *waluta cyfrowa* (CBDC) zastąpi tradycyjne banknoty i monety, które posiadamy w portfelach. Być może niektórym zdaje się, że jest to zbyteczna komplikacja sposobów płatności. W rzeczywistości wirtualna waluta przyszłości będzie dużym ułatwieniem dla płacących. Niektóre kraje na świecie już przeprowadzały testy w tym kierunku. W strefie euro gotowy jest projekt Europejskiego Banku Centralnego dotyczący waluty przyszłości, czyli CBDC. Niektóre kraje, np. Szwecja, Chiny czy Jamajka, przeprowadziły już testy obrotu CBDC. Polska też powinna podjąć się wdrażania "*e-złotówki*". W naszych portfelach wciąż znajdują się banknoty i monety, lecz nieuchronnie zbliża się moment, w którym wprowadzona zostanie waluta przyszłości, czyli wspomniane już CBDC (*central bank digital currency*). CBDC to prawny środek płatniczy, tzw. programowalny pieniądz, który jest emitowany przez władzę monetarną, czyli bank centralny. W dużym uproszczeniu to i banknoty, i monety, którymi się teraz posługujemy, tyle że w formie zdigitalizowanej.

Po tych wiadomościach ze świata wirtualnego przyszłości skupmy swoją uwagę na przykładach wykrywających podatności aplikacji na zagrożenia zewnętrzne cyberprzestrzeni.

[88] https://businessinsider.com.pl/technologie/waluta-przyszlosci-w-naszych-portfelach-co-to-jest-cyfrowa-waluta/g6jz7kj.

Nessus Professional to pojedynczy skaner, który wykrywa podatności przy pomocy dwóch metod skanowania[89]:

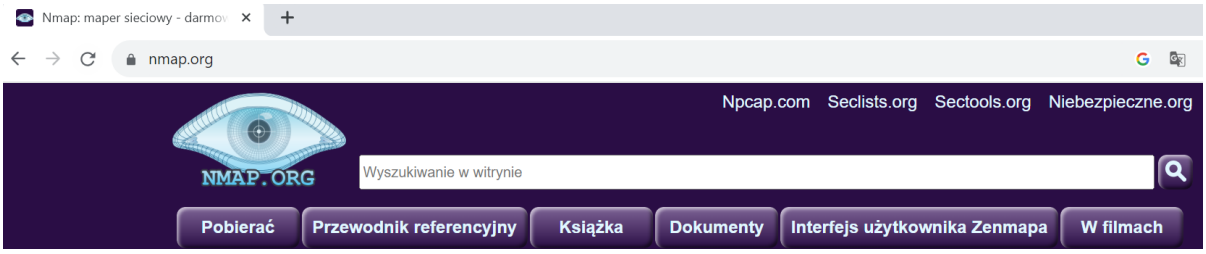
1. *Sieciowe* (wykrywa porty, sprawdza jakie serwisy działają, możliwość zalogowania się do systemu przy pomocy domyślnych haseł).

2. *Z uwierzytelnianiem* (dostarcza bardziej dokładnych informacji np. wersja systemu, uruchomione usługi, informacja czy hosty nie komunikują się bazą botnetową, zmiany w rejestrach, czy systemy są zgodne z regulacjami np. PCI DSS, zgodność z polityka bezpieczeństwa).

Wymieniony wcześniej skaner programistyczny daje następujące możliwości:

- zapobiega atakom identyfikując podatności, które powinny zostać zlikwidowane;
- odpowiada standardom regulatorów i wymogom zgodności w najszerszym zakresie;
- umożliwia dostęp przez przeglądarkę o dowolnej porze i w dowolnym miejscu;
- posiada możliwość dostosowania raportów wg podatności lub urządzenia a także możliwość wygenerowania streszczenia dla kierownictwa lub porównania wyników różnych skanów w celu uwidocznienia zmian.

Kolejne oprogramowanie to *Nmap* (*Network Mapper*), którego ofertę pokazano na rysunku 7.3[90]. *Nmap* jest darmowym i otwartym oprogramowaniem, które stanowi narzędzie do wykrywania sieci i audytu bezpieczeństwa. Wielu administratorów systemów i sieci uważa go również za przydatny do zadań takich jak inwentaryzacja sieci, zarządzanie harmonogramami aktualizacji usług i monitorowanie czasu pracy hosta lub usługi.



Źródło: http://nmap.org.

Rys. 7.3. Strona WWW programu *Nmap*

Nmap wykorzystuje nieprzetworzone pakiety IP w nowatorski sposób, aby określić, jakie hosty są dostępne w sieci, jakie usługi oferują te hosty, jakie systemy operacyjne działają, jakiego typu filtry pakietów/zapory ogniowe są w użyciu i dziesiątki innych cech. Został zaprojektowany do szybkiego skanowania dużych sieci, ale działa równie dobrze dla

[89] https://www.passus.com/produkty/tenable/nessus.
[90] https://nmap.org/.

pojedynczego hosta. Omawiany program działa na wszystkich głównych komputerowych systemach operacyjnych, a mianowicie *Linux, Windows* i *Mac OS X*. Oprócz klasycznego pliku wykonywalnego w postaci binarnej programu *Nmap* z wiersza poleceń *Zenmap* możemy wywołać:

Ncat (elastyczne narzędzie do przesyłania, przekierowywania i debugowania danych),

Ndiff (narzędzie do porównywania wyników skanowania),

Nping (narzędzie do generowania pakietów i analizy odpowiedzi).

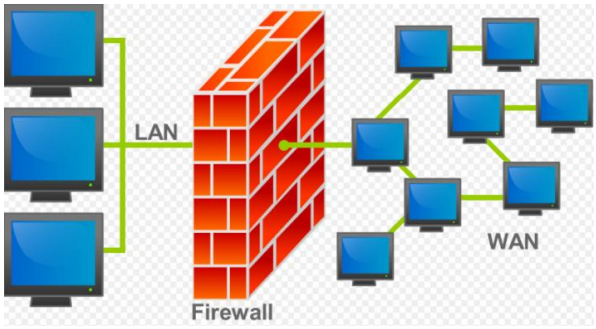
Przy przesyłaniu niektórych danych stosowane są pliki w postaci zakodowanej np. w formacie ZIP jako wstępna metoda „*utajnienia*" danych[91]. ZIP jest popularnym formatem do bezstratnej kompresji i archiwizacji danych. Programy do tworzenia archiwów ZIP oferują możliwość szyfrowania danych, co jest często wykorzystywaną funkcjonalnością przy przesyłaniu plików zawierających dane osobowe pocztą *e-mail*.

Innym sposobem kontroli dostępu do serwera jest tzw. *Dial-up* (połączenie wdzwaniane, połączenie komutowane)[92]. Jest to sposób połączenia komputera z siecią komputerową polegający na wykorzystaniu modemu telefonicznego do połączenia się z serwerem dostępowym sieci. W celu uzyskania połączenia wykorzystywana jest zwykła stacjonarna linia telefoniczna (analogowa lub cyfrowa) w postaci metalowej pętli abonenckiej lub rzadziej, jako radiowe łącze abonenckie albo bezprzewodowe łącze telefonii komórkowej w publicznej sieci telekomunikacyjnej. Serwer dostępowy przekazuje ruch pochodzący z tak połączonego komputera do sieci komputerowej, np. sieci Internet. Tak więc połączenia wdzwaniane to usługi umożliwiające dzwonienie do innych użytkowników sieci telefonicznych z wykorzystaniem pośredniczącego numeru telefonu. Numer pośredniczący może być numerem stacjonarnym lub numerem infolinii (typu 800, 801).

Do identyfikacji elementu w sieci służy także adres IP (*IP address*). Stanowi on liczbowy identyfikator nadawany interfejsowi sieciowemu, grupie interfejsów (*broadcast, multicast*), bądź całej sieci komputerowej w protokole IP, służący identyfikacji elementów sieci w warstwie trzeciej modelu OSI – w obrębie sieci lokalnej oraz poza nią (tzw. adres publiczny)[93]. Rozwińmy jeszcze wspomniane już zabezpieczenie jakim jest zapora sieciowa (f*irewall*)[94], czyli ściana ogniowa (zob. rysunek 7.4). Jest to jeden ze sposobów

[91] Szczegielniak-Rekiel A., Kelner J.M., *Przegląd metod szyfrowania i dekryptażu archiwum ZIP*, czasopismo: Elektronika: konstrukcje, technologie, zastosowania, Warszawa 2022, Wojskowa Akademia Techniczna, Wydział Elektroniki, CEON Biblioteka Nauki, https://yadda.icm.edu.pl/yadda/element/bwmeta1.element.baztech-2555200d-f18b-4187-a5c9-9f71af3b98ff.
[92] https://interneta.pl/dial-up-polaczenie-wdzwaniane/.
[93] https://pl.wikipedia.org/wiki/Adres_IP.
[94] https://pl.wikipedia.org/wiki/Zapora_sieciowa.

zabezpieczania sieci i systemów przed atakami nieupoważnionych osób spoza sieci obiektu. Termin ten może odnosić się zarówno do sprzętu komputerowego wraz ze specjalnym oprogramowaniem, jak i do samego oprogramowania blokującego niepowołany dostęp do komputera, który podlega jego ochronie. Pełni rolę połączenia ochrony sprzętowej i programowej sieci wewnętrznej LAN przed dostępem z zewnątrz, tzn. z sieci publicznych, Internetu. Chroni też przed nieuprawnionym wypływem danych z sieci lokalnej na zewnątrz, a często jest to komputer wyposażony w system operacyjny z odpowiednim oprogramowaniem. Do jego podstawowych zadań należy filtrowanie połączeń wchodzących i wychodzących oraz tym samym odmawianie żądań dostępu uznanych za niebezpieczne.



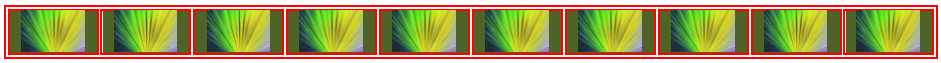
Źródło: https://pl.wikipedia.org/wiki/Zapora_sieciowa#/media/Plik:Firewall.png.

Rys. 7.4. Idea zapory sieciowej między LAN i WAN

Zapoznajmy się jeszcze z funkcjonalnością innego typu zapory sieciowej UTM (*Unified Threat Management*)[95]. Zapora ta ma wiele funkcji ochrony brzegu sieci zgromadzonych w jednym sprzętowym urządzeniu. UTM pozwala zabezpieczyć sieć na wielu płaszczyznach. Funkcjonalność omawianej zapory nie kończy się jednak na udostępnieniu wielu narzędzi *cybersecurity* w ramach jednego rozwiązania. To także automatyzacja zarządzania wieloma procesami związanymi z utrzymaniem centrum zarządzania bezpieczeństwem danych. Z wielu powodów urządzenia UTM są podstawową składową systemu zarządzania bezpieczeństwem w średnich i mniejszych przedsiębiorstwach. Przede wszystkim mniejsze działy IT, dysponujące ograniczonym budżetem mogą dzięki wdrożeniu UTM zagwarantować ochronę najcenniejszych zasobów przedsiębiorstw, bez względu na wielkość. Zautomatyzowanie wielu czynności pozwala uniknąć zatrudnienia dodatkowych specjalistów. Tak wiec w przeciwieństwie do dużych korporacji mniejsze firmy stawiają na sprzętowy UTM z intuicyjną obsługą i szerokim wachlarzem zabezpieczeń.

[95] https://www.netcomplex.pl/czym-jest-utm-zabezpiecz-siec-dzieki-zintegrowanemu-zarzadzaniu-bezpieczenstwem.

8. Studium przykładów wystąpień hakerskich



8.1. Prace nad *Programowalnym Układem Scalonym*

Według badań magazynu InformationWeek oraz firmy konsultingowej Accenture, w 2006 blisko 57% firm doświadczyło problemów z wirusami komputerowymi, 34% z robakami, 18% padło ofiarą ataków DoS, 9% doświadczyło włamań sieciowych, a 8% padło ofiarą kradzieży tożsamości[96]. Ataków doświadczają także użytkownicy indywidualni, których komputery są dość często wykorzystywane jako *zombie* do ataków DDoS oraz wysyłania *spamu*. Celem ataków stają się także coraz bardziej zaawansowane technologicznie telefony komórkowe, konsole gier wideo, systemy obsługujące infrastrukturę telekomunikacyjną i inne platformy.

Firma Network Expert postawiło za swój cel wykonanie systemu Polskiego Elektronicznego Dokumentu Tożsamości (PEDT). Dla jego osiągniecia projektowany jest *Programowalny Układ Scalony* (PUS), który po zainstalowaniu w karcie plastikowej będzie nośnikiem informacji PEDT, a także będzie mógł wykonywać podpis cyfrowy. PUS będzie układem scalonym typu SoC (*System on Chip*), czyli pełnym systemem teleinformatycznym zawierającym procesory, pamięci i układy wejścia/wyjścia oraz rozbudowaną funkcjonalność bezpieczeństwa.

Oprócz układu scalonego w ramach projektu powstaną rozwiązania umożliwiające bezpieczną produkcję PUS. Układ scalony PUS oraz jego warianty mogą zostać zastosowane także w innych rozwiązaniach, w których bezpieczeństwo teleinformatyczne gra główną rolę. Przykładem mogą być urządzenia kryptograficzne, w tym mobilne.

[96] https://networkexpert.pl/cyberbezpieczenstwo/.

8.2. Przykłady wykorzystania złośliwego oprogramowania do spowodowania zakłóceń w ruchu kolejowym

O niektórych wystąpieniach hakerów wspomniałem już we wcześniejszych rozdziałach tej publikacji. Tutaj przytoczone zostaną przykłady wpływu złośliwego oprogramowania na działanie sieci teleinformatycznej i systemów informatycznych. Skorzystano też z wartościowych wiadomości udostępnionych w Internecie, a zwłaszcza pod linkiem: *https://networkexpert.pl/cyberbezpieczenstwo/*.

Przypusza się, że nastąpił atak hakerski na polskie koleje bowiem pasażerowie doznali dolegliwości związane z nieautoryzowanym wykorzystaniem systemu biorącego udział w zarządzaniu ruchem kolejowym[97]. PKP Polskie Linie Kolejowe poinformowały, że w pewnym okresie w województwie zachodniopomorskim doszło do nieuprawnionego nadawanie sygnału „*Radio-stop*", co spowodowało duże utrudnienia w ruchu kolejowym. W tym czasie zakładano, że ktoś wykorzystał kolejowe częstotliwości i nadawał sygnał uruchamiający alarmowe zatrzymanie pociągów. Zdarzenie to stało się polem działania różnych służb i zainteresował się nim także Urząd Komunikacji Elektronicznej.

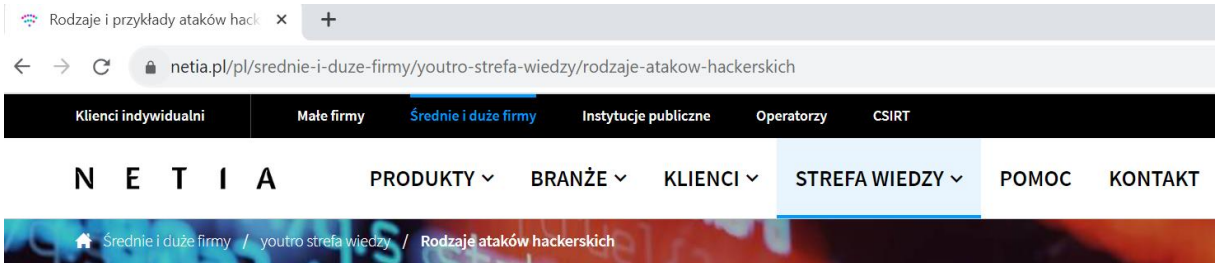
O tej informacji dowiadujemy się też z innej wiadomości podanej w Internecie[98]. W ciągu doby dwukrotnie doszło do bezprawnego użycia sygnału radiowego "*Radio-stop*", który powoduje automatyczne uruchomienie hamulca bezpieczeństwa w pociągu. Sygnał odebrał maszynista pociągu towarowego na trasie Świdwin-Worowo i dyżurny ruchu na stacji kolejowej Rumowo Pomorskie w województwie zachodniopomorskim.

To było drugie tego typu zdarzenie w tym województwie w ciągu doby. Pierwsze bezprawne nadanie sygnału "*Radio-stop*" nastąpiło w nocy z piątku na sobotę. Wtedy doszło do nieuprawnionego nadania sygnału na linii 273 (odcinek Daleszewo - Szczecin Główny) oraz na linii 351 (odcinek Choszczno - Szczecin Główny). Sygnał był odbierany przez posterunki ruchu i maszynistów pociągów znajdujących się w tym obszarze. Składy zostały automatycznie zatrzymane.

[97] https://www.onet.pl/informacje/onetwiadomosci/atak-hakerski-na-polskie-ko leje-przedstawiciel-rzadu-zabiera-glos/8t2e0hv,79cfc278.
[98] https://wiadomosci.onet.pl/szczecin/bezprawnie-nadano-sygnal-do-zatrzymania-pociagow-sprawe-zajmuje-sie-abw/8pd9sqn?utm_medium=push&utm_source=browser&utm_campaign=push_push_go&utm_site=wiadomosci&utm_push_id=64eae3ac2e9ca22f10ac0077.

8.3. Rodzaje ataków hakerskich

Pobieżnie o rodzajach ataków hakerskich wspomniano już we wcześniejszym materiale tej publikacji. Jednak w tym rozdziale skorzystano z opracowania podanego pod linkiem podanym w przypisie[99]: Spotykamy go na stronie WWW firmy Netia (zob. rysunek 8.1).



Źródło: https://www.netia.pl/pl/srednie-i-duze-firmy/youtro-strefa-wiedzy/rodzaje-atakow-hackerskich.

Rys. 8.1. Fragment strony internetowej firmy NETIA

Jest to wyróżnienie ataków hakerskich podane w publikacji T. Łyżaka *„Rodzaje ataków hakerskich*"[100]. Rosnący udział opartych na Internecie rozwiązań dla biznesu staje się atrakcyjnym celem dla grup przestępczych działających w sieci. Wykorzystują one słabości zabezpieczeń i błędy popełniane przez użytkowników rozwiązań *online*. Europol wskazuje, że cyberprzestępczość już niemal dekadę temu była bardziej dochodowa od łącznej wartości globalnej sprzedaży marihuany, kokainy i heroiny[101]. Przedstawmy teraz najpopularniejsze rodzaje ataków hakerskich.

DDoS (Distributed Denial of Service) polegają na bombardowaniu serwerów określonej firmy falą połączeń z innych urządzeń. Serwer otrzymuje nawet setki tysięcy zapytań na sekundę, co może bardzo spowolnić jego pracę lub doprowadzić do zupełnego jej przerwania.

Phishing – najczęściej stosowana przez przestępców metoda wyłudzania danych czy pokonywania zabezpieczeń firmowych. Ofiara otrzymuje wiadomość, która nakłania go bądź do pobrania pliku, bądź do wejścia na dany adres. Taka wiadomość może być adresowana do pracownika odpowiadającego za bezpieczeństwo sieciowe, a takie oddziaływanie to tzw. *spear phishing*). Wyróżnia się dwa najczęściej spotykane motywy wysyłania wiadomości *phishingowych*:

[99] https://www.google.com/search?q=Przyk%C5%82ady+atak%C3%B3w+hakerskich+na+sieci+komputerowe
[100] Łużak T., *Product Manager, Cybersecurity* - Netia S.A., *Rodzaje ataków hakerskich*, https://www.netia.pl/pl/srednie-i-duze-firmy/youtro-strefa-wiedzy/rodzaje-atakow-hackerskich.
[101] https://www.europol.europa.eu/publications-events/main-reports/eu-serious-and-organised-crime-threat-assessment-socta-2013.

1. Umieszczanie na firmowych komputerach *malware*, czyli złośliwego oprogramowania za pośrednictwem zainfekowanego załącznika.

2. Wyłudzanie loginów i haseł przez przekierowanie użytkownika na stronę łudząco podobną do strony logowania do aplikacji firmowej czy banku.

Ataki siłowe służące do przełamywania haseł. Komputery hakerów podejmują tysiące prób logowania do systemu, wykorzystując listę zawierającą tysiące czy dziesiątki tysięcy popularnych haseł.

Ataki na webaplikacje, a ich celem są sklepy internetowe, chociaż mogą być one skierowane w dowolną aplikację internetową. Ataki te obejmują rozmaite techniki takie, jak wstrzykiwanie SQL i zainfekowanych skryptów. Dzięki temu hakerzy mogą przejąć kontrolę nad aplikacją bądź sesją użytkownika. Niektórym z tych ataków można zapobiec, monitorując luki w zabezpieczeniach oraz korzystając z zapór sieciowych aplikacji internetowych czy z bezpiecznego programowania.

Ataki insiderskie. Zagrożenia „*insiderskie*" mogą wynikać zarówno z ujawnienia przez nieostrożnych pracowników danej firmy swoich loginów, hasła lub poufnych danych nieupoważnionym osobom. Pracownicy mają zazwyczaj o wiele szerszy dostęp do firmowych danych, dobrze wiedzą też, gdzie szukać najcenniejszych informacji. Szczególnie jest to istotne w odniesieniu do infrastruktury informatycznej.

8.4. Skutki dużych włamań do systemów

Firma analityczna CyberSecurity Ventures szacuje, że gdyby potraktować straty wyrządzone przez cyberprzestępców w 2021 r., jako PKB państwa byłoby ono trzecią największą gospodarką świata po USA i Chinach. Korzystając z publikacji internetowych spotykamy jeszcze doniesienia o innych zaistniałych atakach hakerskich w minionych latach.

Colonial Pipeline. Atak z 2021 roku, który wstrząsnął amerykańskim rynkiem paliw. W maju hakerzy (*hackerzy*) powiązani z gangiem *ransomware* o nzawie DarkSide dostali się do sieci Colonial Pipeline, jednej z największych amerykańskich firm naftowo-gazowych. Skutkiem włamania było wstrzymanie działania największego rurociągu transportującego benzynę i paliwo lotnicze na wschodnim wybrzeżu USA.

WannaCry i NotPeya. Oba te ataki objęły komputery na niemal wszystkich kontynentach i kosztowały miliardy dolarów. Co gorsza, nastąpiły w odstępie zaledwie kilku tygodni. Najpierw 12 maja 2017 r. wirus *WannaCry* zainfekował ponad 200 tys. komputerów

w 150 krajach. Wystarczyło mu na to kilkanaście godzin. Robak szyfrował dane przejętych urządzeń i wyświetlał wiadomość z żądaniem okupu.

SolarWinds. Na początku 2020 r. grupa hakerów, zdołała pokonać zabezpieczenia firmy SolarWinds i spenetrować jej własną sieć. To firma tworząca oprogramowanie do zarządzania wewnętrznymi sieciami komputerowymi firm i organizacjami. Jej program Orion jest wykorzystywany przez 33 tys. organizacji na całym świecie. Napastnicy podmienili kod aplikacji *Orion* na zmodyfikowaną przez siebie wersję. Automatyczne aktualizacje oprogramowania prowadziły do automatycznych infekcji.

BlackEnergy. Tym określeniem nazwano atak wymierzony w infrastrukturę krytyczną. Zawierające *malware* wiadomości *phishingowe* zostały wysłane do wysokich rangą pracowników ukraińskich firm energetycznych.

W 2016 roku Yahoo poinformowało o wykryciu wycieku danych użytkowników po atakach przeprowadzonych w 2013 i 2014 roku[102]. Na skutek działań hakerów do sieci trafiły informacje o ponad 1 miliarda osób, korzystających z usług platformy. W wyniku przeprowadzonego w 2011 roku ataku hakerskiego na sieć *PlayStation Network* cyberprzestępcy wykradli dane użytkowników około 77 milionów kont i spowodowali prawdziwy paraliż całej sieci. Co najgorsze, wśród przejętych informacji były numery kart kredytowych. Sony wyłączyło swoją usługę aż na 23 dni.

Stuxnet był robakiem komputerowym, infekującym komputery z systemami *Windows*. Jako pierwszy stosowany był do szpiegowania i przeprogramowywania instalacji przemysłowych. W 2016 roku hakerzy przeprowadzili zmasowany atak na serwery Übera, skąd wykradli dane użytkowników platformy oraz dane kierowców. W 2014 roku hakerzy dostali się do serwerów sieci *Marriott*, wykradając informacje o kartach kredytowych należących do siedmiu milionów brytyjskich klientów.

8.5. Ataki na systemy domowe

Ataki na inteligentne domy były możliwe za sprawą niedostatecznie zabezpieczonych urządzeń[103]. Przykładem jest zdalnie sterująca przez hakera kamera monitorująca śpiące dziecko, podczas gdy rodzice spali w pokoju sąsiednim. To wydarzenie było wyraźnym

[102] https://www.komputerswiat.pl/artykuly/redakcyjne/najwieksze-ataki-hakerskie-ostatnich-lat-o-tych-zdarzeniach-mowil-caly-swiat/khfnngd#slajd-1.
[103] https://www.google.com/search?q=inteligentny+haker

sygnałem, że do kamery, przeznaczonej jedynie do monitorowania poczynań dziecka ktoś zdalnie włamał się przez Internet i przejął nad nią kontrolę.

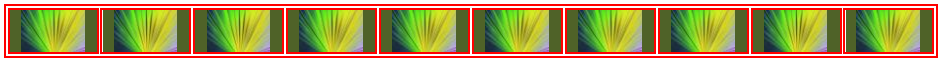
Trzeba nadmienić jeszcze, że rozległy cyberatak, który wykorzystał luki w inteligentnych rejestratorach i kamerach internetowych, wywołał chaos w znacznej części Internetu w Europie i Stanach Zjednoczonych. Wówczas setki tysięcy urządzeń zostało przejętych podczas ataku, który eksperci bezpieczeństwa zidentyfikowali jako rozproszony atak typu "*odmowa usługi*" (DDoS) przy użyciu *botnetu Mirai*. Hakerzy przejęli podłączone urządzenia, a następnie wykorzystali je do zablokowania serwerów firmy Dyn, która wcześniej kontrolowała znaczną część infrastruktury systemu nazw domen internetowych (DNS). Serwisy, w tym *Twitter, The Guardian, Netflix, Reddit,* CNN w Europie i USA, nie działały przez większość dnia.

Użytkownicy domowi na ogół ufają urządzeniom łączącym się z siecią teleinformatyczną. Konsumenci inwestując w nowoczesne przedmioty *Internetu Rzeczy* wychodzą z założenia, że będą one sprawnie działały, automatycznie się aktualizowały i szybko się nie zestarzeją[104]. Telemetria firmy Bitdefender pokazuje, że chociaż serwery NAS nie mieszczą się nawet w pierwszej dziesiątce najczęściej używanych urządzeń w inteligentnych domach, to jednak zajmują pierwsze miejsce pod względem liczby luk występujących w zabezpieczeniach. Aby przeciwdziałać uszkodzeniu cennych danych oprogramowaniem *ransomware* zalecane jest zastosowanie inteligentnego routera, który potrafi wykrywać naruszone urządzenia.

Innym sposobem jest stosowanie aplikacji typu „*programy deransomare*". Programy te to połączenie wiodących w branży technologii Commvault Backup and Recovery oraz niezawodnej skalowalnej, wydajnej pamięci masowej z Nutanix Object[105]. Pozwala to uzyskać niezawodną odporność przed zagrożeniami typu *ransomware*, czy także kierowanymi atakami grup przestępczych. Połączenie zalet zasobów obiektowych wraz z technologią Commvault przyczynia się do tego, że krytyczne dane nie zostaną usunięte, zmodyfikowane ani skopiowane przez złośliwe zagrożenia.

[104] https://techno-senior.com/2021/03/31/inteligentny-dom-celem-hakerow/.
[105] https://s4e.pl/nutanix/

9. Słownik pojęć podstawowych z zakresu *„Bezpieczeństwa telekomunikacyjnego i cyberbezpieczeństwa”*



Termin	Źródło	Opis
Access point	https://www.mediaexpert.pl/poradniki/komputery-i-tablety/access-point-co-to-jest	Punkt dostępowy do Wi-Fi. Sprzęt podłączamy bezpośrednio do naszej sieci przewodowej, np. routera lub switcha, a następnie umieszczamy go w lokalizacji, która ma problem ze stabilnością Wi-Fi. *Access point* emituje sygnał sieci bezprzewodowej i tym samym poprawia komfort korzystania z niej.
ACL (*Access-control list*)	https://pl.wikipedia.org/wiki/Access-control_list	Lista kontroli dostępu – uprawnień skojarzonych z obiektem komputerowego systemu plików. Określa, którzy użytkownicy lub procesy systemowe mają dostęp do obiektów, a także jakie operacje są dozwolone na danych obiektach.
Active Directory (AD)	https://pl.wikipedia.org/wiki/Active_Directory	Usługa katalogowa (*hierarchiczna baza danych*) dla systemów *Windows* – *Windows Server 2019, Windows Server 2016, Windows Server 2012, Windows Server 2008, Windows Server 2003* oraz *Windows 2000*, będąca implementacją protokołu LDAP.
Architektura *klient-serwer*	https://pl.wikipedia.org/wiki/Klient-serwer	Architektura systemu komputerowego, w szczególności oprogramowania, umożliwiająca podział zadań. Polega na ustaleniu, że *serwer* zapewnia usługi dla *klientów*, zgłaszających do serwera żądania obsługi.
Azure AD	https://azure.microsoft.com/pl-pl/products/active-directory	Część usługi *Microsoft Entra*, to korporacyjna usługa zarządzania tożsamościami, która zapewnia uwierzytelnianie wieloskładnikowe logowania jednokrotnego w celu ochrony przed atakami cyberbezpieczeństwa.
Big data	https://pl.wikipedia.org/wiki/Big_data	Termin odnoszący się do dużych, zmiennych i różnorodnych zbiorów danych, których przetwarzanie i

		analiza jest trudna, ale jednocześnie wartościowa, ponieważ może prowadzić do zdobycia nowej wiedzy.
Bioinformatyka	https://pl.wikipedia.org/wiki/Bioinformatyka	Interdyscyplinarna dziedzina łącząca nauki biologiczne i informatyczne. Obejmuje rozwój metod obliczeniowych służących do badania i symulacji struktury, funkcji i ewolucji genów, genomów i białek.
Business intelligence (BI)	https://pl.wikipedia.org/wiki/Business_Intelligence	*Analityka biznesowa* – proces przekształcania danych w informacje, a informacji w wiedzę, która może być wykorzystana do zwiększenia konkurencyjności przedsiębiorstwa.
CEH (*Certified Ethical Hacker*)	https://en.wikipedia.org/wiki/Certified_Ethical_Hacker	Kwalifikacja nadawana przez EC-Councili uzyskana poprzez wykazanie się wiedzą na temat oceny bezpieczeństwa systemów komputerowych poprzez poszukiwanie słabych punktów w systemach docelowych, przy użyciu tej samej wiedzy i narzędzi, co złośliwy haker, ale w sposób zgodny z prawem, w celu oceny stanu bezpieczeństwa systemu docelowego.
CISA (*Certified Information Systems Auditor*)	https://pl.wikipedia.org/wiki/CISA	Certyfikat zawodowy dla osób zajmujących się audytem systemów informatycznych wydawany przez ISACA.
Cisco ISE	https://www.grandmetric.com/pl/cisco-ise-czym-jest/	Rozwiązanie, które ma za zadanie kontrolować politykę bezpiecznego dostępu do sieci, a przez to krytycznych zasobów w organizacji. Jest pojedynczym punktem informacji o zdarzeniach związanych z dołączającymi się do sieci urządzeniami i użytkownikami.
Cisco Webex	https://en.wikipedia.org/wiki/Cisco_Webex	Amerykańska firma, która opracowuje i sprzedaje aplikacje do konferencji internetowych, wideokonferencji i *contact center* jako usługi. Jej oprogramowanie obejmuje *Webex App*, *Webex Suite*, *Webex Meetings*, *Webex Messaging*, *Webex Calling*, *Webex Contact Center* i *Webex Devices*.
CISSP	https://pl.wikipedia.org/wiki/Certified_Information_Systems_Security_Professional	Certyfikat, który jest niezależnym i obiektywnym świadectwem eksperckim w dziedzinie bezpieczeństwa teleinformatycznego. Zgodnie z danymi z lipca 2022 roku, w Polsce certyfikat CISSP posiada 780 osób.

ClickMeeting	https://pl.wikipedia.org/wiki/ClickMeeting	Platforma i aplikacja webowa do prowadzenia webinariów (prezentacji produktów, szkoleń, kursów online), spotkań biznesowych i wideokonferencji, działająca z wykorzystaniem przeglądarki internetowej.
CoBIT (*Control Objectives for Information and related Technologies*)	https://www.auditboard.com/blog/coso-vs-cobit/	Struktura informatyczna założona przez ISACA (Stowarzyszenie Systemów Informatycznych i Kontroli Audytu) w 1996 roku. Odegrała kluczową rolę w pomaganiu organizacjom w opracowywaniu kontroli wewnętrznych w celu zapobiegania oszustwom . W szczególności COBIT stał się standardem w opracowywaniu strategii zarządzania IT i ładu korporacyjnego w celu zapobiegania oszustwom.
Conficker	https://pl.wikipedia.org/wiki/Conficker	Jeden z groźniejszych znanych dotychczas robaków komputerowych. Pojawił się w sieci w październiku 2008 roku. Atakuje systemy operacyjne z rodziny *Microsoft Windows*. Robak wykorzystuje znane luki w zabezpieczeniach platformy systemowej *Windows Server* oraz różne usługi składowe wykorzystywane przez systemy *Windows 2000*, *Windows XP*, *Windows Vista*, *Windows Server 2003* i *Windows Server 2008*.
Contact center	https://pl.wikipedia.org/wiki/Call_center	Wzbogacenie o inne niż telefon sposoby kontaktu. Jeden z kluczowych elementów zarządzania przedsiębiorstwem opartym na CRM.
Coyotos	https://www.gnu.org/software/hurd/microkernel/coyotos.html	Mikrojądro i system operacyjny. Jego głównym celem jest poprawienie niektórych niedociągnięć EROS.
CQUAL	https://www.usenix.org/legacy/publications/library/proceedings/sec02/full_papers/zhang/zhang_html/node7.html	Narzędzie do analizy statycznej oparte na typach, które pomaga programistom w wyszukiwaniu błędów w programach C. CQUAL.
CSIRT (*Computer Security Incident Response Team*)	https://www.nask.pl/pl/dzialalnosc/csirt-nask/3424,CSIRT-NASK.html	Ustawa o krajowym systemie cyberbezpieczeństwa implementująca do polskiego prawa dyrektywę w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. dyrektywę NIS).
Cyberterrory	https://pl.wikipedia.org	Cyberterroryzm – określenie opisujące dokonywanie aktów

zm	/wiki/Cyberterroryzm	terroru przy pomocy zdobyczy technologii informacyjnej. Ma na celu wyrządzenie szkody z pobudek politycznych lub ideologicznych, zwłaszcza w odniesieniu do infrastruktury o istotnym znaczeniu dla gospodarki lub obronności atakowanego kraju. Polega na celowym zakłóceniu interaktywnego, zorganizowanego obiegu informacji w cyberprzestrzeni.
DAM	https://en.wikipedia.org/wiki/Database_activity_monitoring	Monitorowanie aktywności bazy danych, inaczej audyt bazy danych przedsiębiorstwa i ochrona w czasie rzeczywistym to technologia bezpieczeństwa bazy danych służąca do monitorowania i analizowania aktywności bazy danych. DAM może łączyć dane z monitoringu sieciowego i natywnych informacji audytowych, aby zapewnić kompleksowy obraz aktywności bazy danych.
Danologia (*data science*)	https://pl.wikipedia.org/wiki/Danologia	Interdyscyplinarne pole używające naukowych metod, procesów, algorytmów i systemów do wydobywania spostrzeżeń z wielu danych strukturalnych i nieustrukturyzowanych. Powiązana jest z eksploracją danych (*data mining*), uczeniem maszynowym (*machine learning*) i analizą dużych zbiorów danych *Big data*).
DDoS, DoS	https://www.ovhcloud.com/pl/security/anti-ddos/ddos-definition/	Rozproszona odmowa dostępu do usługi (*Distributed Denial of Service*, DDoS) to broń uderzająca w cyberbezpieczeństwo. Jej celem jest zakłócenie działania usług lub wyłudzenie środków finansowych. Z technicznego punktu widzenia atak DDoS jest wersją ataku DoS (*Denial of Service*) i ma doprowadzić do przerwania ciągłości działań operacyjnych. DDoS generuje bardzo duży ruch w celu przeciążenia usługi, serwera lub połączenia sieciowego, co skutkuje ich niedostępnością. Ataki DoS przerywają działanie usługi, natomiast ataki rozproszone (DDoS) przynoszą szkody na większą skalę, gdyż powodują całkowite wyłączenie infrastruktury usługi *cloud*.
Debugger	https://pl.wikipedia.org/wiki/Debugger	Program komputerowy służący do dynamicznej analizy innych programów, w celu odnalezienia i identyfikacji zawartych w nich błędów, zwanych *bugami* (robakami).
Dekryptaż	https://sjp.pwn.pl/sjp/d	Odszyfrowanie zakodowanego tekstu.

	ekryptaz;2554539.html	
Disaster Recovery	https://www.whoa.com/disaster-recovery-business-continuity/	Bezpieczna w przypadku awarii usługa w chmurze, która umożliwia tworzenie kopii zapasowych danych i informacji wraz z ich odzyskiwaniem.
DLP (*Data Leak/Leakage/Loss Protection/Prevention*)	https://pl.wikipedia.org/wiki/Ochrona_przed_wyciekami_informacji	Ochrona przed wyciekami informacji to ogólna nazwa technologii informatycznych wspomagających ochronę danych w postaci elektronicznej przed kradzieżą lub przypadkowymi wyciekami. Systemy DLP wdraża się w organizacjach przetwarzających informacje podlegające ochronie z powodów biznesowych.
DNS (*Domain Name System*)	https://www.ovhcloud.com/pl/domains/dns-server/	Usługa zapewniająca powiązanie domeny z adresem IP danego serwera. Pozwala ona internaucie na dostęp do danej strony internetowej bez konieczności znania jej dokładnego adresu IP.
Domena	https://pl.wikipedia.org/wiki/Domena_internetowa	Domena internetowa – ciąg identyfikacyjny systemu *Domain Name System* (DNS), który określa zakres autonomii administracyjnej, uprawnień lub kontroli w Internecie. Nazwa domeny składa się z co najmniej jednej części (etykiety) umieszczonej w pewnym poddrzewie struktury DNS. Etykiety są łączone i rozdzielane kropkami, np. example.com. W pełni kwalifikowana nazwa domeny (FQDN) to nazwa domeny, która jest w zupełności określona za pomocą wszystkich etykiet w hierarchii DNS, bez pominięcia jakiejkolwiek części. W etykietach w DNS nie ma znaczenia wielkość liter, ale najczęściej nazwy domen są pisane małymi literami.
Dostęp gościnny do sieci Wi-Fi	https://plblog.kaspersky.com/guest-wifi/9740/	Oddzielny punkt dostępowy na routerze. Wszystkie domowe urządzenia łączą się z jednym punktem dostępowym i tworzą sieć; tymczasem sieć dla gości to oddzielny punkt, który umożliwia dostęp do Internetu, ale nie jest siecią domową.
E-government (*E-administracja*)	https://mfiles.pl/pl/index.php/E-Government	*E-administracja* jest to stosowanie technologii informatycznych, Internetu i nowoczesnych środków komunikacji w administracji publicznej. Wiąże się to ze zmianami organizacyjnymi i nowymi umiejętnościami służb publicznych, które mają poprawić jakość świadczonych przez administrację usług.

EROS (*Extremely Reliable Operating System*)	https://en.wikipedia.org/wiki/EROS_(microkernel)	Funkcje tego systemu operacyjnego obejmują automatyczną trwałość danych i procesów, wstępne wsparcie w czasie rzeczywistym oraz zabezpieczenia oparte na możliwościach. EROS jest badawczym systemem operacyjnym.
FDE	https://help.eset.com/efde/pl-PL/encryption_management.html	Zarządzanie szyfrowanymi stacjami roboczymi, które obejmuje zarządzanie logowaniem przed uruchomieniem.
FIPS (*Federal Information Processing Standard*)	https://pl.wikipedia.org/wiki/Federal_Information_Processing_Standard	Publicznie ogłaszane standardy federalnego rządu Stanów Zjednoczonych, z których korzystają cywilne agencje rządowe. Organizacją odpowiedzialną za ustalanie standardów FIPS jest Narodowy Instytut Standaryzacji i Technologii.
Firewall	https://www.cisco.com/c/pl_pl/products/security/firewalls/what-is-a-firewall.html	Zapora sieciowa to urządzenie zabezpieczające sieć, które monitoruje przychodzący i wychodzący ruch sieciowy i decyduje o jego przepuszczeniu lub zablokowaniu w oparciu o zestaw określonych zasad. Zapory sieciowe są pierwszą linią obrony w obszarze bezpieczeństwa sieci.
Flawfinder	https://dwheeler.com/flawfinder/	Główna witryna internetowa dla programu wykrywającego wady, prostego programu, który sprawdza kod źródłowy C/C++ i zgłasza możliwe słabe punkty bezpieczeństwa posortowane według poziomu ryzyka.
Fuzz testing (*fuzzing*)	https://pl.wikipedia.org/wiki/Fuzz_testing	Automatyczna lub półautomatyczna metoda testowania oprogramowania lub znajdowania w nim dziur, przydatnych przy atakach hakerskich. Polega ona na zautomatyzowanym wysyłaniu do programu różnego rodzaju losowych danych wejściowych i rejestrowaniu niepożądanych wydarzeń, np. wycieki pamięci czy nieautoryzowany dostęp.
GDPR/ RODO	https://apollogic.com/pl/it-dla-firm-poznan/gdpr/	Rozporządzenie o Ochronie Danych Osobowych (RODO), znane także jako GDPR (*General Data Protection Regulation*) dotyczy każdej firmy przetwarzającej dane osobowe obywateli Unii Europejskiej.
GhostNet	https://pl.wikipedia.org/wiki/GhostNet	Nazwa nadana przez popularne media sieci komputerowej szpiegowskiej, odkrytej w marcu 2009. Sieć ta zainfekowała komputery w przynajmniej 103 krajach.
Google Meet	https://en.wikipedia.org/wiki/Google_Meet	Usługa opracowana przez Google jest jedną z dwóch aplikacji, które stanowią zamiennik *Google Hangouts*, druga to *Google Chat*.
GUI	https://encyklopedia.p	Graficzny interfejs użytkownika - sposób komunikowania

	wn.pl/haslo/graficzny-interfejs-uzytkownika;3907397.html	się człowieka z oprogramowaniem komputera, wykorzystujący obiekty wyświetlane na monitorze w trybie graficznym. Do wprowadzania danych korzysta się z klawiatury i myszy.
GUU-3	https://bip.skw.gov.pl/ftp/skw/ulotka_WIL-GUU-3.pdf	Urządzenie przeznaczone do kryptograficznej i elektromagnetycznej ochrony informacji o klauzuli do TAJNE włącznie, przesyłanych w synchronicznych, publicznych lub resortowych sieciach teletransmisyjnych.
Haker (*hacker*)	https://pl.wikipedia.org/wiki/Haker_(slang_komputerowy)	Osoba o dużych, praktycznych umiejętnościach informatycznych (lub elektronicznych), która identyfikuje się ze społecznością hakerską. Hakerzy odznaczają się bardzo dobrą orientacją w Internecie, znajomością języków programowania, a także znajomością systemów operacyjnych.
Haking	https://edefinicje.pl/co-to-jest-haking	Szukanie i wykorzystywanie słabości w zabezpieczeniach systemów informatycznych, programów oraz sieci komputerowych.
Haktywizm	https://pl.wikipedia.org/wiki/Haktywizm	Haktywizm (*hacktivism*) to połączenie słów *hacking* i *activism* – użycie komputerów i sieci do promowania celów społecznych i politycznych, zwłaszcza wolności słowa, praw człowieka i dostępu do informacji.
Hierarchiczna baza danych	https://pl.wikipedia.org/wiki/Model_bazy_danych	Dane są przechowywane na zasadzie rekordów *nadrzędnych-podrzędnych*, tzn. rekordy przypominają strukturę drzewa. Każdy rekord (z wyjątkiem głównego) jest związany z dokładnie jednym rekordem nadrzędnym. Dane w takim modelu są znajdowane na zasadzie wyszukiwania rekordów podrzędnych względem rekordu nadrzędnego. Przykładem takiego modelu może być struktura katalogów na dysku twardym komputera.
HPE WebInspect	https://www.prevenity.com/pl/rozwiazania/	Zaawansowane rozwiązaniem do automatycznego testowania bezpieczeństwa aplikacji webowych i usług *Web Services*.
IBTI	https://www.bezpieczneit.com/tag/inspektor-bezpieczenstwa-teleinformatycznego/	Inspektor bezpieczeństwa teleinformatycznego
ICT (*information and*	https://pfr.pl/slownik/slownik-itict.html	Rodzina technologii przetwarzających, gromadzących i przesyłających informacje w formie elektronicznej.

communication technologies)		
IDS (*Intrusion Detection System*)	https://pl.wikipedia.org/wiki/Intrusion_Prevention_System	System – urządzenia sieciowe zwiększające bezpieczeństwo sieci komputerowych przez wykrywanie ataków w czasie rzeczywistym.
IDS (*Intrusion Detection System*)	https://pl.wikipedia.org/wiki/Intrusion_Prevention_System	Systemy wykrywania i zapobiegania włamaniom – urządzenia sieciowe zwiększające bezpieczeństwo sieci komputerowych przez wykrywanie (IDS).
IEC 62443	https://www.phoenixcontact.com/pl-pl/iec-62443-norma-cyberbezpieczenstwa-sieci-przemyslowych	Międzynarodowa seria norm opisująca zasadnicze wymagania w zakresie zapobiegania zagrożeniom bezpieczeństwa dla producentów komponentów, integratorów systemów i użytkowników.
IPS (*Intrusion Prevention System*)	https://pl.wikipedia.org/wiki/Intrusion_Prevention_System	System – urządzenie sieciowe zwiększające bezpieczeństwo sieci komputerowych przez wykrywanie i blokowanie ataków w czasie rzeczywistym.
ISO 22301	https://www.isoqar.pl/pl/certyfikacja/lista-certyfikatow/iso-22301?gclid=CjwKCAjwq-WgBhBMEiwAzKSH6Pb_535Tw5cA9TE_dupqdT6URrIC9k3G4UdTCB7HgUTCXYY8O_ijDRoC4p0QAvD_BwE	Międzynarodowa norma stanowiącą wymagania dla ustanowienia i zarządzania efektywnym systemem zarządzania ciągłością działania w każdej organizacji, niezależnie od rozmiaru i rodzaju prowadzonej działalności.
ISO 24762	https://sklep.pkn.pl/pn-iso-iec-24762-2010p.html	Norma pt. „*Technika informatyczna - Techniki bezpieczeństwa - Wytyczne dla usług odtwarzania techniki teleinformatycznej po katastrofie*”
ISO 27000	https://www.isoqar.pl/pl/aktualnosci/bezpieczenstwo-informacji/jakie-normy-naleza-do-rodziny-iso-27000	Seria, opublikowana przez ISO (Międzynarodową Organizację Normalizacyjną) i IEC (Międzynarodową Komisję Elektrotechniczną), wyjaśnia, jak wdrożyć najlepsze praktyki w zakresie bezpieczeństwa informacji.

ISO 27005	https://www.iso.org.pl/artykuly-i-informacje-dotyczace-systemow-zarzadzania/iso-27005-ocena-ryzyka-w-bezpieczenstwie-informacji/	Nowe wydanie standardu międzynarodowego ma pomóc organizacjom lepiej zarządzać swoim ryzykiem związanymi z bezpieczeństwem informacji.
ISO/IEC 15408-5:2022	https://www.iso.org/standard/72917.html	Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – Kryteria oceny bezpieczeństwa informatycznego – Część 5: Z góry określone pakiety wymagań bezpieczeństwa.
ISO/IEC 27001	https://pl.wikipedia.org/wiki/ISO/IEC_27001	Norma międzynarodowa standaryzująca systemy zarządzania bezpieczeństwem informacji. Została ogłoszona 14 października 2005 r. na podstawie brytyjskiej normy BS 7799-2 opublikowanej przez BSI. W Polsce normę ISO/IEC 27001 opublikowano 4 stycznia 2007 r. jako PN-ISO/IEC 27001:2007. Norma ta zastąpiła PN-I-07799-2:2005, czyli polską wersję brytyjskiego standardu BS 7799-2. ISO/IEC 27001:2005 (PN-ISO/IEC 27001:2007). Jest specyfikacją systemów zarządzania bezpieczeństwem informacji na zgodność z którą mogą być prowadzone audyty i na podstawie których są wydawane certyfikaty.
ISP	https://harbingers.io/definicje/isp	Dostawca dostępu do Internetu, która zapewnia dostęp do sieci osobom fizycznym i podmiotom gospodarczym. Mimo korzystania z usług firmy, usługobiorcy nadal potrzebują sprzętu telekomunikacyjnego, sieciowego i routingu, aby połączyć się z Internetem. ISP utrzymują po swojej stronie duże sieci infrastruktury technologicznej, które zapewniają ciągłość działania sieci.
IT	https://pfr.pl/slownik/slownik-itict.html	Technologie związane z komputerami i oprogramowaniem, nie związane jednak z technologiami komunikacyjnymi i dotyczącymi sieci.
ITSEC (*Information Technology Security Evaluation Criteria*)	https://pl.wikipedia.org/wiki/ITSEC	Zbiór kryteriów oceny bezpieczeństwa systemów teleinformatycznych wprowadzony w latach 90. XX w.
Join.Me	https://webcomm.eu/jo	Platforma do organizacji spotkań *online* oraz *webinarów***.**

	in-czesciowo-bezplatny-program-spotkan-online/	Program dostępny jest tylko w wersji anglojęzycznej, ale korzystanie z niego jest bardzo intuicyjne. Korzystanie z *Join.Me* dla grup do 10. osób jest bezpłatne.
Katalog błędów CVE	https://support.apple.com/pl-pl/HT202194	Zawartość związana z zabezpieczeniami w uaktualnieniu systemu Mac OS X do wersji 10.6.7 i uaktualnieniu zabezpieczeń 2011-001.
Kerberos	https://pl.wikipedia.org/wiki/Kerberos_(informatyka)	Protokół uwierzytelniania i autoryzacji w sieci komputerowej z zastosowaniem centrum dystrybucji kluczy, zaprojektowany w Massachusetts Institute of Technology (MIT).
Konwencja o cyberprzestępczości	https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20150000728	Dz.U. 2015 poz. 728. Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.
Kryptografia	https://en.wikipedia.org/wiki/Cryptography	Kryptografia polega na konstruowaniu i analizowaniu protokołów, które uniemożliwiają osobom trzecim lub opinii publicznej odczytywanie prywatnych wiadomości. Współczesna kryptografia istnieje na przecięciu dyscyplin matematyki, informatyki, bezpieczeństwa informacji, elektrotechniki, cyfrowego przetwarzania sygnałów, fizyki. Podstawowe koncepcje związane z bezpieczeństwem informacji (poufność danych, integralność danych, uwierzytelnianie i niezaprzeczalność) są kluczowe dla kryptografii. Praktyczne zastosowania kryptografii obejmują handel elektroniczny, karty płatnicze z chipem, waluty cyfrowe, hasła komputerowe i łączność wojskową.
KSC	https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-	Ustawa o krajowym systemie cyberbezpieczeństwa, implementującą do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa 2016/1148), tzw. dyrektywa NIS.
Ksenofobia	https://pl.wikipedia.org/wiki/Ksenofobia https://www.welbi.pl/ksenofobia-co-to-jak-leczyc-przyklady/	Ksenofobia - strach przed obcymi. Ksenofobia może dotyczyć wszystkiego, co wiąże się z obcokrajowcami, osobami nieznanymi, innymi pod pewnymi względami. Ksenofobia to bardzo częste uprzedzenie. Szczególnie wyraźnie widać ją teraz, kiedy do Polski

		przybyło wielu uchodźców zza wschodniej granicy. Osoby, które mają naturalną skłonność do uprzedzeń, mają bardzo sztywny światopogląd i są zamknięte na nowe informacje. Wierzą, że uprzedzenia chronią je przed krzywdą ze strony „obcych", okazywana im wrogość służy zaś bezpieczeństwu i spójności grupy, do której należą.
KVM (*Keyboard, Video Mouse*)	https://www.conrad.pl/pl/strefa-porad/komputer-i-biuro/przelaczniki-kvm-zasada-dzialania-i-zastosowanie.html	Urządzenia służące do zarządzania sygnałami związanymi z urządzeniami peryferyjnymi. Dzięki temu możliwe jest odizolowanie komputera jako jednostki roboczej od okablowania związanego z urządzeniami wejścia (mysz, klawiatura) oraz urządzeniem wyjściowym (monitor). Otwiera to nowe drogi konfiguracji stanowisk komputerowych pozwalające na umiejscowienie użytkownika z dala od komputera, wykorzystywanie jednego zestawu urządzeń peryferyjnych do obsługi wielu komputerów.
LM (*Lean Management*)	https://pl.wikipedia.org/wiki/Lean_management	Koncepcja zarządzania przedsiębiorstwem, która rozwinęła się w oparciu o zasady i narzędzia *Systemu Produkcyjnego Toyoty* (TPS).
Mac OS	https://pl.wikipedia.org/wiki/Mac_OS	System operacyjny komputerów Macintosh. Starsze wersje są określane jako *Mac OS Classic*. Mac OS X – tj. Mac OS numer 10 został opracowany w oparciu o całkiem nowe rozwiązania systemowe oraz zasadniczym zmianom uległ także interfejs użytkownika.
Malware (*malware*)	https://pl.wikipedia.org/wiki/Z%C5%82o%C5%9Bliwe_oprogramowanie	Połączenie słów *malicious* „złośliwy" i *software* „oprogramowanie". Złośliwe, szkodliwe oprogramowanie – ogół programów o szkodliwym działaniu w stosunku do systemu komputerowego lub jego użytkownika.
Microsoft Teams	https://pl.wikipedia.org/wiki/Microsoft_Teams	Usługa internetowa oparta na chmurze zawierająca zestaw narzędzi i usług służących współpracy zespołowej. Usługa łączy funkcjonalność z innymi produktami Microsoftu, takimi jak *Microsoft Office* oraz *Skype*.
NAC	https://www.nac.gov.pl	Narodowe archiwum cyfrowe
Nessus Professional	https://www.passus.com/produkty/tenable/nessus	Pojedynczy skaner, który wykrywa podatności przy pomocy dwóch metod: skanowania sieciowego, skanowania z uwierzytelnieniem.
NFV	https://www.linkedin.com/pulse/wirtualizacja-funkcji-sieciowych-	Wirtualizacja funkcji sieciowych to nowoczesna technologia, która umożliwia wdrażanie zwirtualizowanych usług sieciowych zamiast tradycyjnego sprzętu.

	najlepsze-praktyki-slawski/?originalSubdomain=pl	Jest to pomocne w architekturze sieci i może być zastosowane w oddzieleniu funkcji sieciowych od sprzętu. Pojawiło się wiele technologii, od przetwarzania w chmurze i *OpenFlow* po sieci definiowane programowo (SDN).
NIST (*National Institute of Standards and Technology*)	https://pl.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology	Narodowy Instytut Norm i Techniki – amerykańska agencja federalna pełniąca funkcję analogiczną do Głównego Urzędu Miar.
Nmap (*network mapper*)	https://pl.wikipedia.org/wiki/Nmap	Wolny i otwartoźródłowy program komputerowy służący do skanowania portów i wykrywania usług w sieci.
Openflow	https://exatel.pl/wiedza/materialy/artykuly/openflow-omowienie-protokolu/	Protokół *Openflow* jest jednym z najpopularniejszych protokołów SDN (*Software Defined Networking*). Umożliwia zdalne sterowanie warstwą danych switchy *Openflow* oraz zarządzanie mechanizmami QoS.
OpenSSH (*Open Secure Shell*)	https://pl.wikipedia.org/wiki/OpenSSH	Zestaw programów komputerowych zapewniających szyfrowaną komunikację w sieci komputerowej dzięki protokołowi SSH. Opiera się o kod ostatniej wolnej wersji tego programu i od tego czasu rozwija się niezależnie.
OpenSSL	https://pl.wikipedia.org/wiki/OpenSSL	Wieloplatformowa, otwarta implementacja protokołów SSL (wersji 2 i 3) i TLS (wersji 1) oraz algorytmów kryptograficznych ogólnego przeznaczenia. Udostępniana jest na licencji zbliżonej do licencji Apache. Dostępna jest dla systemów uniksopodobnych (*Linux*, BSD, *Solaris*), *OpenVMS* i *Microsoft Windows*. Zawiera biblioteki implementujące wspomniane standardy oraz mechanizmy kryptograficzne, a także zestaw narzędzi konsolowych (przede wszystkim do tworzenia kluczy oraz certyfikatów, zarządzania urzędem certyfikacji, szyfrowania, dekryptażu i obliczania podpisów cyfrowych).
Pharming	https://pl.wikipedia.org/wiki/Pharming	Polega na modyfikacji zawartości adresu WWW w celu przekierowania użytkownika na fałszywą stronę, mimo wpisania prawidłowego adresu strony. Ma to na celu przejęcie wejścia do zaufanych witryn haseł, numerów kart kredytowych i innych poufnych danych.
Phishing	https://pl.wikipedia.org/wiki/Phishing	Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych

		informacji (danych logowania, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem, czy też nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.
Portal autoryzacji	https://stormshield.edu.pl/index.php/portal-autoryzacji-autoryzacja-ssl/	Przykładowo NETASQ UTM daje możliwość autoryzacji użytkowników w oparciu o certyfikat SSL. Funkcjonalność ta może znaleźć zastosowanie w sytuacji, gdy chcemy udostępnić na zewnątrz zasoby z sieci wewnętrznej np. serwis WWW dla naszych klientów lub dostęp do RDP dla pracowników a z różnych powodów autoryzacja certyfikatem jest dla nas bardziej odpowiednia niż standardowa autoryzacja za pomocą hasła. Najlepszym miejscem przechowywania certyfikatu jest *token kryptograficzny* lub karta *smartcard*.
Programy do wideokonferencji	https://nano.komputronik.pl/n/program-do-wideokonferencji/	Lista 7 najlepszych programów, które pozwalają na prowadzenie telekonferencji *online: Microsoft Teams, Zoom, Google Meet, Cisco Webex, Join.me, Skype, WhatsApp.*
Protokół 802.1x	http://kti.eti.pg.gda.pl/ktilab/radius/Opis%20uwierzytelniania%20metoda%20802.1x.pdf	Narzędzie pozwalające na bezpieczne i zcentralizowane uwierzytelnianie użytkowników w operatorskich sieciach dostępowych opartych o różnego rodzaju rozwiązania typu *Dial-up*. Pozwala on serwerom dostępowym (*Network Access Server – NAS*) na określenie czy próbujący połączyć się za ich pośrednictwem z siecią użytkownik posiada stosowne uprawnienia oraz na określenie właściwej dla danego użytkownika konfiguracji połączenia (protokół transportowy, jego parametry, adresy IP).
Protokół Needhama-Schroedera	https://www.mimuw.edu.pl/~sl/teaching/03_04/WPKWK/PREZENTACJE-SPIN_UPPAAL/NS/	Metoda autoryzacji oparta na kluczu publicznym i prywatnym. Jej celem jest ustanowienie wzajemnej autoryzacji między inicjatorem A a odbiorcą B, po której może nastąpić sesja, podczas której A i B będą wymieniać wiadomości.
Przetwarzanie w chmurze	https://azure.microsoft.com/pl-pl/resources/cloud-computing-dictionary/what-is-cloud-computing/	Najprościej rzecz ujmując, *przetwarzanie w chmurze* to dostarczanie usług obliczeniowych – w tym serwerów, magazynu, baz danych, sieci, oprogramowania, analizy i inteligencji – za pośrednictwem Internetu („*chmura*”) w celu zaoferowania szybszych innowacji, elastycznych zasobów i ekonomii skali. Płaci się za używane usługi w chmurze, co pomaga obniżyć koszty operacyjne, wydajniej korzystać z infrastruktury.

Punkt kontaktowy	https://www.infor.pl/prawo/encyklopedia-prawa/p/290823,Punkt-kontaktowy.html	Punkt kontaktowy umożliwia złożenie drogą elektroniczną do właściwych organów wniosków, oświadczeń lub notyfikacji niezbędnych do podjęcia, wykonywania lub zakończenia działalności gospodarczej oraz uznania kwalifikacji zawodowych.
Qualys	https://imns.pl/qualys-dokladnosc-skanowania/	Skanowanie podatności i konfiguracji umożliwia wykrywanie niewidocznych systemów i identyfikowanie podatności, zanim zrobią to przestępcy. Od dokładności tych skanów zależy, jak skutecznie ich wyniki mogą być później wykorzystane przez zespoły IT do znalezienia i naprawienia najpoważniejszych problemów związanych z bezpieczeństwem i konfiguracją.
Ransomware	https://pomoc.home.pl/baza-wiedzy/czym-jest-ransomware-dlaczego-moj-komputer-zostal-zablokowany	Jedna z wielu form złośliwego oprogramowania, którego działanie sprowadza się najczęściej do zablokowania dostępu do określonych danych lub całego komputera.
Router	https://pl.wikipedia.org/wiki/Router	*Ruter* (trasownik) – urządzenie sieciowe pracujące w trzeciej warstwie modelu OSI. Służy do łączenia różnych sieci komputerowych, pełni więc rolę węzła komunikacyjnego. Na podstawie informacji zawartych w pakietach TCP/IP jest w stanie przekazać pakiety z dołączonej do siebie sieci źródłowej do docelowej, rozróżniając ją spośród wielu dołączonych do siebie sieci. Proces kierowania ruchem nosi nazwę trasowania, *routingu* lub *routowania*.
Scam	https://www.politykabezpieczenstwa.pl/pl/a/czym-jest-scam-i-czy-powinnismy-sie-go-obawiac	Każda forma oszustwa, w tym oszustwa przez Internet czy telefonicznego. Jest to próba bezpośredniego wzbudzania zaufania poprzez kontakty osobiste, wysyłanie *e-mali* i tradycyjnych listów, po skomplikowane technicznie zabiegi z użyciem usług internetowych. Najczęstszą formą *scamu* jest masowa korespondencja w formie elektronicznej. Ofiara *scamera* jest przekonana, że dzwoni do niej policjant, urzędnik czy też pracownik banku.
Serwer DNS	https://www.netia.pl/pl/blog/serwer-dns	DNS (*Domain Name System*) to protokół, którego główna funkcja polega na tłumaczeniu łatwych do zapamiętania przez człowieka nazw domen na zrozumiałe dla

		komputerów dane liczbowe. Serwer DNS wyszukuje adres IP danej strony na podstawie wpisu użytkownika zamieszczonego w polu adresu wyszukiwarki. Mechanizm działania systemu DNS przypomina więc książkę telefoniczną, w której do określonych osób przypisane są numery telefonów. Jest to ogromna baza danych umieszczonych w rekordach, z której korzystają użytkownicy z całego świata.
Sieć radiowa	https://www.bryk.pl/wypracowania/pozostale/informatyka/15921-charakterystyka-sieci-radiowej.html	Sieć radiowa stanowi alternatywne rozwiązanie dla sytuacji, w których nie można przeprowadzić kabli pod ziemią, lub gdy chodzi o zachowanie w idealnym stanie na przykład zabytkowego budynku. Znajduje ona zastosowanie również w miejscach, w których istotne jest swobodne poruszanie się i łatwy dostęp do sieci.
SIEM (*Security Information and Event Management*)	https://www.netia.pl/pl/srednie-i-duze-firmy/youtro-strefa-wiedzy/system-bezpieczenstwa-siem-co-to-jest#1	System informatyczny służący poprawie cyberbezpieczeństwa firmy poprzez zbieranie oraz analizowanie informacji o incydentach, błędach i podatnościach w czasie rzeczywistym. Skuteczność tego systemu wynika z symultanicznego analizowania informacji z wielu źródeł pracujących w obrębie sieci firmowej (między innymi z *firewalli*, UTM-ów, serwerów DNS, *routerów*, programów antywirusowych) oraz dostarczaniu kompletnej analizy ryzyka, a nie samych informacji.
Site survey	https://en.wikipedia.org/wiki/Site_survey	Inspekcje obszaru, na którym proponowane są prace, w celu zebrania informacji do projektu lub oszacowania wykonania wstępnych zadań wymaganych do działania na świeżym powietrzu. Określa dokładną lokalizację, dojazd, najlepszą orientację w terenie oraz lokalizację przeszkód.
Skype	https://pl.wikipedia.org/wiki/Skype	Komunikator internetowy firmy Microsoft, oparty na technologii przetwarzania danych w chmurze. Umożliwia prowadzenie darmowych rozmów głosowych oraz obserwację rozmówcy poprzez kamerę internetową, a także płatnych rozmów z posiadaczami telefonów stacjonarnych lub komórkowych za pomocą technologii VoIP (*Voice over IP*). Oprócz tego *Skype* oferuje funkcje bezpośredniej wymiany informacji tekstowych za pomocą ręcznie wpisywanych wiadomości oraz przesyłanie plików.

SMTP (*Simple Mail Transfer Protocol*)	https://pl.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol	Protokół komunikacyjny opisujący sposób przekazywania poczty elektronicznej w Internecie.
SOC	https://en.wikipedia.org/wiki/Security_operations_center	Monitorowa sieć przemysłowa (*Security Operation Center*), która odpowiada za ochronę organizacji przed cyberzagrożeniami. Analitycy SOC prowadzą całodobowy monitoring sieci organizacji i badają wszelkie potencjalne incydenty bezpieczeństwa. W przypadku wykrycia cyberataku analitycy SOC są odpowiedzialni za podjęcie wszelkich kroków niezbędnych do jego usunięcia. Obejmuje trzy elementy składowe służące do zarządzania i wzmacniania stanu bezpieczeństwa organizacji: ludzi, procesów i technologii.
Solaris	https://www.oracle.com/pl/solaris/solaris11/	*Oracle Solaris* to platforma biznesowa. System operacyjny *Oracle Solaris 11* zapewnia spójność i kompatybilność, jest prosty w obsłudze i zaprojektowany tak, aby zawsze zapewniać bezpieczeństwo.
Spamowanie	https://en.wikipedia.org/wiki/Spamming	Wykorzystywanie systemów przesyłania wiadomości do wysyłania wielu niechcianych wiadomości (*spamu*) do dużej liczby odbiorców w celach reklamy komercyjnej, w celu niekomercyjnego nawracania lub w jakimkolwiek zabronionym celu lub po prostu wielokrotnie wysyłając tę samą wiadomość do tego samego użytkownika.
Spear phishing	https://www.kei.pl/slownik/spear-phishing	Rodzaj *phishingu* o bardziej ukierunkowanym charakterze. Personalizacja wiadomości wywołuje u użytkownika wrażenie, że zna adresata – prywatną osobę bądź instytucję. Treść takich wiadomości odwołuje się do osobistych informacji czy wspólnego znajomego. Podszywanie się pod znajomych ma na celu wyłudzenie haseł.
SPIM	https://en.wikipedia.org/wiki/Messaging_spam	*Spam* wiadomości, czasami nazywany SPIM, to rodzaj *spamu* skierowany do użytkowników komunikatorów internetowych (IM), SMS-ów lub prywatnych wiadomości w witrynach internetowych.
Spoofing	https://pl.wikipedia.org/wiki/Spoofing	Grupa ataków na systemy teleinformatyczne polegająca na podszywaniu się pod inny element systemu informatycznego. Efekt ten osiągany jest poprzez umieszczanie w sieci preparowanych pakietów danych lub niepoprawne używanie

		protokołów.
Systemy ICS/OT	https://networkexpert.pl/cyberbezpieczenstwo/bezpieczenstwo-ot-i-ics-bezpieczenstwo-sieci-przemyslowych/	Systemy operacyjne służące do monitorowania, sterowania oraz kontroli procesów podczas produkcji (OT) oraz przemysłowe systemy sterowania (ICS), które są często podłączone do Internetu bez właściwej ochrony sieci.
TCSEC (*Trusted Computer System Evaluation Criteria*)	https://pl.wikipedia.org/wiki/TCSEC	Dokument powstały z inicjatywy Agencji Bezpieczeństwa Narodowego Departamentu Obrony USA oraz Narodowego Biura Standaryzacji. Opisuje podstawowe wymagania, jakie muszą spełnić środki ochrony w systemie komputerowym do przetwarzania informacji podlegającej ochronie. Został zastąpiony przez międzynarodowy standard *Common Criteria*.
Telefon VoIP	https://pl.wikipedia.org/wiki/Telefon_VoIP	Typ aparatu telefonicznego, który w przeciwieństwie do tradycyjnych aparatów PSTN lub ISDN nie jest podłączany do sieci telefonicznej, lecz do sieci komputerowej, a połączenia są realizowane za pomocą technologii VoIP.
Tester zabezpieczeń IT (*Penetration Tester*)	https://www.devire.pl/pentester/	Etyczny haker mający za zadanie włamywanie się do systemów firm na ich własne życzenie, szukając tym samym luk i lokalizując ewentualne słabe punkty, po to, by uchronić system przed prawdziwym atakiem. Do jego obowiązków należy też wytwarzanie złośliwego oprogramowania, tak by zawsze wyprzedzać prawdziwych cyberprzestępców.
TI	https://pl.wikipedia.org/wiki/TI	Technika informatyczna, (*information technology, IT*) – dyscyplina informatyczna i branża na rynku pracy zajmująca się stosowaniem technologii obliczeniowych (oprogramowanie i sprzęt komputerowy) w biznesie, instytucjach państwowych, opiece zdrowotnej, szkołach i innych typach organizacji. W szerszym znaczeniu (jako informatyka techniczna), obejmuje inżynierię oprogramowania, inżynierię komputerową, systemy informacyjne, cyberbezpieczeństwo i *danologię*. Jest ona także powiązana z sektorem teleinformatycznym.
Unified Communication	https://pl.wikipedia.org/wiki/Komunikacja_zintegrowana	Komunikacja zintegrowana – technologia pozwalająca na zintegrowanie w czasie rzeczywistym usług komunikacyjnych, takich jak komunikator internetowy (*czat*), informacja o obecności, połączenie telefoniczne (w

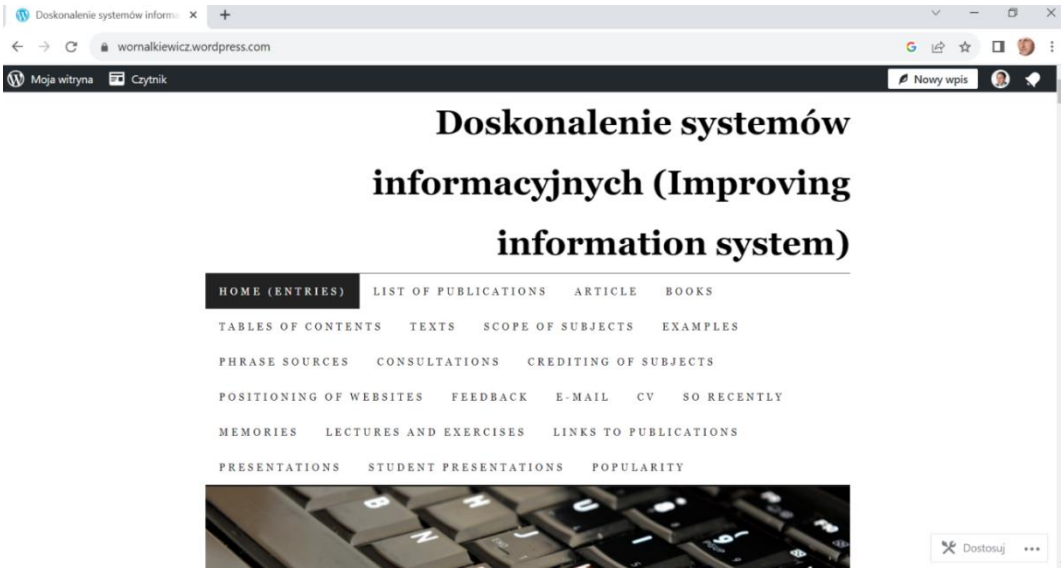
		tym telefonii wykorzystujących protokół IP), możliwość wideokonferencji, udostępnianie danych (w tym wykorzystanie tablicy elektronicznej) oraz ujednoliconej komunikacji (zintegrowana poczta głosowa, *e-mail*, SMS i faks).
URL (*Uniform Resource Locator*)	https://pl.wikipedia.org/wiki/Uniform_Resource_Locator	Ujednolicony format adresowania (określania lokalizacji) zasobów (informacji, danych, usług) stosowany w Internecie i w sieciach lokalnych. Standard URL opisany jest w dokumencie RFC 1738[1]. Tak zwany adres URL najczęściej kojarzony jest z adresami stron WWW, ale ten format adresowania służy do określania lokalizacji wszelkich zasobów dostępnych w Internecie.
VCISO	https://resilia.pl/landing-page/vciso-wirtualny-cyber-ekspert-usluga-dla-firm/	Usługa *outsourcingu* typu *wirtualny cyber ekspert* firmy RESILIA , która umożliwia firmie kompleksowe i wygodne zarządzanie cyberbezpieczeństwem oraz ochroni ją przed cyberzagrożeniami bez konieczności zatrudniania szeregu specjalistów wewnątrz organizacji.
VPN (*virtual private network*)	https://nordvpn.com/pl/what-is-a-vpn/	VPN tworzy zaszyfrowany tunel dla danych użytkownika, chroni jego tożsamość w sieci poprzez ukrycie adresu IP i pozwala bezpiecznie korzystać z publicznych Wi-Fi.
WAN (*Wide Area Network*)	https://pl.wikipedia.org/wiki/Rozleg%C5%82a_sie%C4%87_komputerowa	Rozległa sieć komputerowa znajdująca się na obszarze wykraczającym poza miasto, kraj lub kontynent. Internet jest obecnie największą istniejącą siecią WAN.
WhatsApp	https://pl.wikipedia.org/wiki/WhatsApp	Mobilna aplikacja dla smartfonów, służąca jako komunikator internetowy. Aplikacja ta jest dostępna dla różnych platform: *iOS*, *Android* i *KaiOS*.
Wi-Fi	https://pl.wikipedia.org/wiki/Wi-Fi	Zestaw standardów stworzonych do budowy bezprzewodowych sieci komputerowych. Szczególnym zastosowaniem jest budowanie sieci lokalnych (LAN) opartych na komunikacji radiowej, czyli WLAN. Zasięg od kilku metrów do kilku kilometrów i rzeczywistej przepustowości sięgającej 900 Mb/s, przy transmisji w standardzie 802.11ac na trzech kanałach o szerokości 80 MHz jednocześnie. Produkty zgodne z Wi-Fi mają na sobie odpowiednie logo, które świadczy o zdolności do współpracy z innymi

[1] Berners-Lee T., Masinter L., McCahill M., *Uniform Resource Locators* (URL), IETF, 1994.

		produktami tego typu.
Wireless Network Watcher	https://wireless-network-watcher.softonic.pl/	Darmowy program, umożliwiający wykrycie intruzów w sieci Wi-Fi lub *Ethernet*. Umożliwia zidentyfikowanie osób, które nielegalnie korzystają z naszego łącza internetowego.
Wirtualizacja	https://pl.wikipedia.org/wiki/Wirtualizacja	Proces symulowania przez oprogramowanie istnienia zasobów logicznych, które wykorzystują ustalone podczas konfiguracji zasoby fizyczne. np. wirtualna maszyna stosuje wirtualizację w celu emulowania pracy maszyny z danym systemem operacyjnym pozwalając przez to badać zachowanie tej maszyny i jej oprogramowania bez wpływania na realny system operacyjny, na którym pracujemy.
Wirus komputerowy	https://pl.wikipedia.org/wiki/Wirus_komputerowy	Program komputerowy posiadający zdolność powielania się, tak jak prawdziwy wirus, stąd jego nazwa. Wirus do swojego działania potrzebuje i wykorzystuje system operacyjny, aplikacje oraz tożsamość użytkownika komputera. Wirusa komputerowego zalicza się do szkodliwego oprogramowania (*malware*). Do zwalczania wirusów komputerowych stosuje się programy antywirusowe i skanery wykrywające szkodliwe oprogramowanie (*anti-malware scanners*). W zabezpieczeniu się przed wirusami pomagają również stałe aktualizacje systemu i aplikacji.
Witryny WWW	https://seospace.pl/slownik/co-to-jest-witryna-internetowa/	Witryna internetowa, nazywana też serwisem internetowym, to wszystkie strony, podstrony oraz adresy URL wchodzące w skład jednej domeny. Są one zazwyczaj umieszczone na jednym serwerze.
Zoom	https://pl.wikipedia.org/wiki/Zoom_(oprogramowanie)	Oprogramowanie do wideokonferencji opracowane przez Zoom Technologies z San Jose.

10. Prezentacja wykładów z przedmiotu:
„Bezpieczeństwo telekomunikacyjne i cyberbezpieczeństwo”

Problematyka zagadnienia „*Bezpieczeństwo teleinformatyczne i cyberbezpieczeństwo*” jest bardzo obszerna. W zarysie została zasygnalizowana w zamieszczonej w tym rozdziale prezentacji wykładu 1. „*Wprowadzenie*”. Szersze odniesienie do dalszych wykładów w trybie *online* znajdzie Czytelnik w załączniku stanowiącym integralną część wersji elektronicznej niniejszej pracy. Warto zwrócić uwagę na początku prezentacji wykładów na dość obszerne określenie skrótów i pojęć dotyczących pojętego zagadnienia. Nadmienię jeszcze, że komplet wykładów znajdzie się też, po opublikowaniu tego podręcznika, na moim blogu „*Procesy informacyjne w teorii i praktyce*” prowadzonym na WordPress[2]. Umożliwi to szeroki dostęp Internautom do tego materiału oraz innych zasobów z zakresu doskonalenia procesów informacyjnych z zastosowaniem metod ilościowych wspomaganych techniką IT. Na rysunku 10.1 pokazano stronę tytułową wspomnianego blogu.

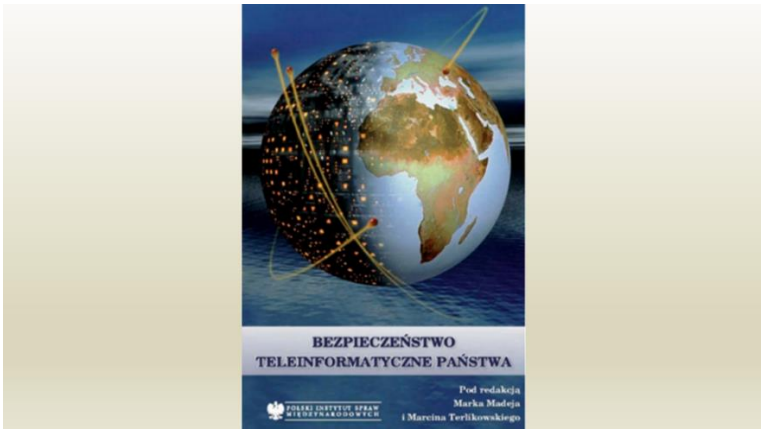


Źródło: Opracowanie własne.

Rys. 10.1. Zakładki blogu „*Procesy informacyjne w teorii i praktyce*”

[2] Wornalkiewicz W., *Popularyzacja metod ilościowych w Internecie*, Wydawnictwo Instytut Śląski, Opole 2017.

Na dalszych kolejnych stronach zestawiono przykładowo slajdy *Wykładu 1*.



Jest to monografia zbiorowa pod redakcją Marka Madeja, która obejmuje zagadnienia:
Rewolucja informatyczna - istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego.
Sieć Internet - znaczenie dla nowoczesnego państwa oraz problemy bezpieczeństwa,

Systemy teleinformatyczne w systemie płatniczym kraju - funkcjonowanie i znaczenie.

Sieci teleinformatyczne jako instrument państwa - zjawisko walki informacyjnej.

Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm.

Monitoring stanu bezpieczeństwa teleinformatycznego państwa.
Kodowanie, szyfrowanie i integralność informacji elektronicznej. Wyzwania dla bezpieczeństwa państw.
Społeczeństwo informacyjne a problemy rozwoju *e-governmentu* w Polsce.
UE a bezpieczeństwo teleinformatyczne - inicjatywy i wyzwania.

Konwencja o cyberprzestępczości - międzynarodowa odpowiedź na przestępczość ery informacyjnej.

Protokół dodatkowy do Konwencji o cyberprzestępczości dotyczący penalizacji czynów o charakterze rasistowskim, ksenofobicznym popełnionych przy użyciu systemów komputerowych.

Polityk, decydując o przyjęciu strategii zapewnienia bezpieczeństwa narodowego w wymiarze teleinformatycznym, musi brać pod uwagę techniczne możliwości wdrożenia proponowanych rozwiązań.

Podobnie administrator sieci, dbający o stabilność nadzorowanego systemu, powinien pamiętać o szerszym kontekście wymogów bezpieczeństwa teleinformatycznego, np. konieczności ich pogodzenia z innymi priorytetami państwa w dziedzinie bezpieczeństwa narodowego.

Opracowania dotyczące problemów bezpieczeństwa teleinformatycznego nierzadko otwierają sugestywne opisy wysublimowanych, ale zarazem bardzo skutecznych ataków na sieci komputerowe, prowadzących do poważnych zakłóceń funkcjonowania wszystkich sfer życia nowoczesnego społeczeństwa.

Sprawcy, najczęściej nazywani cyberterrorystami, kilkoma kliknięciami doprowadzają do przerw w dostawach prądu elektrycznego czy też wody, uniemożliwiają odbiór telewizji lub blokują funkcjonowanie Internetu, powodując w konsekwencji krachy giełdowe i bankructwa banków, a nawet śmierć setek osób w wypadkach lotniczych, kolejowych i przemysłowych.

Jak do tej pory żaden z takich katastroficznych scenariuszy się nie zrealizował.
Nie oznacza to jednak, że problemy bezpieczeństwa teleinformatycznego można bagatelizować. Obraz zagrożeń pojawiających się w tym specyficznym wymiarze bezpieczeństwa państwa jest bowiem skomplikowany, dorównując barwności fikcyjnym scenariuszom.

W ostatnich dniach kwietnia 2007 r. w Estonii, uwikłanej wówczas w konflikt polityczny z Rosją, doszło do zaskakujących zakłóceń ruchu internetowego.

Lawinowo wzrosła ilość danych przesyłanych pod określone adresy, głównie rządowe serwery z informacyjnymi witrynami WWW.

Dość szybko doprowadziło to do ich przeciążenia i – w konsekwencji – niedostępności portali estońskich instytucji rządowych dla użytkowników Internetu.
Stało się jasne, że miał miejsce celowy atak.
W ciągu następnych kilku dni podobne ataki powtórzyły się, a ich siła gwałtownie wzrosła.

W wyniku zalewu danymi w ilości kilkakrotnie większej niż maksymalna przepustowość estońskiej infrastruktury internetowej została ona praktycznie sparaliżowana.
Internet, stanowiący w Estonii istotny, wręcz podstawowy, kanał komunikacji zawodowej i publicznej, rozwijany dynamicznie w ciągu ostatniej dekady i będący chlubą tego kraju, niemal przestał działać.

Pojawiły się sugestie, że jest to kompleksowy, drobiazgowo zaplanowany atak na estoński Internet, przeprowadzony przez bliżej niezidentyfikowany, choć prawdopodobnie pochodzącą głównie z Rosji grupę osób;
mówiono o cyberterroryżmie, cyberwojnie, cybersabotażu.

W kilka miesięcy po tym wydarzeniu media na całym świecie donosiły o aktach cyberszpiegostwa – bezprecedensowej w swej skali kradzieży danych z komputerów wielu najważniejszych instytucji rządowych USA, włącznie z Pentagonem, zorganizowanej przez nieznaną grupę sprawców.

W tym samym czasie eksperci z dziedziny bezpieczeństwa teleinformatycznego zwrócili uwagę na fakt, że na świecie działają setki tysięcy komputerów zainfekowanych odpowiednio spreparowanym oprogramowaniem, które bez wiedzy i woli ich właścicieli pozwala na zdalne przejmowanie nad nimi kontroli i wykorzystywanie do różnych celów.

Największą taka nielegalna sieć, ze względu na swoje rozmiary nazwana Kraken liczyć miała około 800 tys. maszyn
Temat aktów szpiegostwa wymierzonych przeciwko rządowym sieciom USA i innych państw, głównie sojuszników z NATO, powrócił w mediach światowych także na początku 2009 r.

Eksperci z Kanady zaprezentowali raport na temat grupy określającej siebie nazwą GhostNet, która rzekomo zajmuje się „zawodowo" szpiegostwem komputerowym.
W marcu 2009 r. media przestrzegały przed nowym niebezpiecznym wirusem Conficker, który 1 kwietnia miał sparaliżować setki tysięcy komputerów.

O narastających problemach w sferze bezpieczeństwaormatycznego w ostatnich latach mówiono również w Polsce.
Media coraz częściej podejmowały choćby temat oszustw dotykających posiadaczy kont bankowych on-line.

Policja ujawniła przypadki ataków internetowych na nieostrożnych klientów banków, którzy, oszukani w odpowiedni sposób, ujawniali swoje dane złodziejom – cyberprzestępcom.

Wielkości skradzionych w ten sposób środków jednak nie ujawniono.

Jednocześnie, w ciągu kilku kolejnych miesięcy polska Policja informowała o serii działań wymierzonych przeciw osobom rozpowszechniającym pornografię dziecięcą w Internecie – skomplikowane operacje prowadzone przede wszystkim w cyberprzestrzeni doprowadziły do zatrzymań, w skali całej Polski kilkuset osób.

W kontekście każdego z tych wydarzeń mówiono o bezpieczeństwie teleinformatycznym (informatycznym), posługując się jednak czasem odmiennymi terminami.
Również w stosunku do ich sprawców stosowano, zamiennie i niekonsekwentnie, różnorodne, a ponadto z reguły nieprecyzyjne określenia .

Podejmowano także próby klasyfikowania tych zdarzeń, umieszczania ich na mapie zagrożeń związanych z wykorzystywaniem technologii teleinformatycznych.
Wysiłki te dawały jednak zazwyczaj obraz nadmiernie uproszczony, uwypuklający jedynie wybrane aspekty poruszanych problemów, a całkowicie pomijający inne.

Dodatkowo sama dyskusja na te tematy prowadzona była przy użyciu specyficznego technicznego żargonu, co utrudniało zrozumienie istoty problemu.
Sytuacja ta jest konsekwencją wieloznaczności pojęcia bezpieczeństwa teleinformatycznego oraz zróżnicowania sposobów jego definiowania.

Wieloaspektowość i wielopłaszczyznowość tego zagadnienia wynika z różnorodności i dużej liczby poziomów, na których należy je rozpatrywać.

Może się ono bowiem odnosić do bardzo różnych podmiotów.

Począwszy od użytkownika indywidualnego - przez przedsiębiorstwa i instytucje, wykorzystujące całe sieci teleinformatyczne, aż po samo państwo (jego struktury administracyjne, organy i służby czy też gospodarkę), a nawet system międzynarodowy ujmowany całościowo (poziom najwyższy).

Na każdym z tych poziomów zakres pojęcia bezpieczeństwa teleinformatycznego będzie inny, odmienne będą też skala i powaga następstw jego naruszeń oraz metody i środki jego zapewniania.

Co więcej, za zagrożenia uznawane będą różne zjawiska, procesy, wydarzenia czy działania.

Najbardziej rozpowszechnione określenia, często używane w odniesieniu do zagadnień bezpieczeństwa teleinformatycznego, traktowane z reguły – choć nie zawsze zasadnie – jako synonimy i wykorzystywane wymiennie to bezpieczeństwo informacyjne (*information security*) i cyberbezpieczeństwo (*cybersecurity*).

W mediach najczęściej mówi się o cyberprzestępcach, cyberterrorystach, hakerach, przestępcach internetowych a także po prostu o oszustach i złodziejach.
Identyfikacja oraz właściwa ocena rangi i charakteru zagrożeń jest najbardziej skomplikowanym wyzwaniem, towarzyszącym analizie problemów teleinformatycznych.

Niektóre z nich mają bowiem charakter ściśle fizyczny – polegają na groźbie faktycznego zniszczenia materialnych narzędzi służących do przechowywania, przetwarzania lub przesyłania cyfrowej informacji.

Tego rodzaju niebezpieczeństwo może towarzyszyć choćby atakom bombowym na obiekty, w których znajdują się systemy komputerowe przechowujące i przetwarzające określone dane, ale też być wynikiem klęsk żywiołowych (powodzi, pożarów, trzęsień ziemi itp.) lub katastrof technicznych.

Większość z zagrożeń bezpieczeństwa teleinformatycznego wiąże się z działaniami prowadzonymi w cyberprzestrzeni, przy wykorzystaniu odpowiedniego sprzętu i oprogramowania.
Wówczas negatywnemu oddziaływaniu poddawana jest informacja utrwalona w elektronicznej, a nie urządzenia do przechowywania i przetwarzania.

Skutki takiej aktywności zazwyczaj nie wykraczają poza cyberprzestrzeń i objawiają się, nieprawidłową pracą systemów komputerowych.
Następstwa tego rodzaju działań mogą również przejawiać się w świecie fizycznym, np. w postaci wadliwego funkcjonowania jakiś urządzeń, których sprawność działania zależy od dopływu danych.

Pamiętać trzeba, iż poważnym problemem może być również sama niemożność skorzystania z sieci komputerowych, a tym samym z oferowanych przez nie usług.
Zagrożenie bezpieczeństwa może się dotyczyć informacji, czego przykładem jest choćby dostępna przez Internet pornografia dziecięca czy też propaganda.

Złożoność problematyki bezpieczeństwa informatycznego utrudnia znalezienie cech wspólnych wszystkim zagadnieniom.
Istotą bezpieczeństwa teleinformatycznego, bez względu na poziom jest zdolność określonego podmiotu do pozyskania i zachowania, w formie niezmienionej wszelkiego rodzaju informacji cyfrowej.

Nie można zapominać o znaczeniu powiązań między poszczególnymi poziomami bezpieczeństwa teleinformatycznego.
Bezpieczeństwo teleinformatyczne państwa zależy też od stanu zabezpieczeń komputerów i tym podobnych urządzeń znajdujących się w posiadaniu użytkowników indywidualnych.

Bezpieczeństwo danych przechowywanych lub przesyłanych przez poszczególne jednostki z wykorzystaniem ich własnego sprzętu uzależnione jest również od poziomu odporności na rozmaite groźby infrastruktury teleinformatycznej na szczeblu narodowym.

Wielowymiarowość zagadnień bezpieczeństwa teleinformatycznego oznacza też możliwość odmiennych interpretacji zarówno poszczególnych pojęć z tego zakresu, jak i samej istoty tego wymiaru bezpieczeństwa.
W rezultacie różni badacze tego zagadnienia oraz praktycy, odpowiedzialni za zapewnianie bezpieczeństwa teleinformatycznego na poszczególnych jego poziomach, pojmują przedmiot swojej pracy nieco odmiennie.

Inaczej na kwestie bezpieczeństwa teleinformatycznego spogląda bowiem zawodowy informatyk, mający za zadanie utrzymanie sprawnego funkcjonowania instytucjonalnej sieci komputerowej np. przedsiębiorstwa, a inaczej wojskowy specjalista, koncentrujący się na zapewnieniu jednostkom wojskowym nieprzerwanej łącznością.

Odmienne podejście mają też policjant, zajmujący się zwalczaniem umieszczanej w Internecie pornografii dziecięcej i innych nielegalnych oraz polityk odpowiedzialny za stabilność całego państwa.
Każda z tych osób ogranicza się z reguły do analizy i ocenie zagadnień bezpieczeństwa teleinformatycznego, co naturalne i zrozumiałe.

W tym kontekście przytoczyć można „triadę" warunków utrzymania bezpieczeństwa, tj. integralność (spójność, nienaruszona struktura i treści informacji), poufność (zabezpieczenie informacji przed nieuprawnionym dostępem) oraz dostępność (możliwości niezakłóconego dostępu uprawnionych podmiotów do informacji) z własnej perspektywy.

Z tego powodu uznaje się za priorytetowe inne problemy i wyzwania, przyjmuje inną hierarchię zadań i celów, a w konsekwencji – poszukuje innych rozwiązań.

Odmienne definicje bezpieczeństwa teleinformatycznego, pojmowany zakres tego zagadnienia oraz odpowiedzi na problemy sformułowane bez należytego uwzględnienia wszystkich możliwych implikacji, powodują, że znacznie utrudniona jest współpraca i koordynacja działań prowadzonych z myślą o poprawie stanu bezpieczeństwa teleinformatycznego.

Zdolność do efektywnej kooperacji przy przeciwdziałaniu zagrożeniom bezpieczeństwa teleinformatycznego ma niewątpliwie centralne znaczenie dla skutecznego i całościowego rozwiązywania problemów bezpieczeństwa teleinformatycznego na poziomie państwa, a w konsekwencji zapewne również pozostałych użytkowników IT.

Dlatego główną ideą przyświecającą opracowaniu tego procedur było właśnie ukazanie różnorodności perspektyw, z jakich patrzeć należy na problemy bezpieczeństwa teleinformatycznego, oraz doprowadzenie do swoistego „spotkania" tych, często bardzo odmiennych, punktów widzenia.

Powinno to bowiem umożliwić wypracowanie właściwej odpowiedzi na pojawiające się w tej sferze wyzwania.

Polityk decydujący o kształcie strategii kraju w odniesieniu do zagrożeń bezpieczeństwa narodowego w wymiarze teleinformatycznym nie może przecież oczekiwać wdrożenia rozwiązań technicznie niewykonalnych.

Natomiast informatyk dbający o stabilność nadzorowanej przez niego sieci musi pamiętać o szerszym kontekście problemu, np. konieczności pogodzenia wymogów bezpieczeństwa teleinformatycznego z innymi priorytetami państwa w dziedzinie bezpieczeństwa narodowego.

Stąd też tak ważne jest pogłębienie wśród osób zajmujących się bezpieczeństwem informatycznym świadomości różnorodności możliwych ujęć tego problemu, ułatwienie poznania specyfiki poszczególnych jego wymiarów, a także unaocznienie potrzeby łączenia rozmaitych podejść do tego zagadnienia w celu lepszego zrozumienia jego istoty i wagi.

Można tego dokonać jedynie przez rozwój dialogu ukazującego różnorodne perspektywy, z jakich należy na to zagadnienie spoglądać.

Nie będzie on zapewne prowadzić do wypracowania jednej, powszechnie obowiązującej i akceptowanej przez wszystkich definicji zakresu tej problematyki, ani też nie pozwoli ustalić niebudzącej niczyich wątpliwości hierarchii wyzwań i listy priorytetowych zadań w dziedzinie bezpieczeństwa informatycznego państwa.

https://mfiles.pl/pl/index.php/Technologia_informatyczna
Technologia informatyczna (IT, technologia informacyjna, ICT, *Information and Communication Technology*) jest bardzo szerokim pojęciem.
Kryje się pod nimi wiele dziedzin wiedzy takich jak informatyka (wszystkie jej znane działy).

Występuje tu informatyka w zarządzaniu, telekomunikacja, matematyka oraz dziedziny, w których stosuje się narzędzia i technologie związane z przetwarzaniem informacji.
IT jest zaangażowana w pozyskiwanie, gromadzenie, przetwarzanie i dystrybuowanie informacji przez sprzęty elektroniczne, takie jak komputer, telefon, radio czy telewizja.

Nowe i coraz bardziej zaawansowane techniki przekazywania informacji wkraczają w praktycznie każdą dziedzinę ludzkiego życia. Podstawowe technologie informatyczne to:
- gromadzenie danych,
- przetwarzanie danych,
- przesyłanie danych,
- magazynowanie danych,
- internetowe w biznesie.

IT to narzędzie:

- wspomagania biznesowej strategii,
- wspieranie strategicznego rozwoju,
- ukierunkowanie na wirtualizację (zarządzanie wiedzą, sieci biznesowe, interakcje z klientem).

IT jako narzędzie uzyskiwania przewagi konkurencyjnej zmierza do:

- powiększanie relacji z klientami,
- tworzenia wartości wirtualnej,
- indywidualizacji usług i produktów,
- tworzenia nowych struktur rynkowych,
- pełnienia roli organizacyjnych,
- zwiększania kapitału intelektualnego.

Natomiast IT jako narzędzie transformacji prowadzi do:

- ulepszenia koordynacji,
- przeprojektowania procesów,
- efektywniejszego wykorzystanie zasobów informacyjnych,
- poprawy współdziałania,
- poprawy procesów oraz uczenia się,
- innowacji w zakresie usług i produktów.

IT jako narzędzie organizacji i funkcjonowania systemu informacyjnego umożliwia:

- definiowanie procesów,
- kształtowanie architektury,
- zwiększenie efektywności systemu informacyjnego,
- rozwój umiejętności personelu IT,
- poprawę elastyczności systemu informacyjnego.

Obecnie najważniejsze trendy w informatyce to:

- **sztuczna inteligencja i uczenie maszynowe,**
- ***Big Data*,**
- **bioinformatyka i technologia medyczna,**
- **przetwarzanie w chmurze.**

https://networkexpert.pl/cyberbezpieczenstwo/

Rozwój techniki informatycznej wprowadził szereg udogodnień w zakresie nauki zdalnej jak i prowadzenia różnorodnych spotkań w świecie wirtualnym.

Powstało też wiele rozwiązań techniki IT, a jednym z przykładów jest zestaw do wideokonferecji (*All In One*).

Zestaw obejmuje:

- **urządzenie integrujące w sobie ekran dotykowy, kamerę wideo ze śledzeniem mówcy oraz mikrofon;**
- **dwa systemy operacyjne, tj. Windows 10 oraz Android.**

Wbudowany system Windows pozwala na wykorzystanie wszystkich aplikacji komputerowych, w tym aplikacji do obsługi wideokonferencji: Zoom, Skype, clickmeeting.

Ekran dotykowy IdeaHub służy jako tablica dotykowa.

IdeaHub występuje w dwóch wielkościach ekranu o przekątnej 65 oraz 86 cali.

System do wideokonferencji *MS Teams* lub *Webex* obejmuje:
- **zestaw głośnomówiący do telekonferencji,**
- **mikrofon do telekonferencji,**
- **telefon konferencyjny,**
- **kamery do wideokonferencji,**
- **dedykowane kamery do *MS Teams***

Wspomnieć trzeba jeszcze o telefonii IP, która jest nowoczesnym sposobem komunikacji głosowej w sieciach teleinformatycznych i dzięki której pracownicy firmy w łatwy sposób mogą się komunikować się między sobą. Telefon może być w formie tradycyjnej na biurko, aplikacji na komputer lub jako telefon komórkowy.

Firma ICT oferuje:
- **wsparcie konsultingowe i wdrożeniowe w opracowaniu bezpiecznej struktury systemów ICS/OT,**
- **opracowanie strategii podwyższenia cyberbezpieczeństwa,**
- **przegląd i wsparcie w opracowaniu polityk i procedur związanych z cyberbezpieczeństwem,**

- **opracowanie bezpiecznej architektury systemów ICS/OT uwzględniających najnowsze rozwiązania sprzętowe i programowe renomowanych dostawców,**
- **monitorowanie sieci przemysłowych,**
- **SOC (*Security Operation Center*) – świadczenie usług związanych z zorganizowaniem centrum operacyjnego.**

Oferowany jest także audyt bezpieczeństwa, który jest sprawdzeniem zabezpieczeń infrastruktury systemów teleinformatycznych.
Jest to kontrolowanie i nieinwazyjne testowanie konkretnych zasobów w infrastrukturze, tak aby sprawdzić ich podatność na dane zagrożenia.

Ataki wykonywane są przez certyfikowanego specjalistę od cyberbezpieczeństwa.
Audyt zakończony jest raportem na podstawie którego, dzięki dokładnym wskazówkom, można rozpocząć wdrażanie zmian w zakresie cyberbezpieczeństwa.

Przeprowadzenie audytów pod kątem zgodności z wymogami standardów występujących w środowiskach przemysłowych (np. IEC 62443 /wybrane sekcje/, ISO 27001, wymagania KSC, specyficzne standardy kolejowe i motoryzacyjne).
Przeprowadzenie audytu zasobów teleinformatycznych pozwala na proaktywne wykrywanie zagrożeń.

Atak na zasoby teleinfromatyczne danej firmy/organizacji składa się z wielu kroków, przygotowań.

Cyberprzestępcy pozostawiają ślady swojej działalności zanim wykonają atak – nie spodziewają się, że również mogą być obserwowani.

Wcześnie wykryte zdarzenia związane z przygotowaniem ataku mogą mu zapobiec.
Co więcej część ataków, np. kradzież danych jest przeprowadzana w sposób przezroczysty dla użytkownika.
Bez audytu podatności systemów nigdy nie można się zorientować jak cenne informacje (np. handlowe, patentowe, tajne dane) firma mogła by utracić.

Audyt:
- **zwiększa świadomość istniejących zagrożeń,**
- **pozwala dostosować zabezpieczenia zanim dojdzie do niebezpiecznej sytuacji,**
- **pozwala lepiej zarządzać podatnościami,**

- **pozwala dostosować się organizacji do zgodności z normami i regulacjami GDPR RODO, ISO 27000 (konieczność ochrony danych – adekwatny do oszacowanego ryzyka),**
- **wskazuje na ujawniania informacji o incydentach bezpieczeństwa oraz udowodnienia, że zrobiło się wszystko, aby do takich incydentów nie dopuścić.**

Dzięki audytowi następuje:
- **wsparcie w opracowaniu bezpiecznej struktury systemów ICS/OT,**
- **opracowanie strategii podwyższenia cyberbezpieczeństwa,**
- **przegląd i wsparcie w opracowaniu polityk i procedur,**
- **opracowanie bezpiecznej architektury systemów ICS/OT,**
- **monitorowanie sieci przemysłowych.**

https://pl.wikipedia.org/wiki/Bezpiecze%C5%84stwo_teleinformatyczne

Bezpieczeństwo teleinformatyczne to zbiór zagadnień z dziedziny telekomunikacji i informatyki związany z szacowaniem i kontrolą ryzyka wynikającego z korzystania z komputerów, sieci komputerowych i przesyłania danych do zdalnych lokalizacji, rozpatrywany z perspektywy poufności, integralności i dostępności.

Budowanie bezpiecznych systemów teleinformatycznych i aplikacji jest celem starań projektantów sieciowych i programistów.
Konieczne jest opracowanie metod oceny bezpieczeństwa i kontrolowania zagrożeń. Mimo tych starań, ze względu na złożoność i czasochłonność wielu spośród proponowanych procesów, luki zabezpieczeń stanowią jednak poważny i wymierny problem dla użytkowników sieci teleinformatycznych.

https://ccit.pl/bezpieczenstwo-informacji/

Cyberbezpieczeństwo dotyczy zabezpieczenia gromadzonych, przetwarzanych i udostępnianych informacji w formie elektronicznej przy użyciu wszelkich technik cyfrowych i wszelkich dostępnych narzędzi komunikacji elektronicznej.

Polega na zapewnieniu bezpieczeństwa systemów IT przedsiębiorstw w zakresie:
- **danych;**
- **aplikacji i programów (systemy IT);**
- **systemów sieciowych IT;**
- **infrastruktury IT (komputery, serwery, sieć IT, komputery przemysłowe, smartfony);**
- **osób mających dostęp do elementów systemów teleinformatycznych przedsiębiorstwa.**

https://twojepc.pl/news42344/Jak-zadbac-o-bezpieczenstwo-teleinformatyczne-w-firmie.html
Bezpieczeństwo teleinformatyczne nazywane również cyberbezpieczeństwem (cybersecurity) to zagadnienia związane z telekomunikacją oraz informatyką, które odnoszą się do ryzyk związanych z użytkowaniem komputerów, sieci komputerowych, czy Internetu.

Dbając o bezpieczeństwo teleinformatyczne nie tylko chronimy gromadzone i przetwarzane dane, ale również zapewniamy bezpieczeństwo i ciągłość procesów biznesowych wykonywanych w firmie.

Na cyberbezpieczeństwo należy patrzeć z perspektywy zapewnienia poufności, integralności oraz ograniczonej dostępności.

(https://mindworkers.pl/bezpieczenstwo-teleinformatyczne-cybersecurity-czym-jest-oraz-jakie-sa-najwieksze-zagrozenia-w-2021-roku-dla-twojego-przedsiebiorstwa/).

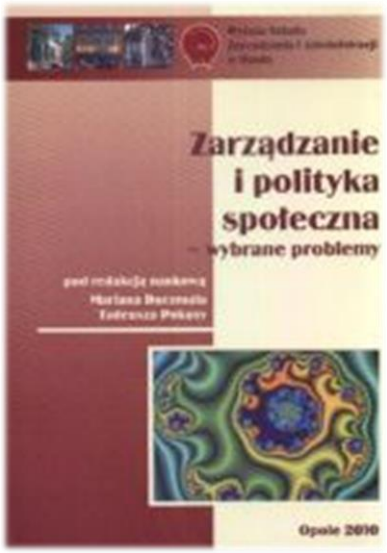
11. Moje wcześniejsze publikacje w latach 2008-2023

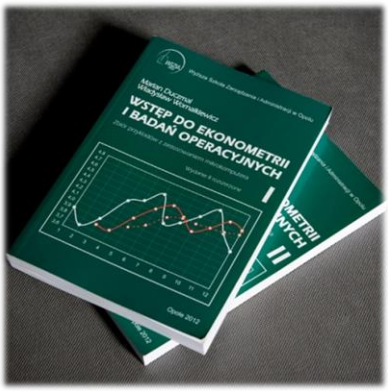
Coraz częściej spotykam się z dużym zainteresowaniem internautów moimi publikacjami i wpisami, a świadczy o tym tygodniowa statystyka w *WordPress* na blogu: *https://wornalkiewicz.wordpress.com/* (zob. rysunek 11.1).

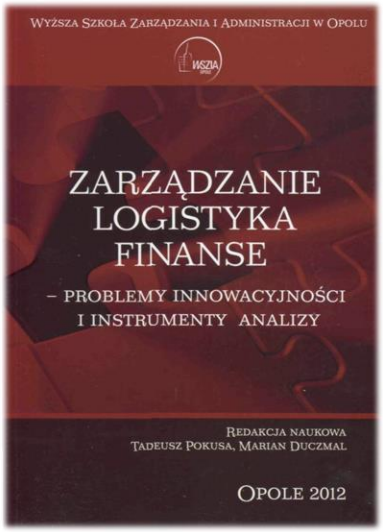
Źródło: Opracowanie własne na podstawie blogu „*Procesy informacyjne w teorii i praktyce*”.

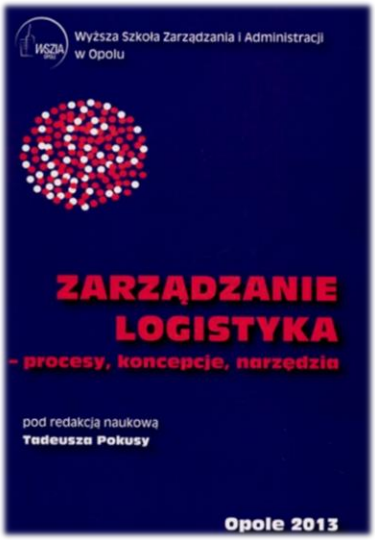
Rys. 11.1. Statystyka w układzie tygodni na blogu moim blogu

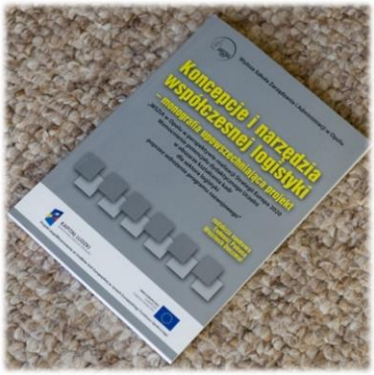
Oprócz tego forum, współpracy z sympatykami metod ilościowych w domenie „*Google*” w Internecie, znajdują się pozycje ze zmiankami o moim dorobku naukowym na stronie WWW Akademii Nauk Stosowanych WSZiA w Opolu. Dalej zostaną zaprezentowane wybrane z tej strony moje pozycje publikacji zarówno jako książki, monografie indywidualne oraz artykuły w monografiach zbiorowych. Zaprezentowane zostaną publikacje sygnalizowane w domenie Google po wywołaniu autora „*Władysław Wornalkiewicz*”. Całość opracowano w układzie kolejności narastającej lat (2008-2023).

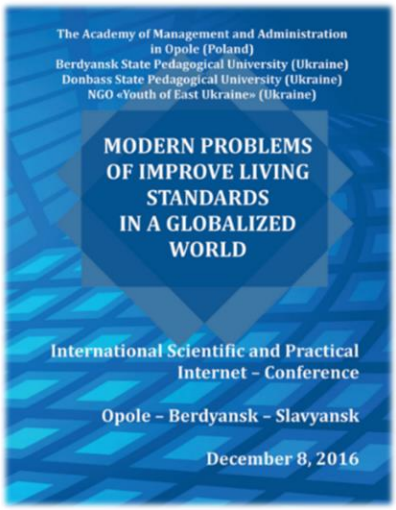
2008	
1. „*Ekonomiczno-społeczne problemy współczesnego zarządzania i komunikacji*”, monografia zbiorowa recenzowana, Opole: Wydawnictwo Instytut Śląski, 2008, 255 s., artykuł „*Dobór metod i parametrów w budowaniu modeli ekonometrycznych*”, strony: 190-204, ISBN 978-83-88980-69-5, 978-83-7511-098-2. Link: https://wordpress.com/media/wornalkiewicz.wordpress.com.	
2010	
1. „*Wstęp do ekonometrii i badań operacyjnych Zbiór przykładów z zastosowaniem mikrokomputera*”, monografia zbiorowa recenzowana (podręcznik akademicki), współautorstwo - Marian Duczmal, Opole: Wydawnictwo Instytut Śląski, 2010, 597 s., ISBN 978-8388980-94-7, 978-83-62105-41-0. Link: https://www.wszia.opole.pl/wp-con-tent/uploads/2020/05/Wstep_do_ekonometrii_i_badan_operacyjnych.pdf.	
2. „*Zarządzanie i polityka społeczna - wybrane problemy*”, monografia zbiorowa recenzowana, Opole: Wydawnictwo Instytut Śląski, 2010, 443 s., artykuł „*Estymacja modeli wielorównaniowych w GRETL*” strony: 255-276, ISBN 978-83-88980-90-9, 978-83-62105-23-6. Link: https://wordpress.com/media/wornalkiewicz.wordpress.com.	

3. „*Nowoczesne zarządzanie - wybrane problemy ekonomiczno-społeczne*”, monografia zbiorowa recenzowana, Opole: Wydawnictwo Instytut Śląski, 2010, 242 s., artykuł: „*Propozycja określenia efektywności województw*”, strony: 189-208, ISBN 978-83-88980-98-5, 978-83-62105-53-3. Link: https://integro.bg.polsl.pl/172200374055/ksiazka/nowoczesne-zarzadzanie-wybrane-problemy-ekonomiczno-spoleczne?bibFilter=17.	
2011	
1. „*Przejawy wielowymiarowości współczesnego zarządzania - formy i instrumenty ekonomiczno-społeczne*”, monografia zbiorowa recenzowana, Opole: Wydawnictwo Instytut Śląski, 2011, 394 s., artykuł: „*Model ekonometryczny zmiennej „liczba bezrobotnych*””, strony: 172-186, ISBN 978-83-62683-20-8, 978 -83-7511-135-4. Link: https://wordpress.com/media/wornalkiewicz.wordpress.com.	
2012	
1. „*Wstęp do ekonometrii i badań operacyjnych Zbiór przykładów z zastosowaniem mikrokomputera*”, wydanie II rozszerzone, część I, monografia zbiorowa recenzowana (podręcznik akademicki), współautorstwo - Marian Duczmal, Opole: Wydawnictwo Instytut Śląski, 2012, 411 s., ISBN 978-83-62683-30-7, 978-83-7511-259-0. 2. „*Wstęp do ekonometrii i badań operacyjnych Zbiór przykładów z zastosowaniem mikrokomputera*”, wydanie II rozszerzone, część II, monografia zbiorowa recenzowana (podręcznik akademicki), współautorstwo - Marian Duczmal, Opole: Wydawnictwo Instytut Śląski, 2012, 223 s., ISBN 978-83-62683-30-7, 978-83-7511-259-0.	

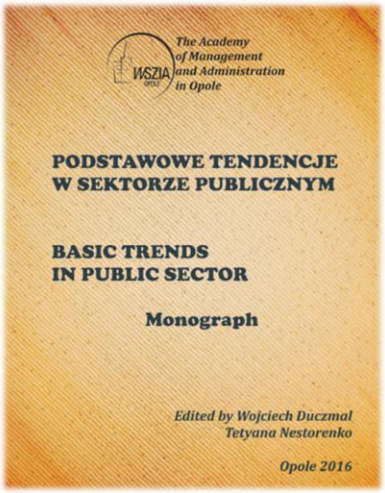
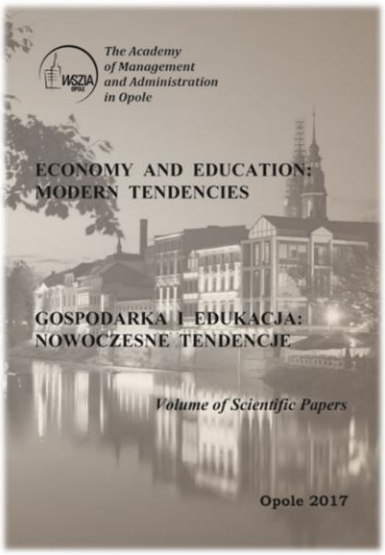
3. „*Zarządzanie Logistyka Finanse - Problemy innowacyjności i instrumenty analizy*”, monografia zbiorowa recenzowana, Opole: Wyższa Szkoła Zarządzania i Administracji w Opolu, 2012, … s., artykuły: „*Model wielorównaniowy PKB*”, strony: 223-249, „Etapy i procedury budowy modelu produktu brutto podregionów”, strony: 261-279, ISBN Link: https://w.bibliotece.pl/1798765/Zarz%C4%85dzanie+logistyka+finanse.	
2013	
1. „*Metoda badania przyczynowo-skutkowego związków między cechami statystycznymi*”, skrypt nr 1/2013 - pomocniczy do przedmiotu Ekonometria, Opole: Wyższa Szkoła Zarządzania i Administracji w Opolu, 2013, 252 s., ISBN 978-83-62683-44-4, 978-83-7511-187-3. Link: https://wordpress.com/media/wornalkiewicz.wordpress.com; https://books.google.pl/books/about/Metoda_badania_przyczynowo_skutkowego_zw.html?id=0d0DoQEACAAJ&redir_esc=y.	
2. „*Modele ekonometryczne PKB obiektów struktury terytorialnej*”, monografia indywidualna recenzowana, Opole: Wydawnictwo Instytut Śląski, 2013, 343 s., ISBN 978-83-62683-36-9, 978-83-7511-170-5. Link: https://integro.bs.katowice.pl/32403087968/wornalkiewicz-wladyslaw/modele-ekonometryczne-pkb-obiektow-struktury-terytorialnej.	

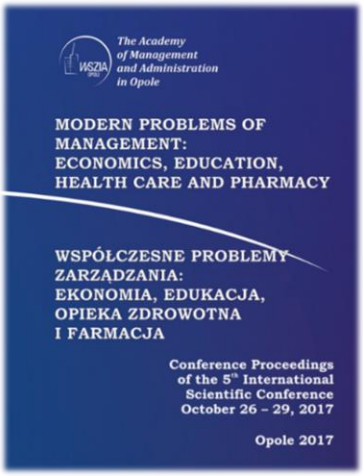
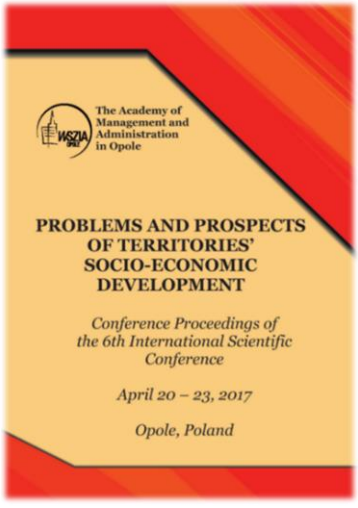
3. „*Zarządzanie Logistyka - procesy, koncepcje, narzędzia*”, monografia zbiorowa recenzowana, Opole: Wydawnictwo Instytut Śląski, 2013, 304 s., , artykuł „*Programowanie wielokryterialne z zastosowaniem WinQSB*”, strony: 168-184, ISBN 978-83-62683-49-9, 978-83-7511-192-7. Link: https://integro.ciniba.edu.pl/integro/192504222555/ksika/zarzdzanielogistykakoncepcjeprocesynarzdzia.	
4. „*Społeczno-ekonomiczne uwarunkowania zarządzania i administracji - innowacyjność, komunikacja*”, monografia zbiorowa recenzowana, Opole: Wydawnictwo Instytut Śląski, 2013, 251 s., artykuł „*Wybór lokalizacji obiektu z zastosowaniem Expert Choice*”, strony: 124-140, ISBN 978-83-62683-53-6, 978-83-7511-103-4. Link: https://wordpress.com/media/wornalkiewicz.wordpress.com.	
2014	
1. „*Formułowanie modeli ekonometrycznych na potrzeby zarządzania”* cz. I, monografia indywidualna recenzowana (podręcznik akademicki), Opole: Wydawnictwo Instytut Śląski, 2014, 665 s., ISBN 978-83-62683-64-2, 978-83-7511-210-8. 2. „*Formułowanie modeli ekonometrycznych na potrzeby zarządzania”* cz. II, monografia indywidualna recenzowana (podręcznik akademicki), Opole: Wydawnictwo Instytut Śląski, 2015, 665 s., ISBN 978-83-62683-64-2, 978-83-7511-210-8. Link: https://integro.bg.polsl.pl/172600881896/wornalkiewicz-wladyslaw/formulowanie-modeli-ekonometrycznych-na-potrzeby-zarzadzania.	

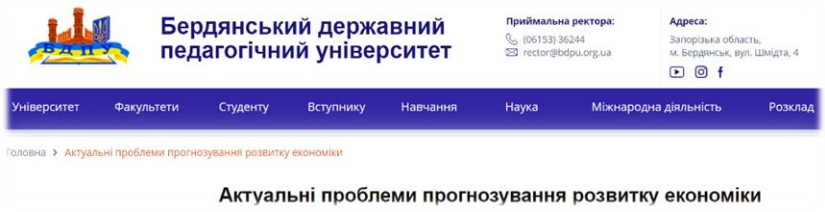
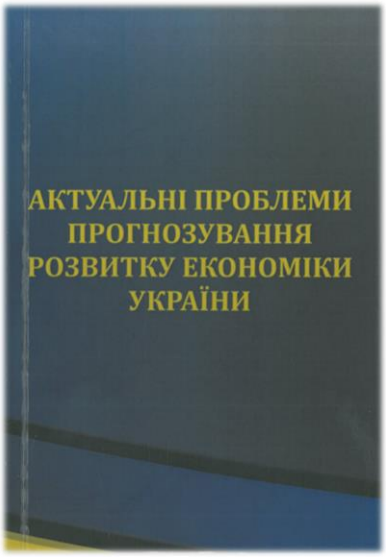
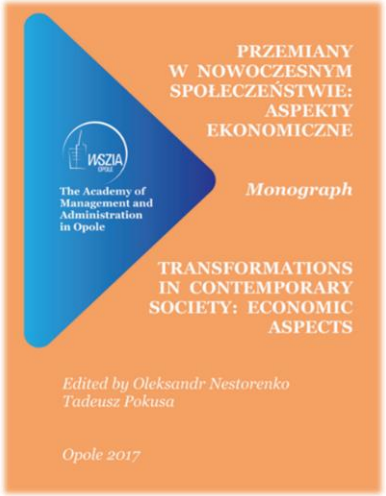
2015	
1. „*Wdrożenie zintegrowanego systemu informatycznego wspomagającego zarządzanie*”, monografia indywidualna recenzowana (podręcznik akademicki), Opole: Wydawnictwo Instytut Śląski, 2015, 370 s., ISBN 978-83-62683-67-3, 978-83-7511-226-9. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/05/Wornalkiewicz_Wdrozenie_zintegrowanego_systemu_informatycznego.pdf.	
2. „*Ekonomiczno-społeczne uwarunkowania rozwoju gospodarczego - zarządzanie informacją i nowymi technologiami*”, monografia zbiorowa recenzowana, Opole: *Wydawnictwo „Instytut Śląski”,* 2015, 507 s., artykuły i strony: *„Przejawy wdrożenia systemów informatycznych*” (85-108), „*Modelowanie procesów zarządzania*” (124-146), współautorstwo: Ryszard Broszkiewicz, „*EDI w procesie logistycznym*” (278-301), „*Analityka biznesowa*” (356-375). Link: https://www.wszia.opole.pl/wp-content/uploads/2020/05/2_2021.pdf.	
3. *„Koncepcje i narzędzia współczesnej logistyki - monografia upowszechniająca projekt „WSZiA w Opolu w perspektywie realizacji Strategii Europa 2020 Wzmocnienie potencjału dydaktycznego Uczelni w obszarze kształcenia kadr dla sektora logistyki poprzez wdrożenie programu rozwojowego””,* praca zbiorowa, Opole: Wydawnictwo Instytut Śląski, 102 s., artykuł „*Implementacja systemów klasy ERP w logistyce*”, ISBN 978-83-62683-75-8, 978-83-7511-235-1. Link: https://wordpress.com/media/wornalkiewicz.wordpress.com.	

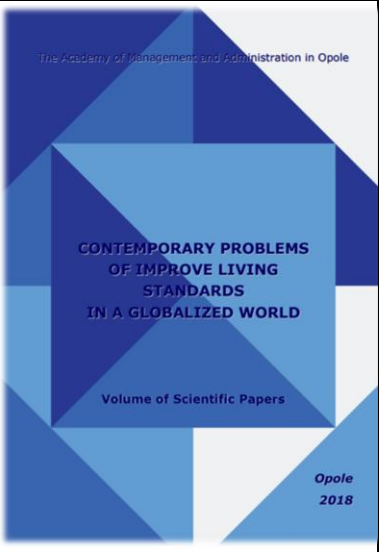
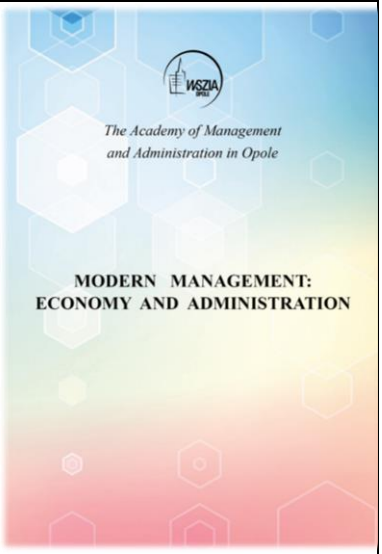
2016	
1. „*Wprowadzenie do projektowanie systemów informatycznych zarządzania*” Część 1, monografia indywidualna recenzowana (podręcznik), Opole: Wydawnictwo Wyższej Szkoły Zarządzania i Administracji w Opolu, 2016, 328 s., ISBN 978-83-62683-97-0, 978-83-7511-243-6. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/05/Projektowanie_systemow_informatycznych_zarzadzania.pdf. 2. „*Wprowadzenie do projektowania systemów informatycznych zarządzania*” część 2, monografia indywidualna recenzowana (podręcznik), Opole: Wydawnictwo Wyższej Szkoły Zarządzania i Administracji w Opolu, 2016, 567 s., ISBN 978-83-62683-97-0, 978-83-7511-243-6. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/05/Wprowadzenie_do_projektowania_Czesc2.pdf.	
3. „*Conference Proceedings of the International Scientific Internet-Conference Modern Problems of Improve Living Standards in a Globalized World*”, materiały pokonferencyjne - monografia zbiorowa recenzowana, Opole - Berdyansk - Slavyansk), 2016, (electronic edition), 534 s., artykuł „*Rozwiązanie problemu transportowego metodą VAM*” (22-28), ISBN 978-83-62683-871. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2016_modern_problems_of_imrpve_living_standards_in_a_globalized_world_slavyansk.pdf.	

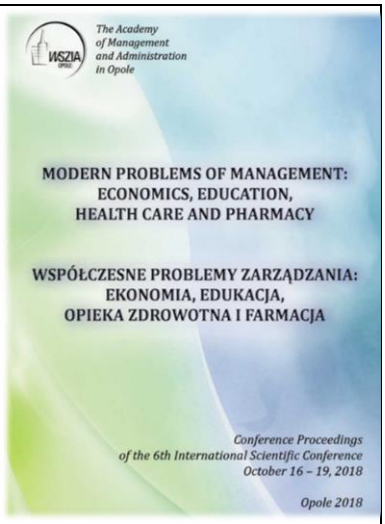
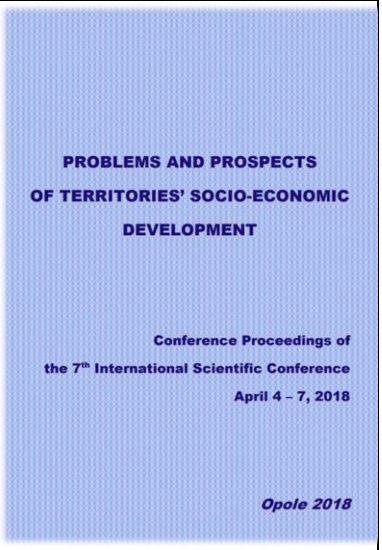
4. „*Social and Economic Priorities in the Context of Sustainable Development*”, monografia zbiorowa recenzowana, Opole: The Academy of Management and Administration in Opole, 2016, 444 s., artykuł „*Product promotion and company image in Internet*” (*Promocja produktu i wizerunku firmy w Internecie*), strony: 138-148, , ISBN 978 - 83 - 62683 -78 - 9. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2016_priorytet_spoleczno_gospodarcze_w_kontekscie_zrownowazonego_rozwoju.pdf.	
5. „*20 lat Wyższa Szkoła Zarządzania i Administracji w Opolu - interdyscyplinarność badań*”, monografia zbiorowa recenzowana jubileuszowa, Opole: Wydawnictwo Instytut Śląski, 2016, 375 s., artykuł: „*Wyszukiwarki i media społecznościowe*”, strony: 320-333, ISBN 978-83-62683-86-4, 978-83-7511-247-4. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2016_wyzsza_szkola_zarzadzania_i_administracji_w_opolu_interdyscyplinarnosc_badan.pdf.	
6. „Соціально-економічний розвиток: роль інформації та нових технологій”, monografia zbiorowa recenzowana, Бердянський державний педагогічний університет, 2016, 295 s., artykuł „*Symulacja biznesowa*”, strony: 197-208, ISBN 978-617-7291-44-1. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2016_%D0%9E%D0%A6%D0%86%D0%90%D0%9B%D0%AC%D0%9D%D0%9E_%D0%95%D0%9A%D0%9E%D0%9D%D0%9E%D0%9C%D0%86%D0%A7%D0%9D%D0%98%D0%99.pdf.	

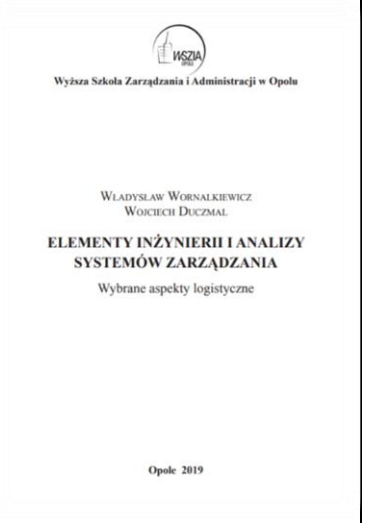
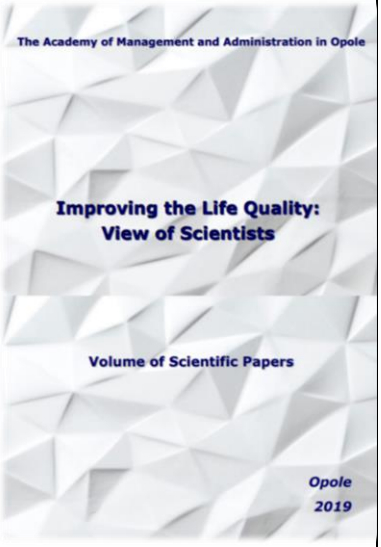
7. „*Освіта і суспільство. Міжнародний збірник наукових праць*”, Бердянський державний педагогічний університет, 2016, 418 s., artykuł *„Ranking metod ilościowych w Internecie*”, strony: 275-285, ISBN 978-617-7291-80-9 (електронне видання). Link: https://bdpu.org.ua/wp-content/uploads/2019/10/Papers_Berdyansk_2016.pdf.	
8. „*Basic Trends in Public Sector*” („*Podstawowe tendencje w sektorze publicznym*”), monografia zbiorowa recenzowana, artykuł: *Designing of managerial consoles* (*Projektowanie pulpitów menadżerskich*), strony: 58-74. Opole: The Academy of Management and Administration in Opole, 2016, 200 s., ISBN 978-83-62683-79-6. Link: https://www.wszia.opole.pl/wp-con-tent/uploads/2020/09/2016_podstawowe_tendencje_w_sektorze_publicznym_duczmal_nestoreka-1.pdf.	
2017	
1. „*Economy And Education: Modern Tendencies*” - *Gospodarka I Edukacja: Nowoczesne Tendencje*, Volume of Scientific Papers, monografia zbiorowa recenzowana, Wyższa Szkoła Zarządzania i Administracji w Opolu, 2017, 362 s., artykuł „*Prognozowanie z wykorzystaniem zasady postarzania informacji*”, strony: 39-43, ISBN 978 - 83 - 62683 - 24 - 6. Link: https://www.wszia.opole.pl/wp-con-tent/uploads/2020/09/2017_economy_andeducation_modern_tendencies.pdf.	

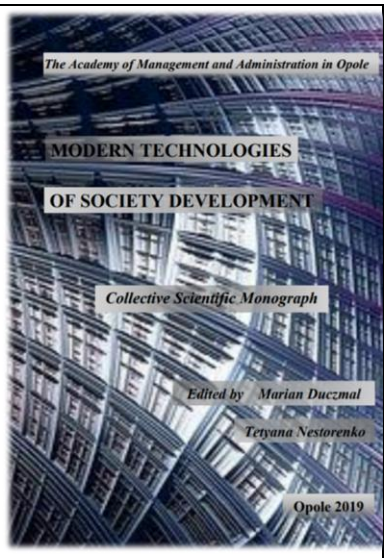
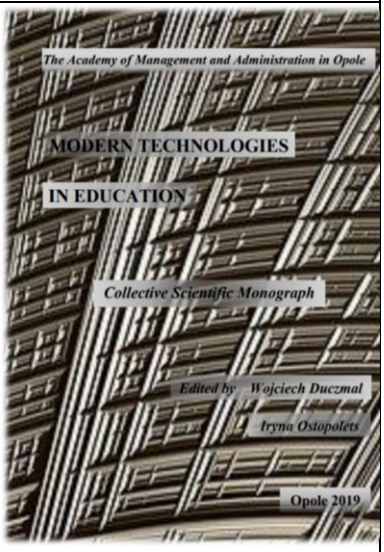
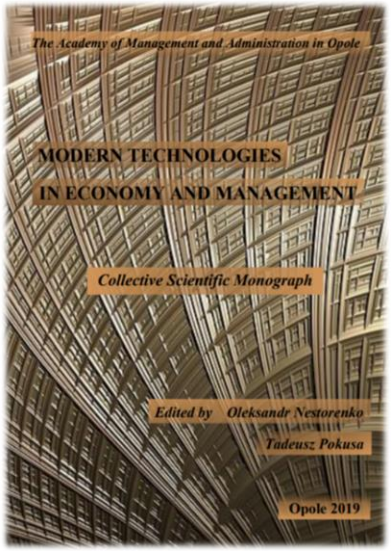
2. „*Modern Problems of Management: Economics, Education, Health Care and Pharmacy*”, Conference Proceedings of the 5 th International Scientific Conference, 232 s., Opole, The Academy of Management and Administration in Opole, 2017, artykuł „*Zastosowanie konwertera plików*”, strony: 25-27, 978-83-62683-23-9. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2017_modern_problems_of_management_econimics_education_health_care_and_pharmacy.pdf.	
3. „*Popularyzacja wybranych metod ilościowych w Internecie*”, monografia indywidualna, Wyższa Szkoła Zarządzania i administracji w Opolu, Opole, 2017, 351 s. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2017_popularyzacja_wybranych_metod_ilosciowych_w_interneice_wornalkiewicz.pdf.	
4. „*Problems and Prospects of Territories’ Socio-Economic Development*”, Conference Proceedings of the 6 th International Scientific Conference, materiały pokonferencyjne, monografia zbiorowa recenzowana, The Academy of Management and Administration in Opole, 2017, 272 s., artykuł: „*Optymalizacja marszrutyzacji przewozów z zastosowaniem funkcji Excela*”, strony: 41-43, ISBN 978-83-62683-10-9. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2017_problems_and_prodprcts_pf_territories_socio_economic_development.pdf.	

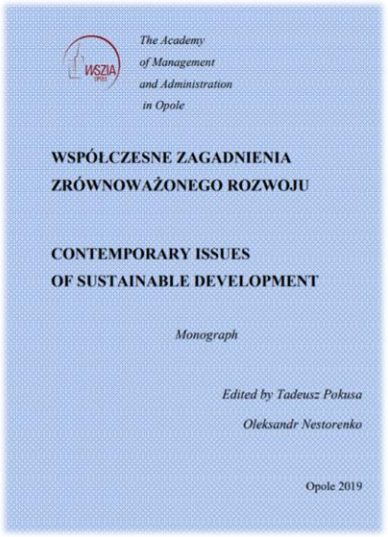
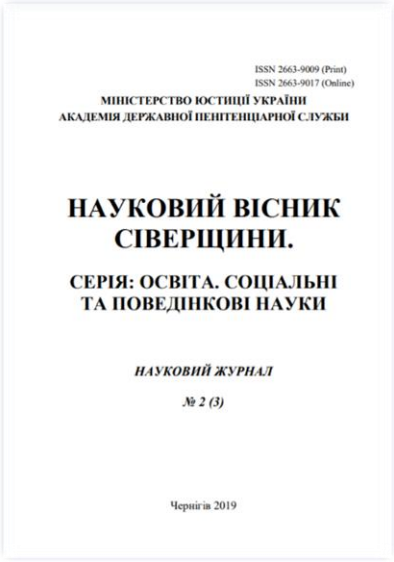
5. „*Актуальні проблеми прогнозування розвитку економіки…*” („*Bieżące problemy prognozowania ekonomiki Ukrainy*”), zbiór prac naukowych - monografia zbiorowa recenzowana, 370 s., КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА (Kijowski Narodowy Uniwersytet im. Tarasa Szewczenki) i inne, 2017, „*Optymalizacja przewozów z zastosowaniem funkcji Excela*” strony: 154-169, ISBN 978-617-7291-98-4. Link: https://bdpu.org.ua/actual-problems-of-forecasting-economic-development/.  	
6. „*Transformations in contemporary society: economic aspects*” (*Przemiany w nowoczesnym społeczeństwie: aspekty ekonomiczne*”, monografia zbiorowa recenzowana, Wyższa Szkoła Zarządzania i Administracji w Opolu, 2017, 348 s., artykuł: „*Forecasting using the multiplicative model*” („*Prognozowanie z zastosowaniem modelu multiplikatywnego*”), strony: 205-212, ISBN 978-83-62683-96-3. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2017_przemiany_w_nowoczesym_spoleczenstwie_aspekty_ekonomiczne_nosferanko_pokusa.pdf.	

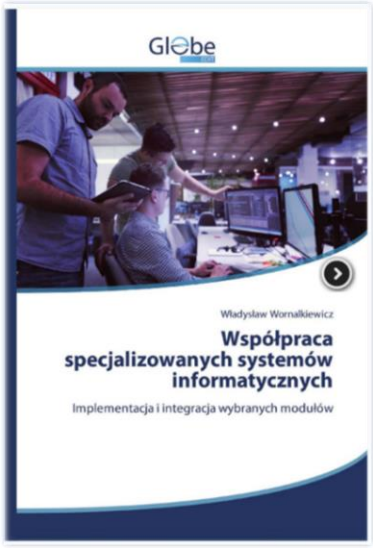
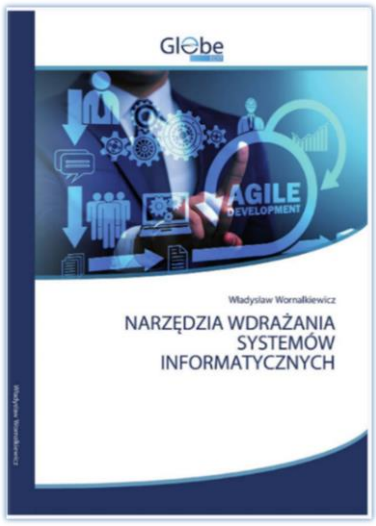
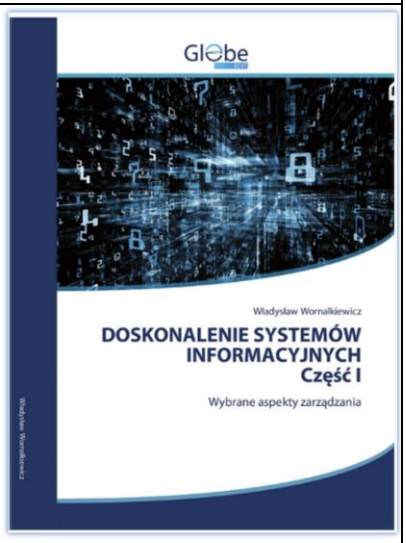
2018	
1. „*Contemporary Problems of Improve Living Standards in a Globalized World*”, Volume of Scientific Papers, monografia zbiorowa recenzowana, The Academy of Management and Administration in Opole, Opole, 2018, electronic edition, 770 s., artykuł „*Echa migracji w wybranej literaturze* (*Stosowane metody i modele*)”, strony: 516-527, ISBN 978-83-946765-1-3. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2018_contemporary_problems_of_improwve_living_in_a_globalized_world.pdf.	
2. „*Modern Management: Economy and Administration*” (*Nowoczesne Zarządzanie: Ekonomia i Administracja*), monografia zbiorowa recenzowana, The Academy of Management and Administration in Opole, Opole, 2018, 218 s., artykuł ”*Applications used in designing websites*” (*Aplikacje stosowane w projektowaniu stron www*) , strony: 154-160, ISBN 978-83-62-683-27-7. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2018_modern_management_economy_and_administration.pdf.	

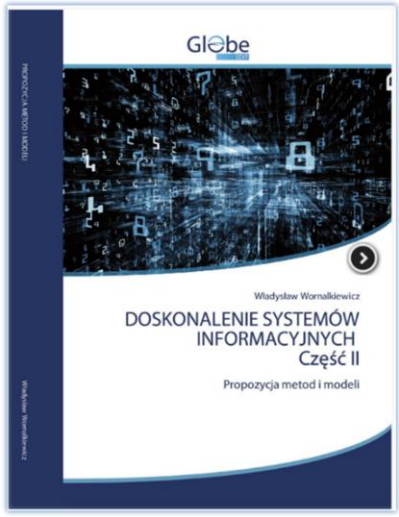
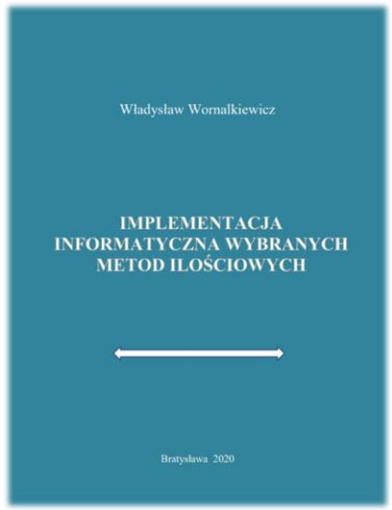
3. „*Modern Problems of Management: Economics, Education, Health Care and Pharmacy*” (*Współczesne problemy zarządzania: Ekonomia, edukacja, opieka zdrowotna i farmacja*), Conference Proceedings of the 6th International Scientific Conference, Opole, The Academy of Management and Administration in Opole, 2018, 116 s., artykuł „*Potrzeba utworzenia piramidy wskaźników procesów ludnościowych*”, strony: 22-25, ISBN 978-83-946765-1-3. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2018_modern_problems_of_management_economics_education_health_nad_pharmcy.pdf.	
4. „*Problems and Prospects of Territories' Socio-Economic Development*” Conference Proceedings of the 7 th International Scientific Conference, Opole, materiały pokonferencyjne, monografia zbiorowa recenzowana, The Academy of Management and Administration in Opole, 2018, 345 s., artykuł „*Ocena nieefektywności gospodarowania zasobami ludności*”, strony: 70-72, ISBN 978 - 83 - 62683 - 25 - 3. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2018_problems_andprospects_of_territories_socio_economic_development.pdf.	
5. „*Uwarunkowania demograficzne rozwoju społecznego i ekonomicznego miasta Nysa i powiatu nyskiego*”, Opole-Nysa, Wyższa Szkoła Zarzadzania i Administracji w Opolu, 2018, 260 s., artykuł: „*Prognozowanie migracji ludności z uwzględnieniem wag harmonicznych*”, strony: 212-233, ISBN 978-83-946765-0-6.	

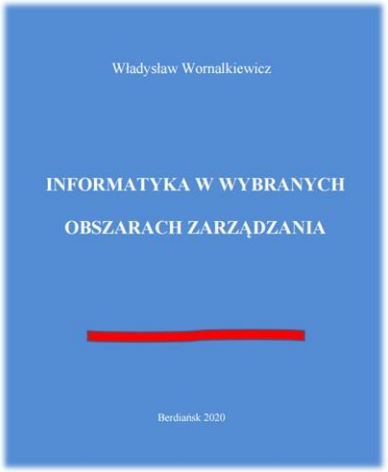
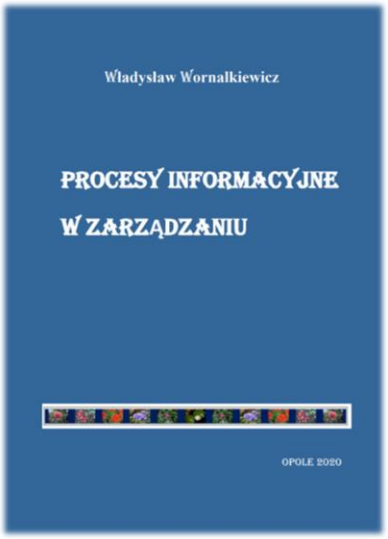
2019	
1. „*Elementy inżynierii i analizy danych systemów zarządzania Wybrane aspekty logistyczne*”, monografia zbiorowa recenzowana (podręcznik akademicki), współautorstwo - Wojciech Duczmal, Opole, Wydawnictwo Wyższej Szkoły Zarządzania i Administracji w Opolu, 2019, 341 s., ISBN 978-83-946765-8-2. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/05/Elementy_inzynierii_i_analizy_systemow_zarzadzania.pdf.	
2. „*Improving the Life Quality: View of Scientists*”, Volume of Scientific Papers, monografia zbiorowa recenzowana, The Academy of Management and Administration in Opole, Opole, 2019, electronic edition, 660 s., artykuły: „*Pozyskiwanie danych o odległościach dla potrzeb zagadnienia transportowego*” strony: 118-136, „*Prognozowanie zewnętrznych usług transportowych*” strony: 137-156, „*Zastosowanie taksonomii wrocławskiej*” (157-188), ISBN 978-83- 946765-3-7. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2019_improving_the_life_quality_view_of_scientists.pdf.	

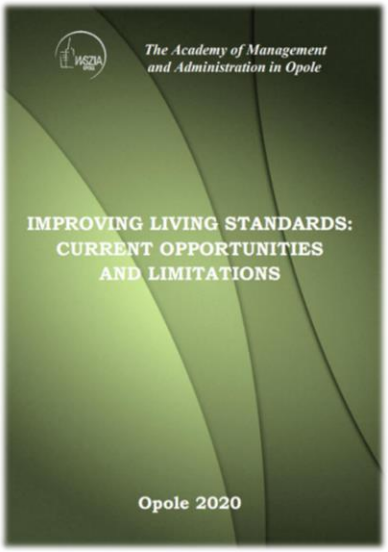
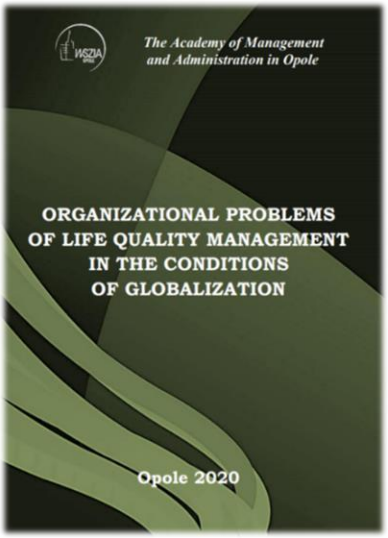
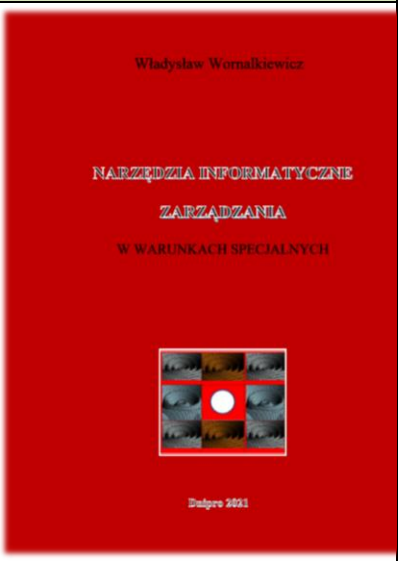
3 „*Modern Technologies of Society Development*”, Collective Scientific Monograph, monografia zbiorowa recenzowana, Opole: The Academy of Management and Administration in Opole, 2019, 410 s., artykuł: „*Verification of the research when comparing in pairs*” (*Weryfikacja badania przy porównywaniu parami*), strony: 119-129, ISBN 978- 83-946765-6-8. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2019_modern_technologies_in_education.pdf.	
4. „*Modern Technologies in Education*”, Collective Scientific Monograph, monografia zbiorowa recenzowana, Opole: The Academy of Management and Administration in Opole, 2019, 495 s., artykuł: „*Converting PDF to DOC*” (*Konwersja pliku formatu PDF na DOC*), strony: 184-194, ISBN 978-83-946765-5-1. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2019_modern_technologies_in_education_dauczan.pdf.	
5. „*Modern Technologies in Economy and Management*”, Collective Scientific Monograph, monografia zbiorowa recenzowana, Opole: The Academy of Management and Administration in Opole, 2019, 493 s., artykuł: „*Mortality modeling*” (*Modelowanie umieralności*), strony: 148-160, ISBN 978-83-946765-4-4. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2019_moderntechnologies_in_ecenomy_and_managment.pdf.	

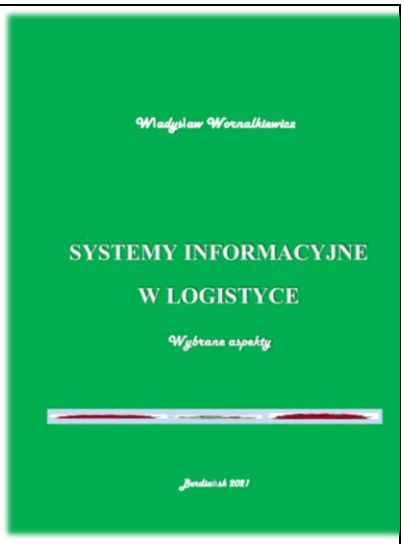
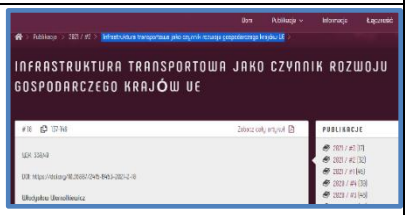
6. „*Contemporary issues of sustainable development*”, monografia zbiorowa recenzowana, Opole: The Academy of Management and Administration in Opole, 2019, 452 s., artykuł: „*Technology of optimization solutions in decision-making task*” (*Techniki rozwiązań optymalizacyjnych zadania decyzyjnego*), strony: 63-82, ISBN 978 - 83 - 946765 - 7 - 5. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2019_wspolczesne_zagadnienia_zrownowazonego_rozwoju.pdf.	
7. „*Наука ІІІ тисячоліття: пошуки, проблеми*”, перспективи розвитку, 2019, Збірник тез, Бердянський державний педагогічний університет, Рада молодих учених, 291 s., artykuł „*Conversion of Audio File to Text File*” (*Konwersja pliku audio na tekstowy*), strony: 199-200, УДК 378:001. (063) Н 34. Link: https://bdpu.org.ua/wp-content/uploads/2019/02/zbirnyk.pdf	
8. „*Науковий вісник Сіверщини. Серія: Освіта*”, Соціальні та поведінкові науки: науковий журнал / Академія Державної пенітенціарної служби”. Чернігів: Академія ДПтС, 2019. № 2 (3). 208 с. artykuł „*Przyszłość → magistrala drogowa Hamburg-Szanghaj*”, strony: 178-207, ISSN 2663-9009 (Print), ISSN 2663-9017 (Online).	
Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2019_%D0%9D%D0%90%D0%A3%D0%9A%D0%9E%D0%92%D0%98%D0%99_%D0%92%D0%86%D0%A1%D0%9D%D0%98%D0%9A.pdf.	

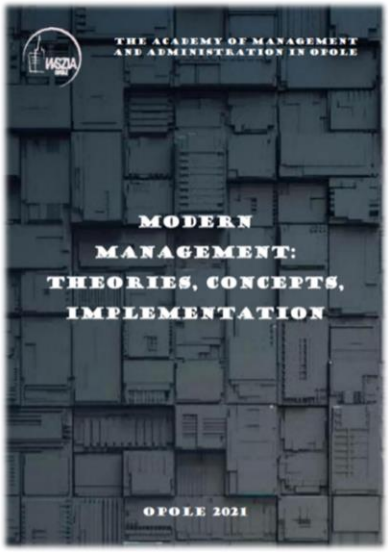
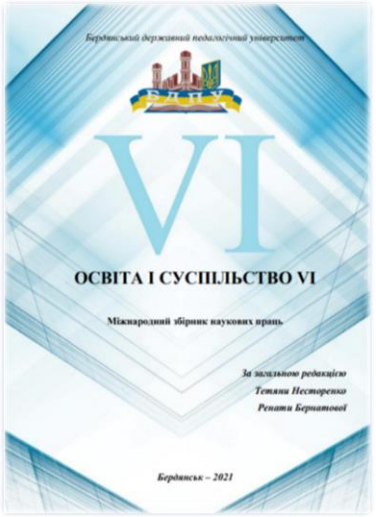
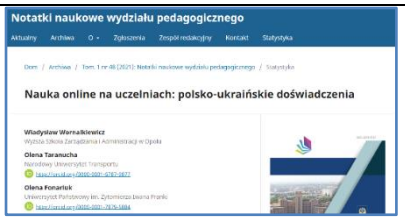
9. „*Współpraca specjalizowanych systemów informatycznych Implementacja i integracja wybranych modułów*”, monografia indywidualna, wydawca: GlobeEdit (International Book Market Service Ltd. , Member of OmniScriptum Publishing Group), Republic of Moldova, druk: Printforce - United Kingdom, 2019, 52 s., ISBN 978-613-42041-4. Link: https://www.morebooks.de/store/gb/book/wsp%C3%B3%C5%82praca-specjalizowanych-system%C3%B3w-informatycznych/isbn/978-613-9-42041-4.	
2020	
1. *„Narzędzia wdrażania systemów informatycznych”*, monografia indywidualna, wydawca: GlobeEdit (International Book Market Service Ltd. , Member of OmniScriptum Publishing Group), Republic of Moldova, druk: Printforce - United Kingdom, 2020, 140 s., ISBN 978-620-0-61025-6. Link: https://www.morebooks.de/gb/p_978-620-0-61025-6; https://www.globeedit.com; https://www.morebooks.de/store/gb/book/narz%C4%99dzia-wdra%C5%BCania-system%C3%B3w-informatycznych/isbn/978-620-0-61025-6.	
2. „*Doskonalenie systemów informacyjnych*” Część I „*Wybrane aspekty zarządzania*”, monografia indywidualna, wydawca: GlobeEdit (International Book Market Service Ltd. , Member of OmniScriptum Publishing Group), Republic of Moldova, druk: Printforce - United Kingdom, 2020, 388 s., ISBN 978-620-0-59233-0. Link: https://www.morebooks.de/store/gb/book/doskonalenie-system%C3%B3w-informacyjnych-cz%C4%99%C5%9B%C4%87-i/isbn/978-620-0-59233-0.	

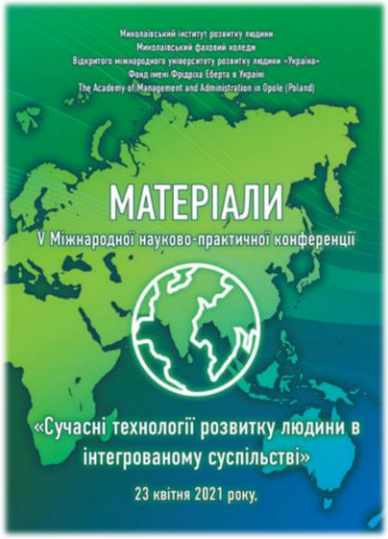
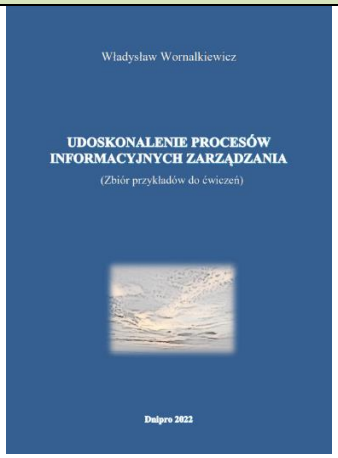
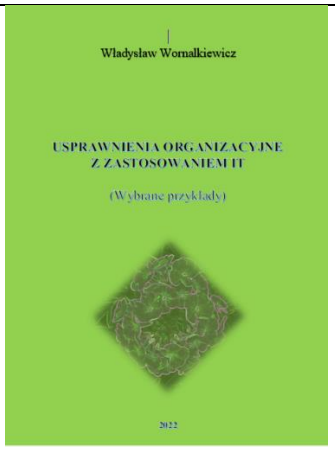
3. „*Doskonalenie systemów informacyjnych*” Część II „*Propozycja metod i modeli*”, monografia indywidualna, wydawca: GlobeEdit (International Book Market Service Ltd. , Member of OmniScriptum Publishing Group), Republic of Moldova, druk: Printforce - United Kingdom, 2020, 452 s., ISBN 978-620-0-59542-3. Link: https://www.morebooks.de/store/gb/book/doskonalenie-system%C3%B3w-informacyjnych-cz%C4%99%C5%9B%C4%87-ii/isbn/978-620-0-59542-3.	
4. „*Освіта і суспільство V*: Міжнародний збірник наукових праць”, Бердянський державний педагогічний університет, Ополє: видавництво Вищої школи управління і адміністрації в Ополє, 422 с., 2020, artykuły: „*MOBILE APPLICATIONS IN LOGISTICS*” („*Aplikacje mobilne w logistyce*”) (strony: 277-287), „*Metadata Editing Programs*”, „*Programy edycji metadanych*” (strony: 288-299), ISBN 978-83-66567-00-9.	
Link: https://www.wszia.opole.pl/wp-content/uploads/2020/09/2020_%D0%9E%D0%A1%D0%92%D0%86%D0%A2%D0%90_%D0%86_%D0%A1%D0%A3%D0%A1%D0%9F%D0%86%D0%9B%D0%AC%D0%A1%D0%A2%D0%92%D0%9E_V.pdf.	
5. *„Implementacja informatyczna wybranych metod ilościowych*”, monografia indywidualna recenzowana, Bratysława: Wydawnictwo DENAKYR, s. r. o., 2020, 500 s., ISBN 978-80-973568-0-4. Link: https://wornalkiewicz.files.wordpress.com/2020/02/implementacja-informatyczna-wybranych-metod-iloc59bciowych.pdf.	

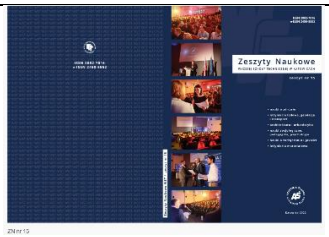
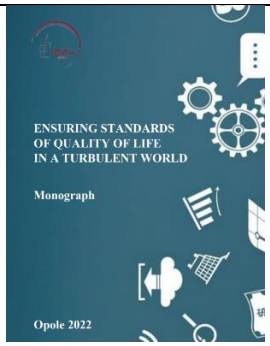
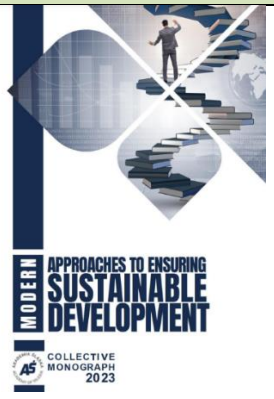
6. „*Informatyka w wybranych obszarach zarządzania*”, monografia indywidualna recenzowana, Berdiańsk: Wydawca „Svidler A.L.”, 2020, 450 s., ISBN 978-617-627-145-1. Link: https://wornalkiewicz.files.wordpress.com/2020/10/informatyka-w-wybranych-obszarach-zarzadzania.pdf.	
7. „*Procesy informacyjne w zarządzaniu*”, monografia indywidualna recenzowana, Opole: Wydawnictwo - Wyższa Szkoła Zarządzania i Administracji w Opolu, 2020, 373 s., ISBN 978-83-665-22-1. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/05/Procesy_informacyjne_w_zarzadzaniu.pdf.	
8. „*Journal of Modern Economic Research*”, Bratysława, monografia zbiorowa recenzowana, artykuł „*Innovative logistic solutions*” (*Innowacyjne rozwiązania logistyczne*), strony: 53-63, współautorstwo: Maksym Kutsenko, 2020, ISSN 2644-4380 nadruk; 2644-6332 online. Link: https://denakyrpublishing.science/index.php/jmer/article/view/40.	

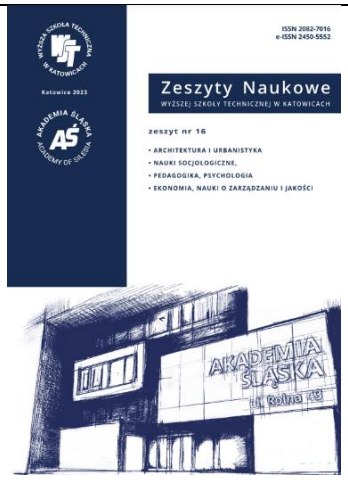
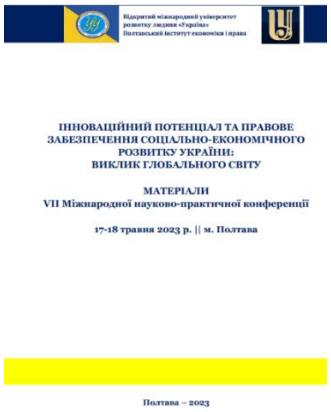
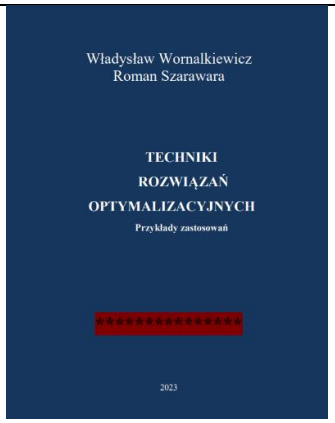
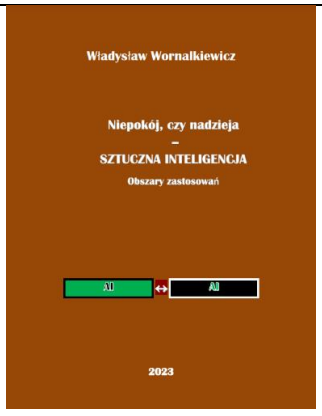
9. „*Improving living standards: current opportunities and limitations*”, monografia zbiorowa recenzowana, 594 s., Opole: The Academy of Management and Administration in Opole, 2020, artykuł „*POS systems*” (*Systemy klasy POS*), strony: 139-167, ISBN 978 - 83 - 66567 - 21 - 4. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/05/Zbirnyk_Osvita-i-suspilstvo-VI_new.pdf.	
10. „*Organizational problems of life quality management in the conditions of globalization*”, Opole: The Academy of Management and Administration in Opole, 428 s., 2020, artykuł „*Existing and intended logistic projects*” (*Istniejące i zamierzone przedsięwzięcia logistyczne*), strony: 309-334, ISBN 978 - 83 - 66567 - 20 - 7. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/05/2_2021.pdf.	
2021	
1. *„Narzędzia informatyczne zarządzania w warunkach specjalnych*”, monografia indywidualna recenzowana, Dnipro: Wydawca „Svidler A.L.”, 2021, 288 s., ISBN 978-617-627-168-0. Link: https://dspace.bdpu.org/handle/123456789/4082	

2. „*Systemy informacyjne w logistyce Wybrane aspekty*”, monografia indywidualna recenzowana, Dnipro: Wydawca „Svidler A/L.”, 2021, 376 s., ISBN 978-617-627-157-4. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/05/Systemy_informacyjne_w_logistyce_Wornalkiewicz.pdf.	
3. „*Економічні науки*”, monografia zbiorowa recenzowana, Вісник Хмельницького національного університету, 2021, № 5, Том I, artykuł: *THE OVERSIZED CARGO FORWARDING: ECONOMIC AND LEGAL ASPECTS*, UDC 330, strony: 175-180, ISSN 2307-5740, współautorstwo: YURII KRAVCHYK, ALLA KAPLUNOVSKA. Link: vknu-es-2021-n-5-298-175-180[1].pdf (khnu.km.ua). 3. „*Економічні науки*”, monografia zbiorowa recenzowana, Вісник Хмельницького національного університету, 2021, № 5, Том I, artykuł: *The Oversized Cargo Forwarding: Economic and Legal Aspects*, UDC 330, strony: 175-180, ISSN 2307-5740, współautorstwo: Yurii Kravchyk, Alla Kaplunovska. Link: vknu-es-2021-n-5-298-175-180[1].pdf (khnu.km.ua).	
4. „*Ukrainian Journal of Applied Economics*”, 2021, Volume 6, Nr 2, artykuł „*Transport infrastructure as a factor of the EU countries' economic development*” („*Infrastruktura transportowa jako czynnik rozwoju gospodarczego krajów UE*”), strony: 137-146, współautorstwo: Alla Kaplunovska, Olena Padchenko, ISSN 2415-8453. Link: https://doi.org/10.36887/2415-8453-2021-2-18.	
5. Huzhou University's Multicultural Center (Wielokulturowe Centrum Huzhou - Chiny), UDC 656.021.2, artykuł „*The perspective of increasing of road capacity*”, („*Perspektywa rozwoju dróg szosowych*”), współautorstwo: Ievegen Medvediev, Seriy Soroka, 2021, strony: 12-24. Link: https://wornalkiewicz.files.wordpress.com/2021/08/uniwersytet-chiny.pdf; http://kwh.zjhu.edu.cn.	2021 年 第 3 期

6. „*SCIENTIFIC NOTES OF THE PEDAGOGICAL DEPARTMEN*”, artykuł „*ONLINE LEARNING AT UNIVERSITIES: POLISH-UKRAINIAN EXPERIENCE*” „*Nauczanie online na uniwersytetach: polsko-ukraińskie doświadczenia*”, strony: 123-132, УДК 378.147.31, 2021, współautorstwo: Olena Taranukha, Olena Fonariuk. Link: 17560-Текст статті-34489-1-10-20210721 (2).pdf; https://periodicals.karazin.ua.	
7. „*Modern management: theories, concepts, implementation*”, monografia zbiorowa recenzowana, Opole: The Academy of Management and Administration in Opole, 2021, 430 s., artykuł „*UNBLOCKING THE "ODRA - DANUBE" WATERWAY*” (*Udrożnienie drogi wodnej Odra - Dunaj*), strony: 121-141, ISBN 978-83-66567-24-2. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/05/7_2021.pdf.	
8. „*Освіта І Суспільство VI*” Міжнародний збірник наукових праць, monografia zbiorowa recenzowana, Bierdiańsk: Wydawnictwo - Wyższa Szkoła Zarządzania i Administracji w Opolu, 2021, artykuł „*Opportunities to make milk reception logistics more modern*” („*Możliwości unowocześnienie logistyki odbioru mleka*”),, strony: 328-343, ISBN 978-83-66567-26-9. Link: https://www.wszia.opole.pl/wp-content/uploads/2020/05/Zbirnyk_Osvita-i-suspilstvo-VI_new.pdf.	
9. „*Scientific Notes of the Pedagogical Departmen*”, artykuł „*Online Learning at Universities: Polish-Ukrainian Experience*” „*Nauczanie online na uniwersytetach: polsko-ukraińskie doświadczenia*”, strony: 123-132, j. ang., УДК 378.147.31, 2021, współautorstwo: Olena Taranukha, Olena Fonariuk. Link: 17560-Текст статті-34489-1-10-20210721 (2).pdf, https://periodicals.karazin.ua; https://periodicals.karazin.ua/pedagogy/article/view/17560.	

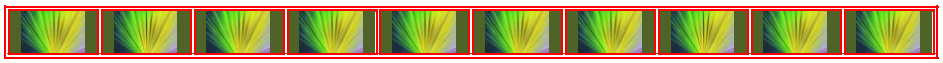
10. „*Сучасні технології розвитку людини в інтегрованому суспільстві*” Матеріали V Міжнародної науково-практичної конференції (*Materiały V Międzynarodowej naukowo-praktycznej konferencji*), 2021, Миколаївський інститут розвитку людини (Instytut w Mikolaiv - Ukraina), monografia zbiorowa recenzowana pokonferencyjna, 308 s., artykuł „*Socio-logistical aspects of the Vistula spit dug-through*”, („*Społeczno-logistyczne aspekty przekopu Mierzei Wiślanej*”), strony: 302-304, удк 371: 378. Link: https://www.wszia.opole.pl/wp-con-tent/uploads/2020/05/Spoleczno_logistyczne_aspekty_przekopu.pdf.	
2022	
1. „*Udoskonalenie procesów informacyjnych zarządzania (Zbiór przykładów do ćwiczeń)*, monografia indywidualna recenzowana, Dnipro: Wydawca „Svidler A.L.”, 241 s., ISBN 978-617-627-170-3.	
2. „*Usprawnienia organizacyjne z zastosowaniem IT (Wybrane przykłady)*, monografia indywidualna recenzowana, Kijów: Wydawca „Majster Knyg”, s. 340, ISBN 978-617-7652-59-4. Link do strony internetowej Narodowego Uniwersytetu Gospodarki Miejskiej im. O.M. Beketova w Charkowie: http://eprints.kname.edu.ua/61802/1/Monografia_7.pdf	

3. „*Zasilanie alternatywne pojazdów samochodowych*”, Zeszyty Naukowe Wyższej Szkoły Technicznej w Katowicach, 2022, nr 15, s. 30, ISSN 2082-7016, eISSN 2450-5552.	
4. Artykuły w ramach monografii *Edukacja i Społeczeństwo VII*, zbiór artykułów naukowych, Opole 2022, strony: 278-320, ISBN 978-83-66567-41-2: ○ „*Modelowanie biznesowe z zastosowaniem UML*”, stron: 16, ○ „*Potrzeba scalania systemów klasy ERP*”, stron: 12, ○ „*Wspomaganie dystrybucji systemem Dynamics NAV*”, s.: 15. Wydanie przez: ANS Opole, Wydział Pedagogiczny Uniwersytetu w Preszowie (Słowacja), Państwowy Uniwersytet Pedagogiczny w Bierdańsku (Ukraina).	
5. „*Projects in the field of 5G network construction*” (*Przedsięwzięcia w zakresie budowy sieci 5G*), s. 277-293, *Ensuring Standards of Quality of Life in a Turbulent World*. Monograph. The Academy of Applied Sciences – Academy of Management and Administration in Opole.	
2023	
1. Artykuły w ramach monografii zbiorowej „ *Modern Approaches to sustainable development* „AŚ Katowice 2023: ○ *Flood Prevention* (*Przeciwdziałanie powodziom wiosennym*), 1.12. s. 95-105, referat na konferencji. ○ *Organization of a rescue action in a situation earthquake (Organizacja akcji ratowniczej w sytuacji trzęsienia ziemi)*, 2.3. s. 285-294. Monografia pokonferencyjna 4th International Scientific Conference „*Role of Science and Education in Subtainable Development*” (*Znaczenie nauki i edukacji w zrównoważonym rozwoju*), konferencja internetowa.	

2. Artykuł „*Procedure implementation of logistics services”* (*Implementacja procedury optymalizacji usług logistycznych*)**,** Zeszyty Naukowe Wyższej Szkoły Technicznej w Katowicach, 2023, nr 16, s. 157-170. ISSN: 2082-7016; e-ISSN: 2450-5512; DOI: 10.54264/0070.	
3. Artykuł „*Cyber security*” (*Cybersecurity*), abstract, s. 5, VII International Scientific and Practice Conference „*Innovative potential and legal suport of social and economic development of Ukraine: the challenge of the global world*”, konferencja internetowa, referat na platformie ZOOM, Połtawski Instytut Ekonomii i Prawa Uniwersytetu „Ukraina”, s. 16-21, Poltava, may, 17-18, 2023, УДК 330.111.66(477):34.	
4. Wornalkiewicz W., Szarawara R., podręcznik „*Techniki rozwiązań optymalizacyjnych Przykłady zastosowań*”, Połtawski Instytut Ekonomii i Prawa Uniwersytetu „Ukraina”, s. 244, UDK 338.24:001.82(075), ISBN 978-966-388-674-9.	
5. Wornalkiewicz W., monografia indywidualna „*Niepokój, czy nadzieja – Sztuczna Inteligencja. Obszary zastosowań*”, s. 165, ISBN 978-617-627-171-0, Państwowy Uniwersytet Pedagogiczny w Berdiańsku, Wydawca „Svidler A.L.”, Dnipro 2023.	

6. Artykuł „*Aplikacje sztucznej inteligencji. Obszary zastosowań*" – w monografii pokonferencyjnej, s. 12, 8. Międzynarodowa Konferencja Naukowo-Praktyczna „*Współczesne problemy podniesienia jakości życia w zglobalizowanym świecie*", 29-30.11.2023, 12 godzin, ANS-WSZiA Opole, w druku.	
7. Artykuł „*Metody ochrony przed cyberprzestępczością*", Zbiór artykułów naukowych, s. 14, Uniwersytet w Preszowie, Słowacja, w druku.	

Bibliografia



Bednarek J., Andrzejewska A., *Zagrożenie cyberprzestrzeni i świata wirtualnego*, Difin 2014, https://bonito.pl/produkt/zagrozenia-cyberprzestrzeni-i-swiata-wirtualnego.

Berners-Lee T., Masinter L., McCahill M., *Uniform Resource Locators* (URL), IETF, 1994.

ITU Cybercrime Legislation Toolkit, Międzynarodowy Związek Telekomunikacyjny, 2010.

Łużak T., *Product Manager, Cybersecurity* - Netia S.A., *Rodzaje ataków hakerskich*, https://www.netia.pl/pl/srednie-i-duze-firmy/youtro-strefa-wiedzy/rodzaje-atakow-hackerskich.

Madej M., Terlikowski M., *Bezpieczeństwo teleinformatyczne państwa*, Polski Instytut Spraw Międzynarodowych, Warszawa 2009.

Making calls from Hangouts - in Gmail and across the web, „Official Gmail Blog" (https://pl.wikipedia.org/wiki/Google_Hangouts).

Płaszczak P., *Co to jest Big Data*, konferencja „*Big Data & Business Intelligence*", Warszawa 2013.

Sawicki M., *Cyberprzestępczość*, Wydawnictwo C.H. Beck, *Monografie prawnicze*, 2013.

Shinder D.L., Tittel E. (Technical Editor), *Cyberprzestępczość Jak walczyć z łamaniem prawa w Sieci* (*Scene of the Cybercrime. Computer Forensics Handbook*), Helion, 2004.

Stępnik A., *Big data w perspektywie memetycznej*, Zeszyt memetyczny 16, 2015.

Szczegielniak-Rekiel A., Kelner J.M., Przegląd metod szyfrowania i dekryptażu archiwum ZIP, czasopismo: *Elektronika: konstrukcje, technologie, zastosowania*, Wojskowa Akademia Techniczna, Warszawa 2022.

Wornalkiewicz W., *Popularyzacja metod ilościowych w Internecie*, Wydawnictwo Instytut Śląski, Opole 2017.

Zacher L. (1997), *Rewolucja informacyjna i społeczeństwo: niektóre trendy, zjawiska i kontrowersje*, Fundacja edukacyjna „*Transformacje*", 1997.

Владислав Ворналкєвіч

ВСТУП ДО ПРОБЛЕМИ

«ІТ-БЕЗПЕКА ТА КІБЕРБЕЗПЕКА»

монографія

польською мовою

Підп. до друку 22.04.2024. Формат 60х84 1/16

Папір офсетний. Друк цифровий. Ум. друк. арк. 9,11.

Обл.-вид. арк. 11,14. Наклад 20 прим.

Надруковано в типографії видавництва «Свідлер А.Л.»

49041, м. Дніпро, а/с 2493,

тел./факс +38 (067) 635-78-83

http://www.garant-sv.com

Dr inż. prof. ANS-WSZiA w Opolu (Polska) Władysław Wornalkiewicz jest autorem książek z zakresu statystyki i ekonometrii z zastosowaniem programów komputerowych. Jego praca naukowa skupia się na testowaniu różnych metod modelowania ekonometrycznego z użyciem danych statystycznych oraz takich narzędzi programistycznych jak pakiety *Excel*, *Gretl*, *WinQSB*, *R*, *DEAP*, *Expert Choice* i innych. Jest absolwentem kilku kierunków na Politechnice Wrocławskiej, gdzie uzyskał tytuły inżyniera mechanika, magistra inżyniera organizatora produkcji, doktora nauk ekonomicznych, pedagoga Ministerstwa Edukacji Narodowej. Ukończył również program edukacyjny „*Polska w procesie integracji europejskiej*".

Zatrudniony jest w Akademii Nauk Stosowanych (ANS-WSZiA) w Opolu na stanowisku Profesora Uczelni. Obecnie ma tam wykłady z przedmiotów: *Procesy informacyjne w zarządzaniu*, *Systemy informacyjne w logistyce*, *Technologie informacyjne*, *Informatyka w zarządzaniu*, *Badania operacyjne*, *Optymalizacja decyzji gospodarczych*. Ponadto prowadzi seminaria dyplomowe licencjackie i magisterskie. W dorobku naukowym ostatnich lat są następujące książki: *Wstęp do ekonometrii i badań operacyjnych,* tom I. *Wybrane modele ekonometryczne, Formułowanie modeli ekonometrycznych do potrzeb zarządzania* - dwa tomy (*Środowiska programowe statystyki opisowej, Zagadnienia ekonometrii*), *Wdrożenie zintegrowanego systemu informatycznego wspomagającego zarzadzanie, Wprowadzenie do projektowania systemów informatycznych zarządzania* - dwie części (*Wybrane systemy zarządzania i sposoby modelowania*, *Narzędzia wspomagające projektowanie systemów*), *Elementy inżynierii i analizy systemów zarządzania Wybrane aspekty logistyczne - rozdziały: 1-9, 16-22, Współpraca specjalizowanych systemów informatycznych.*

W latach 2020-2021 ukazały się monografie indywidualne autora, a mianowicie:

- *Implementacja informatyczna wybranych metod ilościowych*, opublikowana przez wydawnictwo DENAKYR w Bratysławie;
- *Informatyka w wybranych obszarach zarządzania,* Państwowy Uniwersytet Pedagogiczny w Berdyansku (Ukraina);
- *Procesy informacyjne w zarządzaniu,* Wyższa Szkoła Zarządzania i Administracji w Opolu;
- *Systemy informacyjne w logistyce Wybrane aspekty*, Państwowy Uniwersytet Pedagogiczny w Berdyansku (Ukraina);
- *Narzędzia informatyczne zarządzania w warunkach specjalnych*, Państwowy Uniwersytet Pedagogiczny w Berdyansku (Ukraina);
- *Udoskonalenie procesów informacyjnych zarządzania (zbiór przykładów do ćwiczeń)*, Państwowy Uniwersytet Pedagogiczny w Berdyansku (Ukraina);
- *Usprawnienia organizacyjne z zastosowaniem IT (Wybrane przykłady)*, Państwowy Uniwersytet Pedagogiczny w Berdyansku (Ukraina);
- *Doskonalenie systemów informatycznych*: część I. *Wybrane aspekty zarzadzania*, część II. *Propozycja metod i modeli,* GlobeEdit (Niemcy);
- *Narzędzia wdrażania systemów informatycznych*, GlobeEdit (Niemcy);
- *Współpraca specjalizowanych systemów informatycznych*, w GlobeEdit (Niemcy).

Efektem prac badawczych są trzy publikacje: skrypt - *Metoda badania przyczynowo-skutkowego związków między cechami statystycznymi*, książka - *Modele ekonometryczne PKB obiektów struktury terytorialnej*, książka *Popularyzacja wybranych metod ilościowych w Internecie*. Jest autorem wielu artykułów wydrukowanych w monografiach WSZiA w Opolu, opublikowanych przez Uniwersytet Pedagogiczny w Berdyansku (Ukraina), Uniwersytet Pedagogiczny w Presovie (Słowacja), Uniwersytet Technologiczny w Czernigowie (Ukraina) i w innych wydawnictwach.