ODPOWIEDZIALNOŚĆ KARNA ZA HACKING

I INNE PRZESTĘPSTWA PRZECIWKO DANYM KOMPUTEROWYM I SYSTEMOM INFORMATYCZNYM

Filip Radoniewicz

MONOGRAFIE

Wolters Kluwer

ODPOWIEDZIALNOŚĆ KARNA ZA HACKING

I INNE PRZESTĘPSTWA PRZECIWKO DANYM KOMPUTEROWYM I SYSTEMOM INFORMATYCZNYM

Filip Radoniewicz

MONOGRAFIE

Wolters Kluwer

WARSZAWA 2016

Stan prawny na 15 listopada 2015 r.

Recenzent
Dr hab. Andrzej Adamski, prof. UMK

Wydawca
Monika Pawłowska

Redaktor prowadzący
Adam Choiński

Opracowanie redakcyjne
Katarzyna Paterak-Kondek

Łamanie
Wolters Kluwer

ISBN 978-83-264-9467-3
ISSN 1897-4392
ISBN PDF-a: 978-83-8092-212-9

Wydane przez:
Wolters Kluwer SA

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

www.wolterskluwer.pl
księgarnia internetowa www.profinfo.pl

Książkę poświęcam żonie Monice,
z podziękowaniem za wsparcie i wyrozumiałość

Spis treści

Wykaz skrótów

Źródła prawa

ACTA	–	Anti-Counterfeiting Trade Agreement (Umowa handlowa dotycząca zwalczania obrotu towarami podrabianymi)
CMA	–	Computer Misuse Act 1990 (brytyjska ustawa o nadużyciach komputerowych z 1990 r.)
Code Pénal	–	francuski kodeks karny z 1992 r.
d. TUE	–	Traktat o Unii Europejskiej podpisany w Maastricht dnia 7 lutego 1992 r., w brzmieniu sprzed wejścia w życie Traktatu z Lizbony (wersja skonsolidowana uwzględniająca traktaty akcesyjne, które weszły w życie w dniu 1 maja 2004 r. i 1 stycznia 2007 r.: Dz. Urz. UE C 321E z 29.12.2006 r., s. 5)
decyzja ramowa 2002/584 w sprawie ENA	–	decyzja ramowa Rady 2002/584/WSiSW z dnia 13 czerwca 2002 r. w sprawie europejskiego nakazu aresztowania i procedury wydawania osób między Państwami Członkowskimi (Dz. Urz. WE L 190 z 18.07.2002 r., s. 1)
decyzja ramowa 2005/222	–	decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz. Urz. UE L 69 z 16.03.2005 r., s. 67)
decyzja ramowa 2008/841	–	decyzja ramowa Rady 2008/841/WSiSW z dnia 24 października 2008 r. w sprawie zwalczania przestępczości zorganizowanej (Dz. Urz. UE L 300 z 11.11.2008 r., s. 42)

dyrektywa 2013/40	–	dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastepująca decyzję ramową Rady 2005/222/WSiSW (Dz. Urz. UE L 218 z 14.08.2013 r., s. 8)
dyrektywa o handlu elektronicznym	–	dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz. Urz. WE L 178 z 17.07.2000 r., s. 1)
dyrektywa o prywatności i łączności elektronicznej	–	dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. Urz. WE L 201 z 31.07.2002 r., s. 37)
dyrektywa ramowa	–	dyrektywa 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) (Dz. Urz. WE L 108 z 24.04.2002 r., s. 33)
EKPCz	–	Konwencja o ochronie praw człowieka i podstawowych wolności, sporządzona w Rzymie dnia 4 listopada 1950 r. (Dz. U. z 1993 r. Nr 61, poz. 284 z późn. zm.)
k.c.	–	ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (tekst jedn.: Dz. U. z 2014 r. poz. 121 z późn. zm.)
k.k.	–	ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553 z późn. zm.)
Konstytucja RP	–	Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.)
Konwencja o cyberprzestępczości	–	Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz. U. z 2015 r. poz. 728)

k.p.k.	–	ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 z późn. zm.)
k.w.	–	ustawa z dnia 20 maja 1971 r. – Kodeks wykroczeń (tekst jedn.: Dz. U. z 2015 r. poz. 1094 z późn. zm.)
MPPOiP	–	Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz. U. z 1977 r. Nr 38, poz. 167)
nowelizacja z 2004 r.	–	ustawa z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń (Dz. U. Nr 69, poz. 626)
nowelizacja z 2008 r.	–	ustawa z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. Nr 214, poz. 1344)
pr. tel.	–	ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (tekst jedn.: Dz. U. z 2014 r. poz. 243 z późn. zm.)
Protokół dodatkowy do Konwencji o cyberprzestępczości	–	Protokół dodatkowy do Konwencji Rady Europy o cyberprzestępczości dotyczący penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych, sporządzony w Strasburgu dnia 28 stycznia 2003 r. (Dz. U. z 2015 r. poz. 730)
RIPA	–	Regulation of Investigatory Powers Act 2000 (brytyjska ustawa o uregulowaniu środków śledczych z 2000 r.)
rozporządzenie 460/2004	–	rozporządzenie (WE) nr 460/2004/WE Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (Dz. Urz. UE L 77 z 13.03.2004 r., s. 1.)
r.z.t.p.	–	rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (Dz. U. Nr 100, poz. 908 z późn. zm.)
StGB	–	niemiecki kodeks karny (Strafgesetzbuch) z 1871 r. w wersji opublikowanej w dniu 13 listopada 1998 r. (BGBl. I S. 3322)

TFUE	–	Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana Dz. Urz. UE C 326 z 26.10.2012 r., s. 47, z późn. zm.)
Traktat Konstytucyjny	–	Traktat ustanawiający Konstytucję dla Europy (Wspólnoty Europejskiej) podpisany w Rzymie dnia 29 października 2004 r. (Dz. Urz. UE C 310 z 16.12.2004 r., s. 1)
Traktat z Amsterdamu	–	Traktat z Amsterdamu zmieniający Traktat o Unii Europejskiej, Traktaty ustanawiające Wspólnoty Europejskie oraz niektóre związane z nimi akty podpisany w Amsterdamie dnia 2 października 1997 r. (Dz. Urz. WE C 340 z 10.11.1997 r., s. 1)
Traktat z Lizbony	–	Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie dnia 13 grudnia 2007 r. (Dz. Urz. UE C 306 z 17.12.2007 r., s. 1)
Traktat z Maastricht	–	Traktat o Unii Europejskiej podpisany w Maastricht dnia 7 lutego 1992 r. (w brzmieniu pierwotnym) (Dz. Urz. WE C 191 z 29.07.1992 r., s. 1)
Traktat z Nicei	–	Traktat z Nicei zmieniający Traktat o Unii Europejskiej, Traktaty ustanawiające Wspólnoty Europejskie oraz niektóre związane z nimi akty prawne podpisany w Nicei dnia 26 lutego 2001 r. (Dz. Urz. WE C 80 z 10.3.2001 r., s. 1)
TUE	–	Traktat o Unii Europejskiej podpisany w Maastricht dnia 7 lutego 1992 r. (wersja skonsolidowana Dz. Urz. UE C 326 z 26.10.2012 r., s. 13, z późn. zm.)
TWE	–	Traktat ustanawiający Wspólnotę Europejską z 25 marca 1957 r. (w brzmieniu bezpośrednio sprzed wejścia w życie Traktatu z Lizbony) (wersja skonsolidowana uwzględniająca traktaty akcesyjne, które weszły w życie w dniu 1 maja 2004 r. i 1 stycznia 2007 r., Dz. Urz. UE C 321E z 29.12.2006 r., s. 37)
u.i.d.p.p.	–	ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jedn.: Dz. U. z 2014 r. poz. 1114)

u.o.d.o.	–	ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jedn.: Dz. U. z 2015 r. poz. 1309 z późn. zm.)
USC	–	The Code of Laws of the United States of America (United States Code) (skodyfikowany zbiór prawa federalnego obowiązującego w Stanach Zjednoczonych Ameryki)
u.ś.u.d.e.	–	ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jedn.: Dz. U. z 2013 r. poz. 1422 z późn. zm.)
u.z.n.k.	–	ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (tekst jedn.: Dz. U. z 2003 r. Nr 153, poz. 1503 z późn. zm.)
zalecenie (89) 9	–	zalecenie Komitetu Ministrów Rady Europy nr R (89) 9 z dnia 13 września 1989 r. w sprawie przestępstw komputerowych
zalecenie (92) 188	–	zalecenie Rady OECD C (92) 188 z dnia 26 listopada 1992 r. dotyczące wytycznych w zakresie bezpieczeństwa systemów informatycznych
zalecenie (2002) 131	–	zalecenie Rady OECD C (2002) 131 z dnia 25 lipca 2002 r. w sprawie wytycznych w zakresie bezpieczeństwa systemów i sieci informatycznych: w kierunku kultury bezpieczeństwa

Publikatory, czasopisma, zbiory orzecznictwa

BGBl.	–	Dziennik Urzędowy Republiki Federalnej Niemiec
CzPKiNP	–	Czasopismo Prawa Karnego i Nauk Penalnych
Dz. U.	–	Dziennik Ustaw
Dz. Urz. UE	–	Dziennik Urzędowy Unii Europejskiej
Dz. Urz. WE	–	Dziennik Urzędowy Wspólnot Europejskich
e-Biuletyn CBKE	–	e-Biuletyn Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej, Wydział Prawa, Administracji i Ekonomii, Uniwersytet Wrocławski
EP	–	Edukacja Prawnicza

EPS	–	Europejski Przegląd Sądowy
M. Praw.	–	Monitor Prawniczy
OSNKW	–	Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa
OSNwSK	–	Orzecznictwo Sądu Najwyższego w Sprawach Karnych
OSP	–	Orzecznictwo Sądów Polskich
OTK	–	Orzecznictwo Trybunału Konstytucyjnego
OTK-A	–	Orzecznictwo Trybunału Konstytucyjnego, Zbiór Urzędowy, seria A
PiP	–	Państwo i Prawo
Prok. i Pr.	–	Prokuratura i Prawo
PS	–	Przegląd Sądowy
St. Praw.	–	Studia Prawnicze
WPP	–	Wojskowy Przegląd Prawniczy

Organizacje, instytucje, sądy i trybunały

AIDP/AIPL	–	Międzynarodowe Stowarzyszenie Prawa Karnego
ARPA	–	Agencja Zaawansowanych Projektów Badawczych (Advanced Research Project Agency)
CDPC	–	Europejski Komitet ds. Przestępczości (European Committee on Crime Problems)
CERN	–	Europejska Organizacja Badań Jądrowych
DARPA	–	Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności (Defence Advanced Research Project Agency)
ECOSOC	–	Rada Gospodarcza i Społeczna ONZ
EFF	–	Electronic Frontier Foundation
EKES	–	Europejski Komitet Ekonomiczno-Społeczny
ETPCz	–	Europejski Trybunał Praw Człowieka
ETS	–	Europejski Trybunał Sprawiedliwości (od 1 grudnia 2009 r. Trybunał Sprawiedliwości Unii Europejskiej)
Eurojust	–	Europejska Sieć Sądowa
Europol	–	Europejski Urząd Policji
EWG	–	Europejska Wspólnota Gospodarcza

EWI	–	EastWest Institute
ICCP	–	Komitet ds. Polityki Informatyzacji, Komputeryzacji i Telekomunikacji (Committee on Information, Communications and Computer Policy – ICCP Committee)
Interpol	–	Międzynarodowa Organizacja Policji Kryminalnych
ISO	–	Międzynarodowa Organizacja Standaryzacyjna (ang. International Organization for Standarization, fr. Organisation internationale de normalisation)
ITU	–	Międzynarodowy Związek Telekomunikacyjny (International Telecommunication Union)
NSA	–	Naczelny Sąd Administracyjny
OECD	–	Organizacja Współpracy Gospodarczej i Rozwoju (ang. Organization for Economic Co-operation and Development)
SA	–	Sąd Apelacyjny
SN	–	Sąd Najwyższy
TK	–	Trybunał Konstytucyjny
UE	–	Unia Europejska
WE	–	Wspólnota Europejska

Inne

AS	–	system autonomiczny (Autonomous System)
CERT	–	zespół ds. reagowania na przypadki naruszenia bezpieczeństwa teleinformatycznego (Computer Emergency Response Team)
DDoS	–	rozproszona odmowa usługi (distributed denial of service)
DoS	–	odmowa usługi (denial of service)
Explanatory Report	–	Komentarz do Konwencji o cyberprzestępczości (Explanatory Report to Convention on Cybercrime)
GCA	–	Global Cybersecurity Agenda (Globalna Agenda na rzecz Cyberbezpieczeństwa)

HLEG	–	High-level expert group (grupa ekspertów wysokiego szczebla ds. spraw cyberbezpieczeństwa, powołana w ramach ITU)
INGOs	–	międzynarodowe organizacje pozarządowe (International Non-Governmental Organizatons)
ITU Toolkit	–	ITU Toolkit for Cybercrime Legislation
LEX	–	system informacji prawnej LEX
p2p	–	sieci peer-to-peer
PWBiS	–	Przestrzeń Wolności, Bezpieczeństwa i Sprawiedliwości
Raport OECD	–	Computer-Related Crime. Analysis of legal policy in the OECD Area, ICCP Series nr 10, OECD, Paris 1986
WAP	–	Wireless Application Protocol
WPZiB	–	Wspólna Polityka Zagraniczna i Bezpieczeństwa
WSiSW	–	Wymiar Sprawiedliwości i Sprawy Wewnętrzne

Wstęp

Od początku ubiegłego wieku mamy do czynienia z rozwojem techniki na niespotykaną wcześniej skalę. Jej gałęzią, która ostatnimi czasy rozwija się najprężniej, jest wkraczająca we wszystkie dziedziny życia szeroko rozumiana technologia informatyczna, a w szczególności teleinformatyka. Dzieje się tak przede wszystkim w związku z postępującą w ostatnich latach konwergencją informatyki i telekomunikacji, będącą następstwem rozwoju sieci komputerowych oraz Internetu, wymuszającego konieczność zapewnienia szybkiego i efektywnego przetwarzania oraz przekazywania informacji, której rola niepomiernie wzrosła. Stała się ona nie tylko towarem, zyskując ogromne znaczenie ekonomiczne, ale także istotnym instrumentem w dziedzinie polityki i sprawowania władzy. Coraz częściej w związku z tym można spotkać się ze stwierdzeniem, że żyjemy w społeczeństwie „rewolucji informacyjnej", „informacyjnym", a nawet „informatycznym"[1].

Oczywiście, proces ten, poza niewątpliwymi korzyściami, niesie za sobą także zagrożenia. Janusz Barta i Ryszard Markiewicz porównują Internet do Dzikiego Zachodu, jako terenu, „gdzie prawa nie ma lub trudno je egzekwować"[2]. Nie ulega wątpliwości, że skonstruowanie regulacji zapewniającej bezpieczeństwo przepływu informacji stanowi nie lada wyzwanie dla tworzących prawo. Wyzwanie, co należy podkreślić, któremu ustawodawcom niełatwo podołać.

Tematem niniejszego opracowania jest odpowiedzialność karna za przestępstwo hackingu. Już na samym wstępie należy poczynić istotną

[1] Zob. P. Kardas, *Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego*, CzPKiNP 2000, nr 1, s. 25–30; R. Skubisz, *Internet – ku społeczeństwu przyszłości* (w:) *Internet 2000. Prawo – ekonomia – kultura*, Lublin 1999, s. 9–12.

[2] J. Barta, R. Markiewicz, *Internet a prawo*, Kraków 1998, s. 9.

uwagę natury terminologicznej, dotyczącą rozumienia tego pojęcia. Kwestia ta zostanie omówiona obszerniej w rozdziale pierwszym, stanowiącym wprowadzenie do problematyki przestępczości komputerowej. W tym miejscu zasygnalizować jedynie należy, że obecnie termin ten rozumiany jest nieco szerzej, niż pierwotnie. Początkowo pojmowany był jako uzyskiwanie nielegalnego dostępu do zasobów komputerów lub sieci komputerowych. „Współczesne" rozumienie tego terminu jest szersze, obejmuje wszelkie działania mające na celu zakłócenie funkcjonowania sieci, a więc zachowania stanowiące przestępstwa przeciwko bezpieczeństwu informacji we wszystkich jego aspektach (integralności, poufności i dostępności)[3].

Problematyka przestępstw komputerowych przeciwko bezpieczeństwu informacji, mimo swojego wzrastającego znaczenia, nie cieszy się należytym zainteresowaniem doktryny. Zjawisko to w zasadzie nie doczekało się również badań empirycznych[4], stąd jego rzeczywista skala w Polsce nie była znana. Nawet analiza danych pochodzących z oficjalnych statystyk przestępczości ujawnionej (statystyka policyjna), których przedmiotem były przestępstwa stypizowane w art. 267–269b ustawy z dnia

[3] Na marginesie warto zauważyć, iż zwykle w piśmiennictwie dla określenia sprawców przestępstw komputerowych, godzących w funkcjonowanie sieci komputerowych, używa się pojęcia „hackerzy". Postępują tak nawet ci autorzy, którzy starają się przestrzegać wskazanej wyżej konwencji językowej i pod pojęciem hackingu rozumieją jedynie uzyskanie nielegalnego dostępu do systemu komputerowego (czy sieci komputerowej) lub danych komputerowych (zob. S.W. Brenner (w:) R.D. Clifford (red.), *Cybercrime. The Investigation, Prosecution and Defense of a Computer-related Crime,* Durham 2011, s. 18; J. Erickson, *Hacking. Sztuka penetracji*, Gliwice 2004, s. 9–13; D.L. Shinder, E. Tittel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci,* Gliwice 2005, s. 301; U. Sieber, *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka*, Przegląd Policyjny 1995, nr 3, s. 12; M. Siwicki, *Cyberprzestępczość*, Warszawa 2013. s. 158).

[4] Badania z tego zakresu przeprowadzili A. Adamski (*Nadużycia komputerowe w Polsce w świetle wstępnych wyników badań wiktymizacyjnych* (w:) A. Adamski (red.), *Prawne aspekty nadużyć popełnianych z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Materiały z konferencji naukowej, Poznań, 20–22 IV 1994*, Toruń 1994, s. 33–52) oraz R.A. Stefański (*Przestępstwa internetowe w Polsce. Analiza praktyki*, St. Praw. 2005, z. 4, s. 121–128). Jednak przedmiotem badań A. Adamskiego była wiktymizacja (opierały się na analizie ankiet wypełnionych przez pokrzywdzonych) i przeprowadzone zostały w pierwszej połowie lat 90., a więc w okresie, gdy technologia informatyczna, a w związku z tym przestępczość komputerowa, jeszcze „raczkowały". Natomiast badania przeprowadzone przez R.A. Stefańskiego opierały się na analizie 619 wyselekcjonowanych akt spraw zarejestrowanych w latach 2001–2002, których przedmiotem była bardzo zróżnicowana grupa przestępstw („przestępstwa internetowe"), a co za tym idzie – przestępstwa przeciwko bezpieczeństwu danych komputerowych oraz systemów informatycznych stanowiły znikomy ich odsetek (23 sprawy, tj. niespełna 4%).

6 czerwca 1997 r. – Kodeks karny[5], okazała się mało miarodajna (zob. rozdział siódmy).

W związku z powyższym celem niniejszego opracowania była w pierwszej kolejności analiza przepisów art. 267–269b k.k., w których dokonano kryminalizacji przestępstw komputerowych przeciwko bezpieczeństwu informacji, z uwzględnieniem regulacji międzynarodowych i unijnych oraz rozwiązań obowiązujących w wybranych krajach europejskich. Jednocześnie stanowi ono próbę skonfrontowania polskich rozwiązań z wynikami badań empirycznych o zasięgu ogólnokrajowym, których przedmiotem była problematyka odpowiedzialności karnej za przestępstwo hackingu.

Niniejsza monografia składa się ze wstępu, siedmiu rozdziałów i zakończenia. Dwa pierwsze rozdziały mają charakter wprowadzający do omawianej problematyki, rozdział pierwszy jest ogólnym wprowadzeniem do tematyki hackingu, następne pięć ma charakter dogmatyczny, natomiast rozdział ostatni prezentuje wyniki badań empirycznych.

Rozdział pierwszy, poza krótkim przedstawieniem historii sieci komputerowych oraz Internetu i jego ogólnej charakterystyki, zawiera podstawowe informacje mające przybliżyć zasady funkcjonowania sieci komputerowych, jak również zwięzłe omówienie technicznej strony przestępczości komputerowej, czyli metod stosowanych przez przestępców, zwanych potocznie hackerami.

O ile celem rozdziału pierwszego jest ogólne wprowadzenie do tematyki hackingu poprzez przedstawienie podstawowych informacji na temat tego zjawiska oraz omówienie jego technicznych aspektów, o tyle rozdział drugi stanowi niejako właściwy wstęp do niniejszego opracowania. Przedstawione w nim zostały próby zdefiniowania przestępstw komputerowych i ich klasyfikacji, historia kryminalizacji tego zjawiska wraz z wiążącymi się z tym trudnościami oraz wyjaśnienie podstawowych pojęć: informacji, danych komputerowych oraz programu komputerowego.

W rozdziale trzecim omówione zostały najistotniejsze inicjatywy międzynarodowe, których przedmiotem jest przestępczość komputerowa. Ich cechą charakterystyczną jest to, że mają charakter niewiążący. Wyjątek stanowi Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.[6], na którą został położony w związ-

[5] Dz. U. Nr 88, poz. 553 z późn. zm.
[6] Dz. U. z 2015 r. poz. 728.

ku z tym szczególny nacisk. Poza tym aktem zostały zaprezentowane inne dokumenty oraz inicjatywy podejmowane przez organizacje międzynarodowe, zarówno rządowe (Organizacja Narodów Zjednoczonych, Międzynarodowy Związek Telekomunikacyjny, Organizacja Współpracy Gospodarczej i Rozwoju, Rada Europy, Grupa G7/G8), jak i pozarządowe (Międzynarodowa Organizacja Policji Kryminalnych, Międzynarodowe Stowarzyszenie Prawa Karnego, EastWest Institute).

Działaniom Unii Europejskiej w zakresie zwalczania hackingu poświęcony został rozdział czwarty. Rozwiązanie takie było podyktowane odrębnością porządku prawnego Unii Europejskiej od prawa międzynarodowego oraz krajowego[7]. Omówione zostały przede wszystkim decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[8] oraz – zastępująca ją – dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW[9].

Rozdział piąty poświęcony jest polskiej regulacji karnej i zawiera omówienie znamion przestępstw komputerowych zawartych w rozdziale XXXIII kodeksu karnego:

1) uzyskania nieuprawnionego dostępu do informacji (art. 267 § 1 k.k.);
2) uzyskania nieuprawnionego dostępu do całości systemu informatycznego lub jego części (art. 267 § 2 k.k.);
3) nielegalnego podsłuchu i inwigilacji za pomocą urządzeń technicznych i programów komputerowych (art. 267 § 3 k.k.);
4) ujawnienia informacji uzyskanej nielegalnie (art. 267 § 4 k.k.);
5) naruszenia integralności zapisu informacji (art. 268 § 2 i 3 k.k.);
6) naruszenia integralności danych informatycznych, utrudniania dostępu do nich oraz zakłócania ich przetwarzania (art. 268a § 1 i 2 k.k.);
7) sabotażu informatycznego (art. 269 § 1 k.k.);

[7] Wyroki ETS z dnia: 5 lutego 1963 r. w sprawie *NV Algemene Transport en Expeditie Onderneming van Gend and Loos przeciwko Holenderskiej administracji celnej* (26/62) oraz 15 lipca 1964 r. w sprawie *Flaminio Costa przeciwko E.N.E.L.* (6/64). Zob. szerzej np. J. Barcz, *Charakter prawny i struktura Unii Europejskiej. Pojęcie prawa UE* (w:) J. Barcz (red.), *Prawo Unii Europejskiej. Zagadnienia systemowe*, Warszawa 2006, s. 28; S. Biernat, *Prawo Unii Europejskiej a prawo państw członkowskich* (w:) J. Barcz (red.), *Prawo Unii...*, s. 253–254; A. Zawidzka-Łojek, *Prawo Unii Europejskiej a prawo krajowe państw członkowskich* (w:) J. Barcz (red.), *Źródła prawa Unii Europejskiej*, Warszawa 2012, s. 146–147.

[8] Dz. Urz. UE L 69 z 16.03.2005 r., s. 67.

[9] Dz. Urz. UE L 218 z 14.08.2013 r., s. 8.

8) zakłócenia pracy systemu komputerowego lub sieci teleinformatycznej (art. 269a k.k.);
9) tzw. bezprawnego wykorzystania urządzeń, programów i danych (art. 269b § 1 k.k.).

Analiza obejmuje kolejno znamiona przedmiotu ochrony, strony przedmiotowej, podmiotu, strony podmiotowej każdego z nich. Przyjęcie takiego układu treści (niejako komentarzowego) podyktowane zostało potrzebą zachowania odpowiedniej przejrzystości. Ta ostatnia uwaga odnosi się również do sposobu zaprezentowania problematyki zbiegu przepisów, zbiegu przestępstw, wymiaru kary oraz trybu ścigania omówionych w odrębnych podrozdziałach, wspólnych dla wszystkich analizowanych przestępstw.

W rozdziale szóstym zaprezentowano unormowania dotyczące przestępstw komputerowych obowiązujące w wybranych państwach europejskich. Celem opracowania było wyróżnienie pewnych modeli kryminalizacji tego zjawiska oraz przedstawienie wybranych krajowych unormowań, które z jednej strony byłyby typowe dla tychże modeli, a z drugiej – zawierałyby pewne odmienności czy oryginalne rozwiązania. Umieszczenie tego rozdziału w tym właśnie miejscu, a więc po rozdziale poświęconym polskiej regulacji, powinno dać czytelnikowi maksymalnie przejrzysty obraz omawianego tematu.

W ostatnim rozdziale zaprezentowano wyniki badań empirycznych opartych na analizie akt 1163 postępowań przygotowawczych zarejestrowanych w jednostkach organizacyjnych prokuratury całego kraju w latach 2009–2010. Celem badań było dokonanie oceny skali zjawiska hackingu w Polsce, jak również przyjmowanych kwalifikacji prawnych, sposobów zakończenia wszczętych postępowań oraz przyczyn odmowy ich wszczęcia, a także rodzaju i wysokości orzekanych kar i środków karnych.

Niniejsza monografia stanowi zmodyfikowaną i uaktualnioną wersję rozprawy doktorskiej obronionej przeze mnie w dniu 9 grudnia 2014 r. na Wydziale Prawa i Administracji Uniwersytetu Marii Curie-Skłodowskiej w Lublinie. Wybór jej tematu podyktowany był przede wszystkim moimi zainteresowaniami. Wyzwanie stanowiła także stosunkowa nowość problematyki przestępstw komputerowych, ograniczona liczba publikacji po-

święconych omawianym zagadnieniom, a wreszcie brak badań empirycznych, a nawet opracowań statystycznych[10].

W tym miejscu pragnę podziękować osobom, które miały niewątpliwy wpływ na ostateczny kształt pracy. Przede wszystkim Promotorowi – Panu prof. dr. hab. Markowi Mozgawie za sprawowaną opiekę merytoryczną oraz Recenzentom – Panu prof. dr. hab. Piotrowi Kardasowi oraz Panu prof. dr. hab. Jackowi Sobczakowi za cenne uwagi, a także Panu prof. dr. hab. Andrzejowi Siemaszce, wieloletniemu Dyrektorowi Instytutu Wymiaru Sprawiedliwości, który umożliwił mi przeprowadzenie badań empirycznych stanowiących niezwykle istotny element niniejszego opracowania.

Dziękuję również za przekazane uwagi i słowa zachęty autorowi recenzji wydawniczej Panu prof. dr. hab. Andrzejowi Adamskiemu.

[10] Z danych zgromadzonych przez organy Policji, umieszczonych na stronie Komendy Głównej Policji, trudno wyciągnąć miarodajne wnioski (zob. uwagi na ten temat w rozdziale ostatnim).

Rozdział 1
Hacking – zagadnienia ogólne

1.1. Uwagi wstępne

1.1.1. Zarys historii komputerów i sieci komputerowych

Gwałtowny rozwój sieci komputerowych, którego jednym z najważniejszych aspektów jest powstanie Internetu, miał miejsce w ciągu ostatnich 30 lat. Początkowo trudno było bowiem sobie wyobrazić, że postęp techniczny stanie się aż tak intensywny. Pierwszy komputer powstał już w latach 40. ubiegłego wieku w Stanach Zjednoczonych. Zajmował on 139 m^2, używał 17 tysięcy lamp próżniowych i wykonywał 1000 obliczeń na sekundę (dla porównania – obecnie przeciętny komputer osobisty wykonuje w ciągu sekundy kilkaset milionów operacji). Pierwszym „komercyjnym komputerem" był UNIVAC (*Universal Automatic Computer*) skonstruowany w 1951 r.[11] Na zakup komputerów produkowanych w latach 50. i 60. mogły sobie pozwolić instytucje rządowe oraz uczelnie. Przełom nastąpił w latach 70., kiedy na rynku pojawił się Altair 8800 dostępny dla przeciętnego obywatela w Stanach Zjednoczonych[12]. Następnie pojawiły się Atari, Commodore 64 i IBM PC. W latach 70. powstały też pierwsze sieci. Składały się one z głównego komputera (ang. *mainframe*) oraz połączonych z nim terminali, które korzystały z plików, programów i mocy obliczeniowej komputera *mainframe*. Bez niego były bezużyteczne. Wraz z pojawieniem się stosunkowo tanich komputerów osobistych zaistniała

[11] Szerzej B. Gates, *Droga ku przyszłości*, Warszawa 1997, s. 1–72. Por. R. Skubisz, *Internet – ku społeczeństwu przyszłości* (w:) R. Skubisz (red.), *Internet 2000*, Lublin 1999, s. 7–9; J.W. Wójcik, *Przestępstwa komputerowe*, cz. 1, *Fenomen cywilizacji*, Warszawa 1999, s. 12–14.

[12] B. Gates, *Droga...*, s. 17.

możliwość wyposażenia każdego pracownika w taki właśnie sprzęt, a nie tylko terminal. Jednocześnie jednak użytkownicy stracili możliwość korzystania z zasobów komputera głównego, a dane między sobą mogli wymieniać za pomocą fizycznych nośników (tzw. poczta *per pedes*). W celu rozwiązania tego problemu pod koniec lat 70. stworzono standard Ethernet umożliwiający łączenie ze sobą komputerów osobistych w sieć lokalną LAN (ang. *Local Area Network*). Obecnie jest to najpopularniejsza technologia stosowana w sieciach komputerowych[13].

W tym samym czasie zaczęły powstawać tzw. BBS-y[14], czyli sieci powstałe z komputerów połączonych ze sobą przy pomocy modemów i linii telefonicznych; rozwijał się też już ARPANet – „poprzednik" Internetu.

W 1957 r. w Stanach Zjednoczonych, w ramach Departamentu Obrony, powstała Agencja Zaawansowanych Projektów Badawczych (Advanced Research Project Agency)[15]. Pierwotnym celem ARPA była budowa sztucznego satelity. Szybko jednak Agencja zajęła się pracami nad rozwojem nowoczesnych technologii. Jednym z głównych zadań stało się utworzenie sieci komputerowej mającej połączyć uniwersytety i instytucje rządowe. Podstawowym założeniem, jakie przyświecało jej twórcom, było nadanie jej rozproszonego charakteru – skonstruowanie jej bez żadnego centralnego punktu, by nawet w przypadku zniszczenia lub uszkodzenia fragmentu jej struktury, pozostała część mogła funkcjonować. W związku z tym dane nią przekazywane miały być dzielone na pakiety i przesyłane niezależnie,

[13] D.L. Shinder, E. Tittel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, Gliwice 2004, s. 70–71.

[14] Najprostszy BBS to po prostu zwykły komputer osobisty, na którym zainstalowano odpowiednie oprogramowanie. Jego użytkownik udostępniał zasoby, umożliwiając korzystanie np. z poczty elektronicznej, grup dyskusyjnych, gier czy wymianę plików. Aby móc skorzystać z danego BBS-u, należało znać jego numer telefonu i po prostu „zadzwonić". Większość BBS-ów posiadała możliwość komunikowania się z innymi BBS-ami, co umożliwiało wymianę poczty i plików w skali świata. Bardzo szybko BBS-y zaczęły być używane do nielegalnych celów – udostępniano sobie programy hackerskie, rozpowszechniano pirackie oprogramowanie (głównie gry) oraz pornografię. Przykładowo – jak podaje A. Walczak-Żochowska – pierwszy serwis poświęcony w całości pornografii dziecięcej powstał już w 1982 r. (A. Walczak-Żochowska, *Internet a seksualne wykorzystywanie dzieci* (w:) P. Girdwoyń (red.), *Prawo wobec nowoczesnych technologii,* Warszawa 2008, s. 110). W czasach największego rozwoju liczba BBS-ów w samych Stanach Zjednoczonych wynosiła ponad 40.000. Obecnie ich znaczenie spadło praktycznie do zera, gdyż dostęp do Internetu stał się znacznie tańszy przy nieporównywalnie większych możliwościach. Por. P. Grabosky, R. Smith, *Crime in the Digital Age*: *Controlling Telecommunications and Cyberspace Illegalities*, Sydney 1998, s. 5–6; D.L. Shinder, E. Tittel, *Cyberprzestępczość...*, s. 72.

[15] Od 1972 r. Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności (Defence Advanced Research Project Agency).

nawet różnymi trasami, a po dotarciu do celu – składane w oparciu o informacje zawarte w ich nagłówkach (tzw. komutacja pakietów, ang. *packet switching*). Efektem podjętych prac był powstały w 1969 r. ARPANet[16].

W latach 70. pojawiła się poczta elektroniczna, pierwowzór dzisiejszego FTP (ang. *File Transfer Protocol* – protokół transferu plików), grupy dyskusyjne oraz gry dla wielu użytkowników. Cały czas jednak ARPANet ograniczał się zasięgiem do uczelni i instytucji rządowych. Na początku lat 80. do ARPANetu było podłączonych 5000 hostów[17], pod koniec dekady natomiast liczba ta wzrosła do 28.000. Niezwykle ważnym wydarzeniem na drodze budowania sieci otwartej (ang. *open-architecture network environment*) i zacierania granic między różnymi sieciami (proces ten nazywano *internetting*[18])[19] było uznanie w 1982 r. opracowanego w latach 70. protokołu TCP/IP[20] za wiodący standard w funkcjonowaniu sieci. W 1983 r. ARPANet został podzielony na dwie części – Milnet (sieć wojskowa) i NSFNet (sieć cywilna), z której wykształcił się dzisiejszy Internet. W 1987 r. powstał DNS (ang. *Domain Name System* – system nazw domen), który jest protokołem, usługą i siecią serwerów służących zamianie mnemonicznych nazw urządzeń sieciowych (zarówno serwerów, jak i pojedynczych komputerów) na adresy IP zrozumiałe dla urządzeń, które tworzą sieć (np. www.sejm.gov.pl na 194.41.12.17).

W 1992 r. zaczęła funkcjonować usługa *World Wide Web* (WWW). Dzięki zastosowaniu tzw. hiperlinków uczyniła ona Internet znacznie dostępniejszym, umożliwiając korzystanie z niego osobom nieposiadającym fachowych umiejętności. Czynnikiem dodatkowo ułatwiającym „surfowanie" było pojawienie się przeglądarek internetowych. Pierwszą był opracowany w 1993 r. Mosaic. Internet liczył wówczas już ponad milion hostów[21].

---

[16] P. Dawidziuk, B. Łącki, M.P. Stolarski, *Sieć Internet – znaczenie dla nowoczesnego państwa oraz problemy bezpieczeństwa* (w:) M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009, s. 42–43; D.L. Shinder, E. Tittel, *Cyberprzestępczość...*, s. 74–76.

[17] Termin ten można spotkać w dwóch znaczeniach – komputer nadrzędny, udostępniający swoje zasoby innym (czyli serwer), albo po prostu urządzenie podłączone do sieci, posiadające numer IP (np. pojedynczy komputer).

[18] Słowo „Internet" po raz pierwszy zostało użyte w 1974 r. przez V. Cerfa i B. Kahna w sporządzonym przez nich opracowaniu badawczym *A Protocol for Packet Network Interconnection*, dotyczącym protokołu TCP (D.J. Bem, *Tylko IP* (w:) D.J. Bem (red.), *Internet 2006*, Wrocław 2007, s. 7).

[19] K. Dobrzeniecki, *Lex Informatica*, Toruń 2008, s. 36.

[20] Protokoły sieciowe są to zbiory reguł określających sposoby komunikowania się w sieci. Zob. szerzej pkt 1.2.6.

[21] P. Dawidziuk, B. Łącki, M.P. Stolarski, *Sieć Internet...*, s. 42–43.

W 1995 r. rozpoczęły działalność serwis aukcyjny eBay oraz księgarnia Amazon. Rok później zaczął działać Google, najpopularniejsza obecnie wyszukiwarka internetowa. Od 1998 r. rozwijana jest technologia WAP (ang. *Wireless Application Protocol*), umożliwiająca korzystanie z Internetu przy pomocy telefonów komórkowych. W 1999 r. powstał pierwszy (istniejący zresztą do dziś) bank internetowy – First Internet Bank of Indiana (www.firstib.com). Pod koniec lat 90. pojawiają się pierwsze sieci i tzw. programy *peer-to-peer* (p2p – np. Gnutella, Napster, Kazaa, BitTorrent), umożliwiające użytkownikom Internetu wymianę plików na niespotykaną dotąd skalę. Od 2003 r. w Internecie obecny jest Skype – komunikator internetowy (IM – Instant Messenger) oparty na architekturze p2p[22]. W 2005 r. liczba użytkowników Internetu na świecie przekroczyła miliard, w 2007 r. wynosiła ok. 1,319 miliarda (co stanowiło wówczas 20% światowej populacji), a w 2010 r. – 1,6 miliarda[23].

Polska początkowo pozostawała na uboczu procesu tworzenia się i rozwoju Internetu[24]. Jako państwo socjalistyczne została objęta restrykcjami technologicznymi. Zniesiono je w latach 1990–1991. Pierwszym e-mailem przesłanym przez Internet z Polski była wiadomość z dnia 23 sierpnia 1991 r. (niezachowana niestety) wysłana do Hamburga. W 1992 r. powstał POLPAK – pierwsza polska sieć pakietowa. W 1994 r. pojawiły się listy dyskusyjne, a rok później – darmowe konta e-mail. Zaczęły też powstawać BBS-y (np. Bajtek BBS, CHIP BBS, UMCS Olimp BBS) oraz pierwsze strony internetowe[25].

[22] J. Gołaczyński, *Umowy elektroniczne w prawie prywatnym międzynarodowym*, Warszawa–Kraków 2007, s. 15; A. Kasprzak, K. Walkowiak, *Ewolucja sieci Internet* (w:) D.J. Bem (red.), *Internet 2008*, Wrocław 2009, s. 27.

[23] Por. K. Dobrzeniecki, *Lex Informatica...*, s. 38–39; K.M. Rogers, *The Internet and the Law*, Houndmills, Basingstoke–New York 2011, s. 3–4.

[24] Nie oznacza to oczywiście, że w dziedzinie informatyki panował w Polsce zastój. Wprost przeciwnie, mimo restrykcji tworzono przemysł komputerowy – w 1958 r. skonstruowano maszynę cyfrową XYZ, w 1963 r. podjęto seryjną produkcję komputerów UMC-1, a w 1964 r. – komputerów ODRA-1300. Zob. szerzej P. Sienkiewicz (w:) *Społeczeństwo informacyjne: krok naprzód, dwa kroki wstecz*, red. P. Sienkiewicz, J.S. Nowak, Katowice 2008, s. 15–23.

[25] J. Gołaczyński, *Umowy elektroniczne...*, s. 19–20.

1.1.2. Pojawienie się hackerów

O początkach hackingu można w zasadzie mówić już od momentu powstania pierwszych sieci telefonicznych, wtedy bowiem pojawili się tzw. phreakerzy (od ang. *phone freak* – „telefoniczny maniak"). Włamywali się oni do sieci telekomunikacyjnych, by móc nawiązywać darmowe połączenia. Inną grupą przestępców, którzy pojawili się w tym czasie, byli tzw. crackerzy (od ang. *crack* – łupać), którzy specjalizowali się w łamaniu zabezpieczeń systemów telekomunikacyjnych. Obecnie tego terminu używa się głównie w stosunku do „łamaczy" haseł i zabezpieczeń. Obie wyżej wskazane grupy można uznać za poprzedników dzisiejszych hackerów[26] (zresztą wielu z nich zaczynało właśnie w ten sposób swoją działalność). Początkowo termin „hacker" miał trochę inne znaczenie niż obecnie – oznaczał po prostu zdolnego programistę. Później, po zlaniu się w latach 70. subkultury hackerów z phreakerami, zaczął nabierać innego (bliższego dzisiejszemu) znaczenia – kogoś działającego w podziemiu, włamującego się do komputerów i sieci, często ze szlachetnych pobudek, a czasami po prostu dla zabawy i zdobycia sławy. Taki obraz w kulturze utrwaliły filmy (zwłaszcza *Gry wojenne* J. Badhama z 1983 r. czy *Hakerzy* I. Softleya z 1995 r.)[27]. Obecnie pod pojęciem „hacker" zwykle rozumie się osobę, która „sieje zamęt" w Internecie, czyli zarówno włamuje się do sieci komputerowych i komputerów, jak i działa w celu zakłócenia ich pracy[28]. W języku potocznym często określenie to używane jest dla generalnego określenia przestępców działających w Internecie, w tym internetowych oszustów. W związku z powyższym pojęcie „hacking" można rozumieć

[26] Termin „hacker" pochodzi od ang. *hack*, którego używali w latach 60. studenci Massachusetts Institute of Technology na określenie pomysłowych żartów przez nich płatanych (za przykład podaje się modyfikację panelu kontrolnego w windzie, w wyniku której po wciśnięciu przycisku odnoszącego się do wybranego numeru piętra winda jechała na zupełnie inne). Zob. S.W. Brenner, *Cybercrime and the Law. Challenges. Issues, and Outcomes*, Boston 2012, s. 16.

[27] Por. S. Bukowski, *Przestępstwo hackingu*, PS 2006, nr 4, s. 134–137; B. Fischer, *Przestępstwa komputerowe i ochrona informacji*, Kraków 2000, s. 53–58; D.L. Shinder, E. Tittel, *Cyberprzestępczość...*, s. 65–78; J.W. Wójcik, *Przestępstwa komputerowe*, cz. 1..., s. 187–189.

[28] Jednocześnie mamy do czynienia ze swego rodzaju paradoksem – nie ma już konieczności, by hacker, w takim rozumieniu, posiadał zaawansowane umiejętności jak jego poprzednik z wcześniejszych lat. Wystarczy, że pobierze z sieci odpowiedni program, który wszystkie czynności wykona za niego. Ukuty został nawet termin dla określenia takich osób – ang. *script kiddies* – czyli „dzieciaki skryptowe" (skrypt – program napisany w języku skryptowym, który wykonuje pewne działania wewnątrz innego programu – w uproszczeniu jest to niesamodzielny program, np. skrypty JavaScript na stronach WWW, makra w dokumentach MS Office).

na kilka sposobów: jako hacking *sensu stricto*, czyli zachowanie polegające na uzyskaniu dostępu do systemu informatycznego lub danych komputerowych, hacking *sensu largo*, jako wszelkie zamachy na bezpieczeństwo systemów i danych informatycznych (czyli również np. zakłócenie pracy systemu informatycznego, modyfikację lub zniszczenie danych komputerowych), oraz w znaczeniu najszerszym, potocznym – jako zbiorcze określenie praktycznie wszystkich przestępstw popełnianych w sieci (oczywiście z wyjątkiem np. rozpowszechniania pornografii czy naruszania praw autorskich). Przedmiotem niniejszego opracowania jest hacking *sensu largo*.

1.1.3. Sprzęt komputerowy

Przeważającą grupę komputerów korzystających z sieci stanowią komputery osobiste (PC – ang. *Personal Computer*). Bez względu na typ i zastosowanie komputera, składa się on z pewnych podstawowych elementów, są to:

1) płyta główna (ang. *Motherboard*) – jest to główna jednostka sterująca komputera, do której podłączone są dodatkowe komponenty (procesor, pamięć ROM, pamięć RAM, karty rozszerzeń, zasilacz itd.) oraz – za pośrednictwem tzw. portów – urządzenia wejścia/wyjścia i peryferyjne. Elementem, który łączy ze sobą i z procesorem poszczególne części, jest szyna (ang. *Bus*);
2) procesor (CPU – od ang. *Central Processing Unit* – jednostka centralna) – zintegrowany układ scalony wykonujący wszystkie operacje na danych. Może wykonywać różne zadania, korzystając z zaprogramowanych instrukcji (rozkazów);
3) pamięć – dane w komputerze przechowywane są w pamięci (w specjalnych chipach; nie należy mylić z pamięcią dyskową czy zewnętrzną). Wyróżniamy następujące rodzaje pamięci:
    a) pamięć operacyjna, czyli RAM (ang. *Random Access Memory* – pamięć o dostępie losowym; inaczej – pamięć o dostępie swobodnym) – przechowywane są w niej dane i instrukcje bieżących procesów; cechą charakterystyczną tej pamięci jest to, że w momencie wyłączenia zasilania dane w niej przechowywane są tracone;

b) pamięć ROM (ang. *Read Only Memory* – pamięć tylko do odczytu) – przechowywane w niej są programy, które muszą być stale dostępne, np. BIOS, czyli oprogramowanie płyty głównej;
c) pamięć *cache* – jest szybsza i wydajniejsza od pamięci RAM, procesor potrzebnych danych szuka wpierw w niej, dopiero później sięga do RAM;

4) urządzenia wejścia/wyjścia (urządzenia we/wy, urządzenia I/O) – służą do wprowadzania danych (np. klawiatura, skaner, myszka) lub ich „wyprowadzenia" (drukarka, monitor), mogą też pełnić obie te funkcje jednocześnie (np. karta sieciowa, modem). Urządzenia we/wy znajdujące się „poza obudową" nazywane są urządzeniami peryferyjnymi.

Do przechowywania i przenoszenia danych służą nośniki trwałe. Nazwa „trwałe" pochodzi od tego, że dane na tych nośnikach nie są tracone w momencie wyłączenia komputera. Podzielić je można na:

1) dyski twarde (HDD – ang. *hard disk drive*) – zbudowane są z okrągłych talerzy, ułożonych jeden nad drugim, na których dane zapisywane są z obu stron przez głowice elektromagnetyczne, które za pomocą impulsów elektromagnetycznych odpowiednio „magnesują" powierzchnię dysku. Ponadto coraz częściej (zwłaszcza w tzw. ultrabookach) spotyka się zamiast tradycyjnych dysków twardych dyski SSD (ang. s*olid-state drive*), działające na tej samej zasadzie co pamięci *flash*. Mają zwykle mniejszą pojemność niż klasyczne dyski twarde, ale są odporniejsze na czynniki zewnętrzne, a przede wszystkim – charakteryzuje je znacznie krótszy czas dostępu do danych[29];
2) przenośne nośniki danych – jak sama nazwa wskazuje, można je przenieść, czyli odłączyć od napędu (urządzenia służącego do zapisu lub odczytu danych; w przypadku dysków twardych napęd i nośnik to jedna struktura). Można wyróżnić następujące ich rodzaje:
   a) dyskietki (ang. *floppy*) – obecnie niespotykane; najpopularniejszymi były 3,5 calowe o pojemności 1,44 MB; zbudowane są z pokrytego materiałem magnetycznym krążka, umieszczonego w plastikowej obudowie;
   b) płyty CD i DVD (ang. *Compact Disk*, *Digital Versatile Disc* lub *Digital Video Disc*) – plastikowe dyski, pokryte materiałem metalicznym;

[29] Istnieją jeszcze tzw. dyski hybrydowe, niezbyt ściśle nazywane też SSHD (od ang. *Solid-state hybrid drive*), składające się z „klasycznego" dysku twardego i modułu pamięci flash, dzięki czemu łączą zalety obu technologii, zapewniając jednocześnie dużą pojemność oraz prędkość zapisu i odczytu danych. Zob. szerzej https://en.wikipedia.org/wiki/Hybrid_drive, data wejścia 19.10.2015 r.

do odczytywania i zapisywania danych służy laser, stąd nazywane są nośnikami optycznymi;

c) pamięć *flash* (ang. *flash memory*) – układy scalone przechowujące dane, występujące obecnie w dwóch zasadniczych postaciach: jako pamięci USB (tzw. pendrive'y) oraz karty pamięci;

d) nośniki magnetooptyczne (MO).

Najpowszechniejszym urządzeniem służącym do komunikacji komputera z siecią jest karta sieciowa (NIC – *Network Interface Card*). W zasadzie wszystkie nowe komputery (zarówno przenośne, jak i stacjonarne) standardowo wyposażone są we wbudowaną w płytę główną kartę sieciową Ethernet. Oczywiście kartę można zamontować w gnieździe rozszerzeń (PCI) płyty głównej lub podłączyć przez port USB. Kabel do niej podłączony jest poprzez gniazdo (najczęściej RJ-45). Ponadto do łączenia się z siecią mogą służyć modemy (w przypadku połączenia przez sieć telefoniczną).

Karta sieciowa, modem czy fizyczne interfejsy routera (porty) są przykładami tzw. interfejsów sieciowych. Pojęciem tym określa się wszystkie fizyczne urządzenia podłączone do sieci[30].

1.2. Ogólne informacje o sieciach komputerowych

1.2.1. Kodowanie

Na wstępie kilka słów należy poświęcić problematyce kodowania danych komputerowych. Dane zapisywane są w języku binarnym (zwanym też językiem maszynowym lub kodem maszynowym) w systemie dwójkowym, czyli w postaci ciągów „0" i „1". Każda cyfra jest nazywana bitem. Większą jednostką jest bajt (ang. *byte*), na który składa się 8 bitów[31]. Re-

[30] S. Knott, W. Odom, *Akademia sieci Cisco. CCNA semestr I. Podstawy działania sieci*, Warszawa 2007, s. 621.

[31] Przy okazji należy zwrócić uwagę, że w informatyce stosowane są zarówno bity, jak i bajty. Te pierwsze używane są przy określaniu szybkości transferu danych (bity/s), natomiast bajty (B) – do określenia wielkości pamięci. Ponadto należy pamiętać, iż przy określaniu wielokrotności tych jednostek stosuje się przedrostki dwójkowe (binarne), które mają identyczne nazwy i skróty jak stosowane w układzie SI („kilo", „Mega", Giga", choć czasami jako skrót „kilo" używa się litery „K"), ale mnożnik dziesiętny (10^3) zastąpiony jest binarnym (2^{10}), stąd 1 kb = 1024 b (2^{10} b), 1 Mb = 1024 kb = 1048576 b itd. Podobnie jest w przypadku bajtów, z tymże zarówno w skrócie nazwy tej jednostki, jak i w przedrostkach, stosuje się „wielkie litery" (1 KB = 1024 B, 1 MB = 1024 KB itd.)

prezentuje on jeden znak (litera alfabetu, cyfra lub symbol). Zastosowanie języka binarnego wynika z faktu, że ten najłatwiej zamienić na impulsy energetyczne (w drodze kodowania). Istnieje wiele metod kodowania, zależnych od sposobu reprezentowania „0" i „1". Jedną z popularniejszych jest schemat *Manchester*, w którym „1" reprezentowana jest przez niskie napięcie w pierwszej połowie bitu i wysokie w drugiej. Przeciwny sygnał oznacza „0"[32]. Jest to praktyczniejsze niż definiowanie wartości logicznych (tj. „0" i „1") jako określonych poziomów napięcia (np. +5 V dla „1"), ponieważ uchwycenie samych zmian poziomu sygnału jest po prostu łatwiejsze[33].

Oczywiście nikt nie programuje w języku binarnym, tylko w którymś z tzw. języków wyższego poziomu. Językiem wyższym od binarnego jest asembler, pozwalający na używanie skrótów i nazw, tłumaczonych na język binarny przez program, który również nazywa się asembler. Najczęściej programiści korzystają z języków wysokiego poziomu (BASIC, C++), które podobne są do języka „ludzkiego". Napisany program jest automatycznie tłumaczony na język binarny.

Dane zazwyczaj nie są przesyłane w całości – ze względu na wielkość muszą być dzielone na pakiety, które przesyłane są niezależnie, często różnymi trasami. Po dotarciu do komputera docelowego są „składane" w oparciu o informacje zawarte w nagłówkach pakietów.

1.2.2. Składniki sieci

Sieć komputerowa stanowi bardzo szerokie pojęcie. W jego zakresie mieści się zarówno sieć składająca się z dwóch połączonych komputerów, jak i sieć o zasięgu globalnym, taka jak np. Internet. Generalnie można przyjąć, iż pod pojęciem sieci komputerowej należy rozumieć kombinację czterech grup elementów:

1) sprzętu komputerowego;
2) okablowania (medium sieciowego);
3) urządzeń sieciowych;
4) oprogramowania komputerowego (elementów programowych)

[32] D.L. Shinder, E. Tittel, *Cyberprzestępczość...*, s. 203–204.

[33] Zob. szerzej D.E. Comer, *Sieci komputerowe i intersieci. Kompendium wiedzy każdego administratora,* Gliwice 2012, s. 134–135.

– używanych łącznie w celu umożliwienia komputerom wzajemnego komunikowania się[34].

1.2.2.1. Medium sieciowe

Komputery, by móc się komunikować, potrzebują wspólnego medium. Może do tego służyć kabel miedziany, światłowód lub fale elektromagnetyczne (np. światło, podczerwień, fale radiowe). Poniżej zostaną omówione skrótowo najpopularniejsze rodzaje mediów, zaczynając od zapewniających łączność „przewodową". W pierwszej kolejności należy wskazać oczywiście kable miedziane, a mianowicie:

1) kabel koncentryczny (kabel współosiowy, ang. *coaxial cable)*, zbudowany z przewodu miedzianego, którym przesyłane są impulsy elektryczne, otoczony osłoną z tworzywa (izolacja wewnętrzna) oraz tzw. ekranem – oplotem (metalową siatką) lub (w kablach półsztywnych) tuleją, pełniących funkcję ekranującą, zatopiony zwykle w powłoce z PCV. Obecnie rzadko stosowany w sieciach komputerowych. Ponadto służy do łączenia anten, do połączeń AV oraz spotykany jest w sieciach kablowych. Kable koncentryczne dzielimy wg ich impedancji falowej. W sieciach komputerowych stosowano dwa ich rodzaje:
   a) 10BASE5 (tzw. „gruby Ethernet", ang. *Thicknet*) – jest to pierwsze medium używane przez sieci Ethernet (od roku 1980) – gruby kabel (średnica 0,5 cala) o impedancji 50 Ω. Maksymalna odległość między stacjami wynosiła 500 m. Pracował z przepustowością 10 Mb/s;
   b) 10BASE2 (tzw. „cienki Ethernet", ang. *Thinnet*) – od wyżej wskazanego różnił się przede wszystkim średnicą – 0,25 cala oraz maksymalną odległością między stacjami – 185 m.

W sieciach opartych na kablu koncentrycznym używano końcówek BNC (ang. *British Naval Connector)*[35];

2) tzw. skrętki, z których najprostsza to skrętka nieekranowana (kabel skrętkowy nieekranowany, ang. *Unshielded Twisted Pair,* UTP), składająca się z ośmiu przewodów w różnobarwnych izolacjach, skręconych w cztery pary (ma to na celu niwelowanie zakłóceń elektromagnetycz-

[34] S. Knott, W. Odom, *Akademia sieci...*, s. 31.
[35] K. Krysiak, *Sieci komputerowe. Kompendium,* Gliwice 2005, s. 38–40.

nych oraz zakłóceń wzajemnych). W miejscach, gdzie występują zakłócenia elektromagnetyczne EMI (ang. *electromagnetic interference)* oraz radiowe RFI (ang. *radio frequency interference*), znajdują zastosowanie kable skrętkowe ekranowane różniące się od skrętki nieekranowanej metaliczną osłoną, mającą na celu redukować zakłócenia (czyli ekranem). Przykładowo wskazać można skrętkę ekranowaną siatką (ang. *Shielded Twisted Pair, STP)*, folią (ang. *Foiled Twisted Pair*), folią i siatką (SFTP) oraz podwójnie ekranowaną (SSTP).Wszystkie skrętki korzystają ze złącza RJ45 (*Registered Jack – type 45*)[36];

3) kable energetyczne – można je w zasadzie wykorzystywać do przesyłania danych (tzw. technologia PLC – *Power Line Communication*), jednak z uwagi na brak ochrony przed szumami zakłócającymi nie nadają się do transmisji na większe odległości[37].

Znacznie większą szybkość transmisji – od wyżej omówionych „klasycznych" kabli miedzianych – zapewniają kable światłowodowe (zaliczane też – obok fal podczerwonych oraz lasera – do mediów optycznych), zbudowane z włókien szklanych lub z tworzywa sztucznego, otoczonych plastikową osłoną. U podstaw techniki światłowodowej leży zjawisko całkowitego wewnętrznego odbicia fali świetlnej na granicy dwóch ośrodków o różnym współczynniku załamania. W technologii światłowodowej bity są zamieniane na impulsy świetlne. Na jednym końcu kabla znajduje się źródło światła w postaci lasera lub diody LED (ang. *Light Emitting Diode*), na drugim natomiast – fotodetektor odbierający docierające do niego światło. Zwykle pojedyncze włókno służy do transmisji danych w jednym kierunku. Łącza światłowodowe zapewniają dużą przepustowość oraz szybkość przesyłania danych również na dalsze odległości, dlatego są zwykle stosowane do budowy szkieletu sieci. W związku ze spadkiem ich ceny oraz kosztów instalacji są używane nie tylko w rozległych sieciach WAN, ale – coraz powszechniej – również w sieciach lokalnych LAN. Kable światłowodowe są w pełni dielektryczne, a zatem są odporne na zakłócenia elektromagnetyczne. Światłowód zbudowany jest z rdzenia, zwykle szklanego, otoczonego płaszczem załamującym światło (powoduje jego odbicie, tak by nie wydostało się poza rdzeń), które z kolei znajdują się w otulinie, tzw. płaszczu ochronnym, z tworzywa zabezpieczającego przed przerwaniem lub złamaniem. Dalej znajduje się przędza poliamidowa, umożli-

[36] K. Gromaszek, W. Wójcik (red.), *Sieci komputerowe*, Lublin 2011, s. 23–25.
[37] Zob. szerzej K. Krysiak, *Sieci komputerowe...*, s. 384–387.

wiająca zginanie światłowodu, oraz osłona zewnętrzna. Kable światłowodowe nie mogą być zginane pod dowolnym kątem, ale mogą być układane w łuki o średnicy mniejszej niż 5 cm. Wyróżnia się:

1) światłowody wielomodowe, w których źródłem światła jest dioda elektroluminescencyjna LED, przesyłające wiele modów (fal) o różnej długości, co powoduje „rozmycie" impulsu wyjściowego i ogranicza szybkość lub odległość transmisji;
2) światłowody jednomodowe, w których źródłem światła jest laser, będące efektywniejszymi od wyżej wskazanych światłowodów wielomodowych (pozwalając transmitować dane na odległość 100 km bez wzmacniacza) oraz droższymi (ze względu na wysoki koszt interfejsów przyłączeniowych)[38].

Komunikacja bezprzewodowa (ang. *wireless*) opiera się na wykorzystaniu fal elektromagnetycznych o różnej długości:

1) IrDA (ang. *Infrared Data Association*) – technologia przekazywania danych za pośrednictwem podczerwieni. Jako źródło promieniowania fal elektromagnetycznych wykorzystuje się diody LED lub diody laserowe. Zasada działania jest identyczna, jak w przypadku np. pilotów do sprzętu RTV. Fale podczerwone rozchodzą się szybko, mogą się odbijać od gładkich, twardych powierzchni. Technologia IrDA weszła na rynek w 1993 r., z założenia miała służyć do zestawiania połączeń zarówno międzybudynkowych, jak i wewnątrz pomieszczeń. Jej zaletą był brak wymogu licencji, jak to ma miejsce przy połączeniach przy użyciu fal radiowych. Z uwagi jednak m.in. na małą odporność na warunki atmosferyczne, niewielki zasięg (do kilku metrów) oraz wymóg, by nadajnik i odbiornik bezpośrednio „widziały się", zastosowanie tej technologii ograniczyło się do pomieszczeń, głównie do komunikacji między urządzeniami peryferyjnymi a komputerem. W końcu została ona wyparta przez *Bluetooth*[39];
2) w podobny sposób, jak fale podczerwone w przypadku komunikacji IrDA, można wykorzystać laser. W tym wypadku jednak nadajnik i odbiornik muszą być niezwykle precyzyjnie wycelowane w siebie (wiązka laserowa jest bardzo cienka). Natomiast przewaga technologii lasero-

[38] D.E. Comer, *Sieci komputerowe...*, s. 146–149; K. Gromaszek, W. Wójcik (red.), *Sieci komputerowe...*, s. 26–27.

[39] D.E. Comer, *Sieci komputerowe...*, s. 150 i 301; K. Krysiak, *Sieci komputerowe...*, s. 123–124.

wej nad IrDA polega przede wszystkim na nieporównywalnie większym zasięgu[40];

3) *Bluetooth* – standard komunikacji znajdujący zastosowanie głównie do przesyłania danych między różnymi urządzeniami lub urządzeniami a komputerem. Obejmuje trzy klasy mocy nadawczej: o zasięgu 100, 10 oraz 1 metra w otwartej przestrzeni. Najczęściej spotykaną klasą jest ta druga. Technologia korzysta z fal radiowych o częstotliwości 2,4 GHz[41];
4) bezprzewodowe sieci lokalne WLAN (ang. *Wireless Local Area Network*), zwykle stanowią „uzupełnienie" sieci lokalnych – są stosowane tam, gdzie użycie kabli jest niemożliwe lub nieopłacalne. Do przesyłania danych wykorzystywane są fale radiowe (mikrofale) o częstotliwości 2,4 GHz lub 5 GHz (w zależności od standardu). Sieć WLAN składa się z trzech podstawowych elementów: punktu dostępowego (nazywanego też stacją bazową), komponentu przyłączeniowego (np. switcha lub routera – zob. pkt 1.2.2) oraz stacji bezprzewodowych (poszczególnych hostów, tzw. węzłów bezprzewodowych). Mogą funkcjonować jako sieci infrastrukturalne (ang. *infrastructure*), w których stacje bezprzewodowe wymieniają dane jedynie z punktami dostępowymi, pośredniczącymi w ich przekazywaniu oraz *ad hoc*, w których poszczególne stacje komunikują się ze sobą bezpośrednio. W budynkach, z uwagi na przeszkody w postaci sufitów i ścian, zasięg wynosi ok. 50 m. Natomiast w otwartej przestrzeni – pod warunkiem braku przeszkód w postaci np. drzew – nawet do kilku kilometrów. Jako synonim WLAN używane jest często pojęcie Wi-Fi (skrót od ang. *Wireless Fidelity*), oznaczające w rzeczywistości zestaw standardów stworzonych do budowy sieci bezprzewodowych. W interfejsy Wi-Fi wyposażone są różnego rodzaju urządzenia (komputery, telefony komórkowe, urządzenia peryferyjne), które pozwalają w prosty sposób zapewnić im dostęp do zasobów sieci komputerowej[42];
5) sieci komórkowe – systemy komórkowe zostały opracowane przede wszystkim w celu zapewnienia połączeń głosowych. Sieć składa się z komórek (ang. *cells*) obejmujących obszar najczęściej o kształcie zbliżonym do okręgu, choć optymalnym rozwiązaniem jest, gdy komórki mają kształt sześcioboków, będących w zasięgu jednej stacji bazowej.

[40] D.E. Comer, *Sieci komputerowe...*, s. 150–151.

[41] Tamże, s. 288, 299; K. Krysiak, *Sieci komputerowe...*, s. 123–124.

[42] D.E. Comer, *Sieci komputerowe...*, s. 292–293; K. Gromaszek, W. Wójcik (red.), *Sieci komputerowe...*, s. 27; K. Krysiak, *Sieci komputerowe...*, s. 123.

Stacjami bazowymi zarządza centrala sieci komórkowej (ang. *Mobile Switching Center*). Jej zadaniem jest śledzenie urządzenia użytkownika i przekazywanie jego obsługi do kolejnego nadajnika, w zasięgu którego – w związku z przemieszczaniem – się on znajdzie. Jeżeli abonent przemieszcza się po większym obszarze, w przełączanie mogą być zaangażowane dwie centrale. Możliwość transmisji danych za pomocą sieci komórkowych pojawiła się w tzw. systemach komórkowych drugiej generacji (2G), dzięki technologiom GPRS (ang. *General Packet Radio Service*) oraz EDGE (ang. *Enhanced Data Rates for GSM Evolution*). W systemach trzeciej generacji (3G), w Polsce opartych na standardzie UMTS (ang. *Universal Mobile Telecommunications System*), przesyłanie danych umożliwiają technologie WCDMA (*Wideband Code Division Multiple Access*) oraz HSDPA (ang. *High Speed Downlink Packet Access*). Obecnie rozwijane są standardy czwartej generacji: *Long Term Evolution* (LTE), *Evolved High Speed Packet Access* (HSPA+) oraz *Ultra Mobile Broadband* (UMB)[43];

6) łączność satelitarna – pozwala na uzyskanie dostępu do Internetu w najdalszych zakątkach świata. Do korzystania z niej konieczne jest posiadanie anteny parabolicznej („talerzowej")[44], dekodera i oczywiście odpowiedniego odbiornika (np. komputera, telewizora). Dane w ten sposób są zwykle przyjmowane, natomiast ich wysyłanie odbywa się inną drogą. Istnieją również systemy dwukierunkowe, w których cała komunikacja odbywa się przez satelitę[45].

1.2.2.2. Urządzenia sieciowe

Pod pojęciem „urządzenia sieciowe" (ang. *networking devices*) rozumie się urządzenia komputerowe służące tworzeniu sieci. Są to elementy aktywne, w odróżnieniu od pasywnych, czyli okablowania. Ze względu na wielkie zróżnicowanie sieci (od małych, łączących dwa komputery, do rozległych, łączących znaczną liczbę komputerów na wielkich obszarach) istnieje bardzo wiele rodzajów urządzeń służących do ich obsługi. O urzą-

[43] D.E. Comer, *Sieci komputerowe...*, s. 301–306.

[44] Innym, rzadziej spotykanym typem anteny, jest antena panelowa (potocznie nazywana „płaską"). Zob. szerzej https://pl.wikipedia.org/wiki/Antena_panelowa, data wejścia 19.10.2015 r.

[45] D.E. Comer, *Sieci komputerowe...*, s. 306–307; K. Gromaszek, W. Wójcik (red.), *Sieci komputerowe...*, s. 27.

dzeniach zapewniających dostęp do sieci była mowa w poprzednim rozdziale (zob. pkt 1.1.3). W tym miejscu zostaną omówione te, które służą do budowy struktury sieci, a także łączenia ich w większe zespoły oraz dzielenia na mniejsze jednostki (segmenty; podział ten jest jedynie fizyczny – logicznie sieć stanowi całość) w celu zmniejszenia obciążenia sieci poprzez zmniejszenie ruchu sieciowego. Istnieje kilka rodzajów takich urządzeń[46]:

1) repeatery (regeneratory, wzmacniaki, retransmitery) – proste, zwykle dwuportowe urządzenia, które wzmacniają i naprawiają zniekształcony sygnał w sieci, łączą segmenty sieci o tej samej architekturze, używające tych samych protokołów i technik transmisyjnych, ale mogą łączyć segmenty sieci o różnych mediach transmisyjnych (np. skrętka i kabel koncentryczny). Umożliwiają one zwiększenie zasięgu sieci (np. maksymalna długość kabla 10BASE2 wynosi 185 metrów, możliwe jest jednak połączenie kilku takich kabli wzmacniakami, co zwielokrotnia zasięg sieci). Nie są „inteligentnymi urządzeniami" – wzmacniają wszystko, co otrzymają, nie odróżniając właściwego sygnału od szumów. Obecnie są rzadko spotykane, gdyż ich funkcje z powodzeniem pełnią koncentratory, przełączniki, mosty lub routery, które regenerują sygnał w każdym porcie;
2) koncentratory (*hubs*) – to urządzenia wieloportowe, które poza łączeniem segmentów sieci (tzw. koncentratory pasywne – jedynie łączą kable), mogą wykonywać dodatkowe zadania (np. koncentratory aktywne – wzmacniają sygnał, stąd czasami nazywane wieloportowymi wzmacniakami, a tzw. *smart hubs* mogą monitorować transmisję). Ponieważ przesyłają sygnały elektryczne z jednego portu (gniazda) na wszystkie pozostałe, transmitowane dane trafiają do wszystkich komputerów do nich podłączonych. Obecnie rzadko spotykane – zostały wyparte przez przełączniki;
3) mosty (ang. *bridges*) – dwuportowe urządzenia działające w warstwie łącza danych modelu OSI i łączące segmenty sieci w całość. Są to urządzenia inteligentniejsze od koncentratorów – filtrują przesyłane dane, kierując je na podstawie adresów MAC do konkretnych hostów na podstawie tzw. tablic mostowania (ang. *bridging table*);

[46] D.E. Comer, *Sieci komputerowe...*, 315–320; K. Gromaszek, W. Wójcik (red.), *Sieci komputerowe...*, s. 9–10, 73–79; K. Krysiak, *Sieci komputerowe...*, s. 110–122; D.L. Shinder, E. Tittel, *Cyberprzestępczość...*, s. 221–227.

4) przełączniki (ang. *switches*) – podobnie jak mosty (poniekąd są one wieloportowymi mostami, wyposażonymi jednak w wyspecjalizowane układy scalone – tzw. ASIC, ang. *Application Specific Integrated Circuit*, dzięki temu przy mniejszych gabarytach mogą o wiele szybciej obsługiwać większy ruch sieciowy) łączą segmenty sieci. Ponadto umożliwiają tworzenie wirtualnych sieci lokalnych (VLAN – ang. *Virtual Local Area Network*) – sieci urządzeń wydzielonych logicznie w ramach innej większej sieci fizycznej. Urządzenia tworzące sieć VLAN, niezależnie od swojej fizycznej lokalizacji (mogą znajdować się w różnych segmentach sieci), mogą się ze sobą komunikować, tak jakby były w jednej wspólnej sieci lokalnej. Komunikacja między sieciami wirtualnymi może następować jedynie z wykorzystaniem urządzeń do kierowania ruchem na poziomie warstwy 3. modelu OSI, czyli routerów;
5) router jest wieloportowym urządzeniem służącym do łączenia kilku (co najmniej dwóch) różnych sieci lub logicznej segmentacji sieci (dzielenia na podsieci). Może pełnić również funkcje mostu. Routery umożliwiają również fizyczną segmentację sieci. Przede wszystkim wykonują działania związane z routingiem (pośredniczeniem w przesyłaniu danych między hostami znajdującymi się w różnych sieciach; szerzej na ten temat zob. pkt 1.2.7). Mogą to być specjalne urządzenia, ale ich funkcje mogą pełnić również zwykłe komputery mające odpowiednie oprogramowanie. Ponadto routery mogą filtrować pakiety i pełnić rolę firewalla. Pierwsze routery nazywano również bramami (ang. *gateways*). Obecnie termin ten używany jest w stosunku do różnych urządzeń, w szczególności łączących sieci rozległe WAN oraz lokalne LAN. Rolę tę pełnią często routery.

Urządzeniami, które nie służą do łączenia lub dzielenia sieci, ale często są montowane w jej ramach, są wspomniane wyżej zapory ogniowe (ang. *firewall*). Firewall jest specjalnym urządzeniem, którego zadaniem jest zapewnienie ochrony przed zagrożeniami z zewnątrz sieci, przede wszystkim poprzez filtrowanie pakietów – zwykle na kilku poziomach – w celu zablokowania potencjalnie niebezpiecznych. Jeżeli firewall wyposażony został w odpowiedni system, wykrywa określone ataki i podejmuje odpowiednie, zdefiniowane z góry działania. Jego funkcje może też pełnić router lub zwykły komputer po zainstalowaniu odpowiedniego oprogramo-

wania. Nazwa *firewall* oznacza również aplikację w komputerze osobistym, chroniącą go przed niebezpieczeństwami z sieci[47].

1.2.2.3. Oprogramowanie

Bez elementów programowych, sieć komputerowa, nawet zawierająca wszystkie pozostałe zespolone ze sobą elementy, będzie „martwa". To oprogramowanie „dostarcza komputerowi motywacji i powodów, dla których komputer próbuje się skomunikować z siecią"[48]. Należy wskazać w tym miejscu: sterowniki urządzeń (oprogramowanie *firmware*) odpowiadające za ich funkcjonowanie oraz oprogramowanie komunikacyjne, które wykorzystując możliwości przesyłania danych – stworzone przez protokoły sieciowe i sterowniki urządzeń – umożliwia korzystanie z usług sieciowych (takich jak np. FTP, czyli *File Transfer Protocol* – przesyłanie plików, czy WWW, czyli *World Wide Web* – przeglądanie stron internetowych). Usługi sieciowe wywoływane przez użytkowników są bowiem udostępniane przez odpowiednie programy – aplikacja zainstalowana na jednym komputerze (pełniącym rolę klienta) komunikuje się z aplikacją na innym komputerze (pełniącym rolę serwera). Przykładami programów komunikacyjnych są zatem programy do przesyłania plików, programy pocztowe służące do korzystania z poczty elektronicznej, a przede wszystkim tzw. przeglądarki internetowe (Internet Explorer, Mozilla Firefox, Opera, Chrome) korzystające z protokołu HTTP (ang. *HyperText Transfer Protocol*), umożliwiające pobieranie danych (stron internetowych) z serwera[49].

1.2.2.4. Metody dostępu do medium sieciowego

Omawiając zagadnienia dotyczące urządzeń sieciowych oraz medium sieciowego w sieciach LAN, warto odnieść się do kwestii sposobu dostępu do niego. Wyróżnia się trzy zasadnicze metody dostępu do medium

[47] Zob. D.L. Shinder, E. Tittel, *Cyberprzestępczość...*, s. 368–371; J. Muszyński (w:) *Vademecum teleinformatyka III*, red. T. Janoś, Warszawa 2004, s. 206–207.

[48] S. Knott, W. Odom, *Akademia sieci...*, s. 31.

[49] D.E. Comer, *Sieci komputerowe...*, s. 31; K. Gromaszek, W. Wójcik (red.), *Sieci komputerowe...*, s. 10; S. Knott, W. Odom, *Akademia sieci...*, s. 54–55.

(czwarta z omówionych niżej metod stanowi w rzeczywistości modyfikację pozostałych)[50]:

1) rywalizacji (współzawodnictwa, czyli „kto pierwszy, ten lepszy") – wszystkie urządzenia konkurujące ze sobą o dostępne pasmo szerokości tworzą tzw. domenę kolizji. Współzawodnictwo jest dość prostym sposobem regulowania dostępu, gdyż rozwiązanie to nie przewiduje żadnych scentralizowanych mechanizmów regulacyjnych. Zamiast tego każde urządzenie przyłączone do sieci przyjmuje na siebie ciężar samodzielnego przeprowadzenia transmisji. Za każdym razem, kiedy urządzenie chce przesyłać dane, musi sprawdzić, czy kanał transmisyjny jest wolny czy też nie. W tym drugim wypadku musi odczekać określony przedział czasu i ponownie podjąć próbę wysłania danych. Protokoły typu CSMA (ang. *Carrier Sense Multiple Access* – wielodostęp z rozpoznaniem stanu kanału) wykorzystują informacje uzyskane poprzez śledzenie stanu kanału. Każda transmisja poprzedzona jest nasłuchiwaniem i tylko w przypadku stwierdzenia wolnego łącza dane są wysyłane. W przypadku wystąpienia kolizji, stacja nadająca rezygnuje z transmisji i dokonuje ponownej próby po upływie losowo określonego czasu;
2) korzystania z tokenu – jest to metoda charakterystyczna dla sieci LAN o topologii pierścienia. Token (żeton) jest krążącym w sieci sygnałem, sterującym dostępem do niej, i decydującym, który komputer w danym momencie może przesyłać dane. Token jest przesyłany w jednym kierunku do kolejnych urządzeń wchodzących w skład pierścienia. Uznawany jest przez wszystkie urządzenia za element decydujący o dostępie do nośnika. Aby przesłać dane, urządzenie musi znajdować się w posiadaniu tokenu. W przeciwnym wypadku musi poczekać, aż otrzyma go od sąsiada poprzedzającego go w pierścieniu;
3) priorytetu żądań (tzw. odpytywanie cykliczne) – jest to metoda cyklicznego przyznawania prawa dostępu, w której centralny koncentrator regularnie sprawdza stan przyłączonych do niego portów w celu określenia, które z nich zgłaszają żądania transmisji. Po rozpoznaniu zgłoszenia koncentrator określa jego priorytet (normalny lub wysoki). Powodem wprowadzania priorytetów jest potrzeba umożliwienia

[50] K. Gromaszek, W. Wójcik (red.), *Sieci komputerowe...*, s. 40–44; D.L. Shinder, E. Tittel, *Cyberprzestępczość...*, s. 211.

uprzywilejowanego dostępu do nośnika procesom, które muszą być obsłużone w określonym czasie;
4) przełączania, która nie jest w istocie metodą dostępu, ale stanowi modyfikację wyżej omówionych metod, coraz częściej stosowaną w celu zwiększenia sprawności i wydajności sieci LAN. Sprowadza się bowiem do modyfikacji dotychczasowych zasad dotyczących topologii i metodologii dostępu do sieci LAN. Polega na „uczeniu się" przez przełącznik (ang. *switch*) adresów i „zapamiętywaniu" ich w wewnętrznej tabeli, tworząc między nadawcą i odbiorcą ścieżki przełączania, którymi następnie przesyłane są dane. Każdy port oraz urządzenie, które jest do niego przyłączone, ma własną szerokość pasma.

1.2.3. Podział sieci komputerowych

1.2.3.1. Podział sieci ze względu na zasięg

Sieci można klasyfikować przyjmując różne kryteria. Stosując kryterium zasięgu, najczęściej wyróżnia się[51]:
1) sieci osobiste (PAN – ang. *Personal Area Network*) – jest to sieć lokalna o zasięgu do ok. 10 metrów, odnosząca się do przestrzeni osobistej jednej osoby, zapewniająca komunikację między używanymi przez nią urządzeniami (np. komputer, drukarka z interfejsem bezprzewodowym, smartfon);
2) sieci lokalne (LAN – ang. *Local Area Network*) – obejmują niewielki obszar: jeden, ewentualnie kilka blisko siebie położonych budynków, używając zazwyczaj „własnych" mediów (np. własnego okablowania), bez konieczności korzystania z infrastruktury sieci publicznej. Sieci komputerowe LAN składają się ze stacji sieciowych (komputerów, serwerów, zwanych ogólnie hostami), połączonych okablowaniem strukturalnym z wykorzystaniem aktywnych urządzeń sieciowych;
3) WAN (ang. *Wide Area Network*) – sieci rozległe; korzystają zazwyczaj z linii telefonicznych, łącz dedykowanych lub satelitarnych;
4) MAN (ang. *Metropolitan Area Network*) – obejmują obszar miasta[52];

[51] K. Gromaszek, W. Wójcik (red.), *Sieci komputerowe...*, s. 10–11. Zob. szerzej S. Knott, W. Odom, *Akademia sieci...*, s. 116–122.

[52] Z kwestią rozległości sieci związane są technologie zastosowane przy ich tworzeniu. Im sieć większa, tym oczywiście kosztowniejsza. W praktyce rzadko spotyka się technologie sieci MAN.

5) sieci pamięci masowych (SAN – ang. *Storage Area Network*) – zapewniają dostęp do pamięci masowych (np. pojemnych dysków twardych), zawierających np. dane o towarach znajdujących się w ofercie dużego sklepu internetowego, takiego jak Amazon.com;
6) prywatne sieci wirtualne (VPN – ang. *Virtual Private Network*) – stanowią sposób komunikacji polegający na tworzeniu, przy pomocy takich protokołów, jak PPTP (ang. *Point-to-Point Tunneling Protocol*), IPSec (ang. *IP Security Protocol*) czy IKE (ang. *Internet Key Exchange*), prywatnych, szyfrowanych połączeń. Zwykle VPN tworzą komputery podłączone do Internetu, dzięki czemu hosty mogą znajdować się w dowolnej części świata. Możliwe jest tworzenie VPN również w ramach sieci nieposiadających połączenia z Internetem (konieczne jest wtedy zawarcie umowy z dostawcą usług telekomunikacyjnych, który w celu utworzenia VPN wydziela ze „swojej sieci" połączenie pomiędzy routerami granicznymi sieci LAN lub hostami, które mają być połączone w VPN). Rozwiązanie to znajduje zastosowanie przede wszystkim w sieciach korporacyjnych, używanych przez przedsiębiorstwa w celu zapewnienia bezpiecznych połączeń np. między sieciami komputerowymi głównej siedziby a sieciami odległych oddziałów (intranet), czy umożliwiających zdalny dostęp do tej sieci pracownikom z ich komputerów w domu lub podczas podróży (dostępowa sieć VPN) albo pomiędzy sieciami (komputerami) należącymi do różnych przedsiębiorstw (np. sprzedawcy i jego dostawcy)[53].

1.2.3.2. Podział sieci ze względu na sposób konfiguracji

Zagadnieniem niejako z pogranicza problematyki budowy sieci i oprogramowania sieciowego jest kwestia metodologii dostępu do ich zaso-

Stąd rozwiązania używane do ich obsługi zaliczane są do technologii WAN. Zob. D.E. Comer, *Sieci komputerowe...*, s. 246–247.

[53] Zob. szerzej S. Knott, W. Odom, *Akademia sieci...*, s. 121–124; D.L. Shinder, E. Tittel, *Cyberprzestępczość...*, s. 220. Por. L. Dostálek, *Bezpieczeństwo protokołu TCP/IP. Kompletny przewodnik*, Warszawa 2006, s. 64–66; M. Kołodziej, *Ukrywanie i podszywanie się w Internecie* (w:) J. Kosiński (red.), *Przestępczość teleinformatyczna. XII seminarium naukowe*, Szczytno 2009, s. 69; K. Krysiak, *Sieci komputerowe...*, s. 459–461.

bów – czyli sposobu ich przyłączania do sieci. Wyróżnić możemy w oparciu o powyższe kryterium dwa typy sieci[54]:

1) sieci scentralizowane – w takich sieciach centralny komputer – serwer (spotkać można nazwę „serwer uwierzytelniający" – ang. *authentication server* lub po prostu „serwer sieciowy") zarządza, zapewnia bezpieczeństwo, nadzoruje dostęp do sieci, przechowuje dane o uprawnieniach użytkowników (prawach dostępu do zasobów). Serwer realizować różne funkcje, oferując określone usługi – od udostępniania drukarek i innych zasobów, po udostępnianie plików i baz danych. W związku z tym wyróżnia się serwery:
   a) usług konfiguracyjnych – np. serwery NAT, DNS,
   b) usług sieciowych – np. serwery WWW, FTP, pocztowe,
   c) serwery bezpieczeństwa – np. serwery Proxy, Firewall,
   d) serwery autoryzacji.

   Inna używana powszechnie klasyfikacja wyróżnia serwery plików, aplikacji i wydruku. Serwery korzystają z sieciowych systemów operacyjnych (ang. *Network Operating System* – NOS). Muszą być bardzo wydajnymi komputerami, pracującymi bez przerwy i stabilnie (awaria serwera jest równoznaczna zaprzestaniu funkcjonowania sieci). Termin „serwer" oznacza również program zainstalowany na komputerze przeznaczonym do udostępniania wybranych zasobów i realizacji wskazanych wyżej funkcji;
2) sieci *peer-to-peer* (komputerów równorzędnych) – nazywane też sieciami grup roboczych (ang. *workgroups*). Jest to model, który sprawdza się w sieciach składających się z małej liczby komputerów. W tym wypadku brak jest komputera centralnego – każdy z podłączonych komputerów pełni jednocześnie funkcję i serwera (udostępnia swoje zasoby), i klienta (może korzystać z zasobów innych hostów). Takie rozwiązanie ma swoje wady i zalety. Do niewątpliwych zalet zaliczyć można oszczędność, gdyż nie ma potrzeby zakupu kosztownego oprogramowania serwerowego, nie trzeba inwestować w komputer centralny – serwer, który – jak wskazane zostało wyżej – musi być znacznie wydajniejszym, a co za tym idzie droższym komputerem. Ponadto do obsługi sieci z serwerem uwierzytelniającym potrzeba osoby lub osób, które będą nim zarządzać. Wśród wad należy wskazać mniejsze bez-

[54] Por. K. Gromaszek, W. Wójcik (red.), *Sieci komputerowe...*, s. 37–38; S. Knott, W. Odom, *Akademia sieci...*, s. 261–265; D.L. Shinder, E. Tittel, *Cyberprzestępczość...*, s. 229–231.

pieczeństwo takiej sieci oraz fakt, że aby uzyskać dostęp do zasobów innego komputera, użytkownik musi posiadać na nim konto (czyli liczba kont jest równa liczbie pozostałych komputerów) bądź znać specjalne hasło do poszczególnych zasobów danego komputera (gdy sieć liczy wiele komputerów, liczba haseł jest odpowiednio duża). Obecnie każdy nowszy system operacyjny może pełnić jednocześnie rolę zarówno serwera, jak i klienta w sieciach równorzędnych. Wśród systemów operacyjnych klienckich najpopularniejsze są systemy Microsoftu (Windows XP, Vista, 7, 8, 8.1 i 10). Inne to Linux i Macintosh OS X. Komputery klientów sieci nie muszą mieć zainstalowanego systemu operacyjnego tego samego dostawcy, którego oprogramowanie obsługuje serwer. Najpopularniejszymi systemami serwerowymi są systemy Microsoftu (przede wszystkim Windows 2012 Server), Novell NetWare (kiedyś potentat na rynku) oraz Unix/Linux, z których Unix jest systemem działającym wyłącznie na serwerach, Linux natomiast jego wersją, która również może działać na komputerach klientów. Oba systemy dostępne są w bardzo wielu wersjach, zarówno komercyjnych, jak i *open source* (tzw. wolne oprogramowanie).

Nie są sieciami komputerowymi tzw. systemy wielodostępowe (ang. *Thin Client Computing*). Jest to struktura składająca się z centralnego komputera (ang. *mainframe*) oraz komputerów klientów (terminali). Na terminalu znajduje się jedynie graficzna reprezentacja systemu i aplikacji znajdujących się na głównym komputerze. W ten sposób terminale mogą mieć małą moc obliczeniową, bo system i programy znajdują się na centralnym komputerze[55]. Przykładem systemu wielodostępowego jest sieć bankomatów, które pełnią rolę terminali łączących się z centralnym komputerem banku w momencie realizacji transakcji w celu jej przeprowadzenia.

1.2.4. Topologie sieciowe

Pod pojęciem topologii rozumie się układ sieci, sposób organizacji urządzeń sieciowych (zarówno aktywnych, jak i pasywnych) i okablowania. Można mówić o topologii fizycznej (ang. *physical topology*), będącej zbiorem zasad fizycznego łączenia poszczególnych części sieci ze sobą, takich jak np. koncentratory, mosty, przełączniki, oraz logicznej (ang. *lo-*

[55] Por. D.L. Shinder, E. Tittel, *Cyberprzestępczość...*, s. 229.

gical topology), charakteryzującej standardy komunikacji, z których korzystać powinna każda stacja robocza w celu komunikowania się w sieci. Topologia fizyczna jest ściśle powiązana z logiczną – np. sieć w standardzie Ethernet można zbudować w oparciu o topologię gwiazdy lub magistrali, ale nie pierścienia[56].

Wskazać należy następujące topologie fizyczne[57]:

1) punkt-punkt (ang. *point-to-point*) – połączenie dwóch stacji, np. dwa komputery połączone łączem szeregowym (np. USB), radiowym czy skrętką telefoniczną;
2) łańcuch (ang. *chain*) – rozwinięcie wariantu punkt-punkt – szeregowe połączenie większej liczby (więcej niż dwóch) stacji, czego konsekwencją jest przerwanie funkcjonowania tej struktury na skutek „wypadnięcia" z niej jednej stacji;
3) pierścień (ang. *ring*) – komputery połączone są szeregowo (w łańcuch), ale ostatni połączony jest z pierwszym. Awaria przewodu lub jednego hosta powoduje przerwanie działania sieci, chyba że zastosowano dodatkowy sprzęt, tworząc drugi pierścień (ang. *double ring topology*); natomiast przed uniemożliwieniem funkcjonowania sieci przez awarię czy odłączenie jednego komputera chroni podłączanie hostów do pierścienia za pośrednictwem innego urządzenia;
4) magistrala (ang. *bus*) – kable ułożone są liniowo, od komputera do komputera; poszczególne stacje są podłączone do medium sieciowego, nie stanowią węzłów sieci, jak w przypadku wyżej omówionych rodzajów;
5) gwiazda (ang. *star*) – kable zbiegają się w centralnym punkcie;
6) siatka (ang. *mesh*) – komputery połączone są „każdy z każdym" (inna nazwa – krata);
7) topologia drzewa – jest to struktura złożona, powstała na skutek łączenia sieci o różnych topologiach;
8) topologia komórkowa – obszar sieci podzielony jest na częściowo zachodzące na siebie komórki, reprezentujące punkty połączenia.

[56] K. Gromaszek, W. Wójcik (red.), *Sieci komputerowe...*, s. 28; K. Krysiak, *Sieci komputerowe...*, s. 27.

[57] K. Gromaszek, W. Wójcik (red.), *Sieci komputerowe...*, s. 29–33. Por. A. Chodorek, R.R. Chodorek, A.R. Pach, *Dystrybucja danych w sieci Internet*, Warszawa 2007, s. 4–5; D.E. Comer, *Sieci komputerowe...*, s. 250–252. Zob. szerzej S. Knott, W. Odom, *Akademia sieci...*, s. 125–131.

Topologie logiczne definiowane są przez IEEE[58]. Najpopularniejszymi są[59]:

1) Ethernet – opracowana w latach 60., oparta na metodzie dostępu przez „współzawodnictwo". Z kolei sieci Ethernet można podzielić na rodzaje w zależności od użytego okablowania, topologii i szybkości transferu danych (np. 10 Mb Ethernet, 100 Mb Ethernet – Fast Ethernet, Full Duplex Ethernet, 1 Gb Ethernet, 10 Gb Ethernet, 100 Gb Ethernet);
2) Token Ring – opracowana przez IBM z wykorzystaniem metody dostępu do sieci z tokenem;
3) Fiber Distributed Data Interface (FDDI) – standard transmisji danych oparty na technologii światłowodowej. Transfer w tych sieciach wynosi 100 Mb/s. Sieć ta zbudowana jest z dwóch pierścieni – pierścienia pierwotnego i pierścienia zapasowego (wtórnego).

Jak zostało wskazane wyżej, topologia logiczna i fizyczna są ze sobą powiązane. Stąd poniżej zostały przedstawione przykładowe topologie logiczne przyporządkowane do odpowiednich topologii fizycznych:

1) topologia gwiazdy oraz magistrali:
   a) IEEE 802.3 – 10 Mb Ethernet (10Base-5 – sieć z szyną wielodostępną w formie linii prostej wykorzystująca gruby kabel koncentryczny (tzw. gruby Ethernet); zasięg do 500 m, przepustowość 10 Mb/s);
   b) IEEE 802.3u – 100 Mb Ethernet (Fast Ethernet, 100Base-TX – sieć w formie gwiazdy bądź szkieletowa[60], wykorzystująca 2 pary nieekranowanej skrętki, zasięg do 100 m, przepustowość 100 Mb/s);
   c) IEEE 802.3z – 1 Gb Ethernet (1000Base-LX – sieć szkieletowa wykorzystująca włókna światłowodowe (jednomodowe); zasięg do 5 km; przepustowość 1Gb/s);
2) topologia pierścienia:
   a) IEEE 802.5 – Token ring;
   b) IEEE 802.6 – Sieci metropolitalne (MAN);
3) topologia podwójnego pierścienia:
   a) Fiber Distributed Data Interface (FDDI).

[58] IEEE (ang. Institute of Electrical and Electronics Engineers – Instytut Inżynierów Elektryków i Elektroników) – międzynarodowa organizacja typu non-profit skupiająca profesjonalistów, zajmująca się m.in. ustalaniem standardów konstrukcji urządzeń elektronicznych, w tym również standardów dla urządzeń i formatów komputerowych oraz przesyłania danych.

[59] Zob. szerzej D.E. Comer, *Sieci komputerowe...*, s. 347–348; K. Krysiak, *Sieci komputerowe...*, s. 347–350.

[60] Sieć szkieletowa (ang. *backbone network*) – sieć łącząca sieci lokalne.

1.2.5. Wąskopasmowe i szerokopasmowe technologie dostępowe

Dostęp do Internetu zapewniany jest z wykorzystaniem wielu technologii, które – przyjmując za kryterium przepustowość łącza[61] – generalnie dzielone są na dwie kategorie:

1) wąskopasmowe;
2) szerokopasmowe.

Pojęciem technologii wąskopasmowych obejmuje się zwykle te, które zapewniają przepustowość niższą niż 128 kb/s. Do tej grupy zalicza się połączenia modemowe[62] (maksymalna przepustowość wynosi 56 kb/s), niektóre usługi transmisji danych oferowane przez dostawców usług telekomunikacyjnych (np. ISDN[63], choć ten często – z uwagi na podział pasma na kanały – mimo niskiej przepustowości, zaliczany jest do technologii szerokopasmowych) oraz łącza cyfrowe o niskiej przepustowości. Natomiast szerokopasmowy dostęp, przez zwiększenie używanych częstotliwości i podzielenie pasma na kanały, pozwala na równoległe przesyłanie danych cyfrowych (zapewniając tą drogą np. dostęp do Internetu czy telewizji – tzw. kablówka), łącznie z analogową lub cyfrową komunikacją głosową (dlatego też ISDN, w którym w podstawowej wersji stosuje się dwa kanały B po 64 kb/s dla danych oraz kanał sygnalizacyjny D o przepływności 16 kb/s, zaliczany bywa do połączeń szerokopasmowych). Do najpopularniejszych technologii szerokopasmowych należy zaliczyć cyfrowe linie abonenckie (DSL[64]) oraz łącza bazujące na okablowaniu sieci

[61] Przepustowość łącza (ang. *Channel capacity*, pojemność kanału) – maksymalna ilość danych (mierzonych w bitach), jaka może być przesyłana przez dany kanał telekomunikacyjny lub łącze w jednostce czasu (w 1 sekundzie).

[62] Technologia dostępu do Internetu, w której medium sieciowym jest linia telefoniczna, a zamiast karty sieciowej używany jest modem, który moduluje sygnał z cyfrowego sygnału komputerowego na analogowy (używany w sieci telefonicznej). Komputer łączy się z serwerem dostawcy usług internetowych, który nadaje adres IP. W ten sposób uzyskuje się połączenie z siecią, a dalej wszystko przebiega standardowo. Do połączenia służy protokół PPP (ang. *Point-to-point Protocol*) lub SLIP (ang. *Serial Line Internet Protocol*).

[63] ISDN (ang. *Integrated Services Digital Network*, czyli sieć cyfrowa z integracją usług) – technologia sieci telekomunikacyjnych mająca na celu wykorzystanie infrastruktury publicznej sieci telefonicznej do bezpośredniego udostępnienia usług cyfrowych użytkownikom końcowym (bez pośrednictwa urządzeń analogowych, ang. *end-to-end circuit-switched digital services*).

[64] DSL (ang. *Digital Subscriber Line*) – cyfrowa linia abonencka – technologia szerokopasmowego dostępu do Internetu przy użyciu istniejących sieci telekomunikacyjnych. Rozwiązanie to występuje w wielu wariantach, zbiorczo określanych jako xDSL. Najważniejsze odmiany to: ADSL – (ang. *Asymmetric DSL* – asymetryczna cyfrowa linia abonencka) zapewniająca teoretycznie maksy-