Ius et Securitas 1/2024 | ISSN 3071-799X

Bogdan Grabowski
Wydział Humanistyczny
Politechnika Koszalińska
ORCID: 0009-0006-0413-6345
grabowski.bogdan.54@wp.pl

Cyfrowe zagrożenia – zarys problemu

Streszczenie

Historia powstania Internetu sięga początków II połowy XX wieku[1]. We wrześniu 1969 roku w Uniwersytecie Kalifornijskim w Los Angeles podczas badań na potrzeby wojska, stworzono sieć ARPANET, która stała się prekursorem dzisiejszego Internetu[2]. W Polsce Internet pojawił się dokładnie w dniu 17 sierpnia 1991 roku, gdyż jest to data wymiany pakietów TCP/PP między naszym państwem a Danią[3]. Od tego czasu nastąpił gwałtowny rozwój rozwiązań e-commerce, komunikacji bezprzewodowej i szerokiej gamy usług świadczonych w sieci internetowej. Jest to znaczne ułatwienie życia, ale także stanowi szereg zagrożeń, zarówno w życiu codziennym, jak i w zarządzaniu strategicznym czy też w obszarze obronności państwa i obronie cywilnej. Celem niniejszego artykułu jest analiza zagrożeń, wynikających z nieodpowiedzialnego lub nieświadomego korzystania z zasobów sieci. W artykule poruszono zagrożenia wynikające z korzystania z Internetu, takie jak: mowa nienawiści, manipulacja, dezinformacja,

[1] Słowo „Internet" może być pisane z wielkiej lub małej litery, w zależności od kontekstu znaczenia. Na potrzeby niniejszego artykułu przyjęto pisownię zaczynającą się z wielkiej litery. Według Słownika Języka Polskiego, Internet jest nazwą własną konkretnej globalnej sieci komputerowej. Jednym ze źródeł wątpliwości co do pisowni tego słowa jest fakt, że Internet ma strukturę hierarchiczną i w konsekwencji laikom może się wydawać, że istnieje wiele sieci, https://sjp.pwn.pl/poradnia/haslo/Internet-czy-internet;228.html, [dostęp: 9.01.2025].

[2] K. Grygiel, *Początki Internetu*, https://katarzynagrygiel.staff.tcs.uj.edu.pl/students/www.pdf, [dostęp: 9.01.2025].

[3] IBM, Protokoły TCP/IP. Protokoły umożliwiają komputerom i programom aplikacji wymianę informacji. Protokół TCP/IP określa sposób przenoszenia informacji od nadawcy do odbiorcy. Docelowo, protokoły odbierają dane z aplikacji, dzielą je na mniejsze części zwane pakietami, dodają adres docelowy, a następnie przekazują pakiety wraz z następną warstwą protokołu, do sieci Internet, https://www.ibm.com/docs/pl/aix/7.3?topic=protocol-tcpip-protocols, [dostęp: 9.01.2025].

cyberterroryzm oraz cyberprzemoc. Należy jednak przy tym wskazać, że bezpieczny i mądry rozwój technologii informacyjno-komunikacyjnych jest szansą na polepszenie jakości życia społeczeństw, ale pod warunkiem świadomego i odpowiedzialnego korzystania z nich. W niniejszym artykule, podejmując się badania opisywanego zjawiska i korelujących ze sobą współzależności, autor zastosował metodę behawioralną, porównawczą, oraz uzupełnił ją podejściem historycznym, uzupełniając materiał badawczy analizą literatury przedmiotu.

Słowa kluczowe: Internet, dezinformacja, hejt, fake news, manipulacja, zagrożenia.

Wprowadzenie

Do powstania Internetu przyczynił się wyścig zbrojeń, jaki miał miejsce pomiędzy ZSRR a Stanami Zjednoczonymi Ameryki Północnej, szczególnie wystrzelenie w kosmos przez Związek Radziecki rakiety Sputnik 1 w październiku 1957 roku. Wydarzenie to wstrząsnęło Stanami Zjednoczonymi, wywołało strach i niepewność wśród społeczeństwa amerykańskiego. Nagle przestała istnieć odległość dzieląca ewentualnych wrogów. W związku z zaistniałą sytuacją Stany Zjednoczone powołały do życia w 1958 roku Agencję Zaawansowanych Projektów Badawczych (ARPA). Dekadę później, nowe pokolenie naukowców i informatyków, techników i inżynierów stworzyło Internet[4]. Inspiratorem do stworzenia sieci komputerowych było wojsko, wykorzystano do tego celu pierwsze masowo produkowane przez IBM modemy telefoniczne. W latach 70-tych ścisłą kontrolę nad Internetem miała armia Stanów Zjednoczonych, aż do 1983 roku, kiedy to rozdzielono Internet na część cywilną i militarną[5].

Dziś, możemy mówić o tzw. „Internecie rzeczy", niewyobrażalnej wprost liczbie użytkowników sieci. Zjawisko to pojawiło się w momencie, w którym liczba rzeczy i obiektów podłączonych do Internetu przekroczyła liczbę ludności. Na przełomie 2008 i 2009 roku liczba urządzeń podłączonych do Internetu po raz pierwszy przekroczyła liczbę mieszkańców Ziemi[6].

[4] E. Jankowska, D. Korzan, *Technologie elektroniczne wykorzystywane w nauczaniu języka angielskiego*, „Edukacja Otwarta" 2018, nr 2, s. 28-29.

[5] A. Kloch, *Wędrówka do utopii,*, „Academia. Magazyn Polskiej Akademii Nauk" 2017, nr 1, s. 67.

[6] E.M. Kwiatkowska, *Rozwój Internetu rzeczy-szanse i zagrożenia,* „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2014, nr 3, s. 2.

Internet jest medium które pozwala na przeniesienie się w wirtualny świat rozrywki, usług, biznesu, komunikacji. Jest to narzędzie służące zarządzaniu strategicznemu i przechowywaniu danych (tzw. chmura). Internet to również narzędzie wykorzystywane przez administrację państwową i wojsko. Z dostępem do Internetu i korzystaniem z sieci, również za pośrednictwem telefonów komórkowych, wiążą się jednakże zagrożenia w postaci przechwytywania danych, cyberataków, fake newsów, phishingu, włamań do kont bankowych i innych. Cyfrowym zagrożeniem jest również uzależnienie od Internetu.

Uzależnienie od Internetu

We współczesnym świecie ważne miejsce zajmuje informacja, a szczególnie szybkość jej pozyskiwania i przekazywania. Narzędziem umożliwiającym jej przepływ, jak też i preparowanie jest Internet. O jego roli decydują podstawowe cechy: światowy zasięg, multimedialność, interaktywność. W komunikacji w wirtualnym świecie najważniejszy jest komputer, gdzie często interakcja z maszyną staje się ważniejsza, a człowiek schodzi na dalszy plan. Czynnikiem wpływającym na liczbę osób uzależnionych od sieci jest powszechny dostęp do Internetu oraz konsekwencje spowodowane szybkim postępem technologicznym. Internet ma cztery najważniejsze cechy odpowiedzialne za jego popularność: wyobraźnię, interaktywność, dostępność, anonimowość[7]. Wyobraźnia pozwala uwolnić się od fizycznych wad i codzienności realnego świata i sprawia że cyberprzestrzeń nabiera atrakcyjności. Interaktywność daje możliwość wchodzenia w relacje z innymi użytkownikami w sposób prostszy i szybszy, niż w rzeczywistości. Dostępność i anonimowość dają pewność i swobodę. Chociaż na ogół osoby wykorzystują sieć celowo i funkcjonalnie (udogodnienie pomagające załatwić im codziennie sprawy) i nie wiąże się to z negatywnymi konsekwencjami, jest jeszcze druga grupa osób. Te tracą kontrolę nad swoim czasem, spędzają w sieci wiele godzin, Internet staje się ich podstawowym środowiskiem funkcjonowania. W literaturze przedmiotu funkcjonują różne określenia uzależnień od Inter-

[7] T. Majcherkiewicz, D. Żuchowska-Skiba, *Internet i nowe technologie komunikowania. Ich rola w procesie kształtowania środowiska młodzieży akademickiej,* [w:] *Akademicka społeczność informacyjna. na przykładzie środowiska akademickiego Akademii Górniczo-Hutniczej, Uniwersytetu Jagiellońskiego i Akademii Górniczo-Hutniczej*, L. Haber [red.], Kraków 2005, s. 297-310.

netu: siecioholizm, sieciozależność, cyberzależność, internetoholizm, infoholizm, infozależność[8]. Wyróżnia się pięć podtypów uzależnienia od Internetu: 1) internetowa erotomania czyli przymusowe przeglądanie stron internetowych dla dorosłych, zawierających treści pornograficzne; 2) cybernetyczne uzależnienie od internetowych komunikatorów społecznych; 3) obsesyjny hazard on-line, zakupy, transakcje handlowe w sieci; 4) uzależnienie od gier komputerowych; 5) obsesyjne przeglądanie stron i przeszukiwanie różnego typu baz danych[9].

Uzależnienie od stron internetowych rozwija się stopniowo, z upływem czasu korzystanie z komputera i Internetu zaczyna dominować w życiu użytkownika, powodując odsunięcie na dalszy plan codziennych czynności, kontaktu z innymi ludźmi, rodziny i pracy. Źródło nadużywania Internetu ma negatywny wpływ na jednostki w sferze: psychicznej, społecznej, rodzinnej, w relacjach międzyludzkich oraz w sferze ekonomicznej[10].

Zagrożenia wynikające z korzystania z Internetu

Komisja Europejska określiła aż 8 najpoważniejszych zagrożeń, na jakie narażony jest użytkownik Internetu. Są to: ransomware, malware, zagrożenia socjotechniczne, zagrożenia dla danych, denial services, zagrożenia dostępności do Internetu, dezinformacja oraz ataki na łańcuch dostaw[11].

Ransomware, to sytuacja gdy hakerzy przejmują kontrolę nad czyimiś danymi i żądają okupu za przywrócenie do nich dostępu. Malware ma miejsce, gdy poprzez sieć internetową użytkownik ściągnie złośliwe oprogramowanie, które uszkadza system bądź wpływa w sposób niepożądany na jego działanie. Są to różnego rodzaju wirusy, programy szpiegujące czy tzw. konie trojańskie. Zagrożenia socjotechniczne wykorzystują naiwność i brak świadomości użytkowników Internetu, koncentrują się na wykorzystaniu błędów ludzkich do naruszenia systemów bezpieczeństwa. Może być to otwarcie

[8] D. Nicholas, *Ocena potrzeb informacyjnych w dobie Internetu: idee, metody, środki,* Warszawa 2001, s. 123.

[9] T. Majcherkiewicz, D. Żuchowska-Skiba, *Internet*..., s. 297-310.

[10] K. Polańska, *Informacja, jej wiarygodność i co z ich dla nas wynika*, [w:] *Informacja – dobra lub zła nowina,* A. Szewczyk [red.], Szczecin 2004, s. 58.

[11] S. Witkowski, *Odporni na cyberataki? Poziom cyfrowego bezpieczeństwa Polski*, Warszawa 2023, s. 9.

złośliwych plików, wiadomości mailowych, bądź wchodzenie na zainfekowane strony internetowe. Najczęstszym atakami tego rodzaju jest phising, czyli podszywanie się pod inną osobę czy instytucję w wiadomości e-mail w celu wyłudzenia danych, np. dostępu do konta bankowego. Zagrożenia dla danych natomiast, to możliwość dostępu osób nieuprawnionych do zabezpieczonych informacji, ich wykorzystanie na zewnątrz. Zagrożeniem może być również denial services czyli odmowa, blokada dostępności do usługi internetowej, telekomunikacyjnej. Obecnie rośnie popularność wykorzystywania dostępności denial services w konfliktach militarnych, np. w cybernetycznej wojnie rosyjsko-ukraińskiej, w konflikcie izraelsko-palestyńskim. Zagrożenia dostępności do Internetu to nic innego jak uniemożliwienie korzystania z samej sieci, atak na infrastrukturę i pozbawienie danych. Wreszcie ataki na łańcuchy dostaw, oznaczające zakłócenie relacji między dostawcami a odbiorcami dóbr i usług. W tym konkretnym przypadku, działanie to jest wymierzone w gospodarkę i handel.

Na zaprezentowanych powyżej przykładach zagrożeń, widać więc że Internet może być niebezpiecznym narzędziem w rękach profesjonalistów, którzy mogą wyrządzić szkody nie tylko korporacjom, administracji państwowej, ale także zwykłemu obywatelowi. Internet może być także narzędziem informacji i dezinformacji. Przykładem mogą być internetowe wyszukiwarki, z których najpopularniejsze to np. onet.pl, wp.pl, altavisa.com, hotbot.com, chip.pl, yahoo.com, excite.com[12]. Ponieważ wyszukiwarki internetowe to automaty, które mogą popełniać błędy, zaufanie do wyników wyszukiwania powinno być ograniczone.

Ograniczone również powinno być zaufanie do dostarczanych danych oraz treści, zwłaszcza tych budzących sensację lub skrajne emocje. Są to tzw. fake newsy, czyli przekazywane informacje, które opierają się na celowej dezinformacji lub oszustwie. W XXI wieku wpływ fake newsów poprzez wszechobecny Internet jest zjawiskiem ogólnoświatowym, a użycie terminu stało się powszechne. Mianem fake newsa bądź mistyfikacji określa się wiele zjawisk, np.: nieprawdziwe wiadomości, chwyty reklamowe, oszustwa o charakterze kryminalnym, krzywoprzysięstwo, plagiat[13]. Fake news czyli mistyfikacja albo kłamstwo, musi spełniać określone warunki: przede wszystkim

[12] D. Nicholas, *Ocena...*, s. 134.

[13] A. Boese, *Fake newsy i inne fałszerstwa od średniowiecza do XXI wieku,* Warszawa 2018, s. 153.

zawierać elementy skandalu, pomysłowości, dramatyzmu, sensacji i przyciągać zainteresowanie opinii publicznej, czyli prasy brukowej, a informacja ma być traktowana jako towar. Według przeprowadzonych badań, obywatele Unii Europejskiej aż w 85% czują się zagrożeni fake newsami. Podobnie jest także w Stanach Zjednoczonych[14]. Aby walczyć z fake newsami można zastosować dwie formuły. Jedną z nich są kampanie informacyjne w społeczeństwie połączone z edukacją, druga możliwość to promowanie dobrych praktyk i monitorowanie treści w Internecie. W obu przypadkach, działania te mogą realizować organizacje pozarządowe i agendy.

Internet – hejt, źródło dezinformacji

Od fake newsów, wypaczających światopogląd, już tylko krok do hejtu, mowy nienawiści, nakierowanej na mniejszości narodowe, osoby o innej orientacji religijnej lub seksualnej. Hejt może się przejawiać za pomocą słów, grafik, memów, gifów, czy filmów. Obiektem hejtu może stać się każdy[15]. Jak wynika z badań z 2014 roku, przeprowadzonych przez SW Research, co czwarta osoba korzystająca z Internetu padła ofiarą hejtera, a ponad 11% użytkowników przyznaje się do obraźliwego komentowania innych ludzi, zjawisk i wydarzeń[16]. Według badań opinii społecznej 40% Polaków uważa mowę nienawiści za znaczący problem społeczny, a 77% odczuwa dyskomfort w związku z obraźliwymi wypowiedziami pojawiającymi się w przestrzeni publicznej. Warto zaznaczyć, że podjęto próbę analizy zachowania samych hejterów, chcąc ustalić mechanizm napędzający mowę nienawiści. Okazuje się, że hejt pobudza ośrodek przyjemności, stymuluje układ nagrody. Do jego pobudzenia dochodzi wtedy, kiedy odczuwamy zadowolenie. Można to porównać do reakcji mózgu na rzeczy takie jak uprawianie seksu, zażywanie narkotyków, picie alkoholu, jedzenie czekolady[17]. Wiek i pozycja społeczna również ma wpływ na postrzeganie zjawiska hejtu. Dla dzieci hejt oznacza negatywne komentarze pod zdjęciami umieszczanymi na profilach w portalach społecznościowych, które

[14] M. Tomaszewska-Michalak, *Fake news – wstępna analiza zjawiska*, „Przegląd Politologiczny" 2021, nr 1, s. 62.

[15] A. Boese, *Fake*..., s. 195.

[16] A. Kukliński, *Hejt w Internecie, jako zagrożenie bezpieczeństwa człowieka,* „Kultura bezpieczeństwa. Nauka, praktyka, refleksje" 2018, nr 3.

[17] Ibidem, s.136.

doprowadzały do usunięcia fotografii. Inny problem to przerabianie zdjęć czy wysyłanie do adresata wulgarnych filmów, inwektyw i wyzwisk. Natomiast hejt nie wpływa znacząco na postrzeganie lekarzy w danym środowisku, za to jest dość szkodliwy dla osób publicznych, ale o wiele mniej dla celebrytów[18]. W walce z hejtem potrzebna jest świadomość społeczna, kampanie i programy edukacyjne (zwłaszcza te, skierowane do młodzieży), ale także ważny jest aspekt prawny- za czyn ten grożą sankcje karne i finansowe.

Internet to doskonała pożywka dla dezinformacji. Istnieje jednak kilka cech, które pozwalają zwrócić uwagę na potencjalne zagrożenie treścią[19]. Dezinformacja oznacza rozprzestrzenianie nieprawdziwych informacji, zafałszowanie prawdziwego obrazu, np. w ujęciu polityki, natomiast osoby biorące w niej udział to dezinformujący (nadawca treści) i dezinformowany (jej odbiorca)[20]. Na dezinformację wskazywać mogą sensacyjne, krzykliwe tytuły, dziwny adres www albo nazwa źródła, nierówne formatowanie tekstu, wykrzykniki, błędy ortograficzne, zła odmiana słów, dużo kalek językowych, nacechowany emocjonalnie język lub krzykliwe zdjęcia. Ponadto brak najczęściej brak jest podanego autora, brak źródła podnoszącego temat. Dezinformacji sprzyjają tematy które powodują podziały społeczne, język nienawiści, używanie emocjonalnych zwrotów, informacje, teksty, podsycające radykalne emocje. Dezinformacja dziś przenosi się głównie w sferę portali społecznościowych, należy więc weryfikować profile, wpisy uczestników, dokonać weryfikacji materiału audiowizualnego. Warto korzystać tylko z oficjalnych, wiarygodnych źródeł informacji[21]. Mogą być nimi statystyki policyjne, strony urzędowe, dane Głównego Urzędu Statystycznego, dane Eurostatu, informacje Polskiej Agencji Prasowej, rejestry i sprawdzone bazy danych. W komitecie prasowym Unii Europejskiej z 12 marca 2018 roku, poświęconemu dezinformacji i walce z tym zjawiskiem, grupa ekspertów zaleca rozwój umiejętności korzystania z mediów w celu przeciwdziałania dezinformacji, opracowanie narzędzi, które pomogą użytkownikom i dziennikarzom zwalczać dezinformację, zachowanie różnorodności i stabilności europejskich mediów informacyjnych i dalsze badania wpływu

[18] K. Garwol, *Hejt w Internecie- analiza zjawiska*, „Edukacja-Technika-Informatyka" 2016, nr 4, s. 4.

[19] A. Boese, *Fake*..., s. 225.

[20] M.J. Wachowicz, *Ujęcie teoretyczne pojęcia dezinformacji*, „Wiedza Obronna" 2019, nr 1-2, s. 230.

[21] K. Polańska, *Informacja*..., s. 68.

dezinformacji na społeczeństwo w Europie. Zarekomendowano opracowanie kodeksu zasad dla funkcjonowania platform internetowych czy serwisów społecznościowych, tj. powinny one zapewniać przejrzystość i podawać, w jaki sposób algorytmy wybierają dla nas informacje. We współpracy z europejskimi serwisami informacyjnymi serwisy internetowe powinny także zwiększyć widoczność rzetelnych i wiarygodnych informacji i jednocześnie ułatwić dostęp do nich użytkownikom[22].

Cyberbullying czyli nękanie w sieci

Cyberbullying to zjawisko nękania w Internecie, do którego wykorzystuje się komunikację cyfrową: najczęściej posty, komentarze w mediach społecznościowych, wiadomości wysyłane przez komunikatory internetowe, a także e-maile i SMS-y. Działania te służą do poniżania, nękania lub zastraszania ofiary. Najbardziej znane formy cyberbullyingu to m.in. publikowanie fałszywych, ośmieszających, a nawet agresywnych komentarzy, zdjęć i filmików w sieci [23]. Sprawca ma jeden cel: przy użyciu nowych technologii komunikacyjnych i informacyjnych dąży do skrzywdzenia danej osoby bądź grupy. Ofiarami są dzieci, młodzież, jak też osoby dorosłe. Raport opracowany przez Naukową i Akademicką Sieć Komputerową Państwowego Instytutu Badawczego pod nazwą „Nastolatki 3.0 2021 r." informuje, że co piąty uczeń doświadczył przemocy w Internecie, takie jak wyzywanie (29,7%), ośmieszanie (22,8%), poniżanie (22%) i straszenie (13,4%). Jednocześnie 74,7% rodziców nie zdaje sobie sprawy z tego, że ich dziecko miało kontakt z przemocą online. Coraz częściej celem nękania w sieci stają się dorośli, co może prowadzić do problemów zdrowotnych, zawodowych i wizerunkowych. Można jednocześnie spróbować zdefiniować przyczyny zjawiska cyberprzemocy i jego sprawców[24]. Liberalne wychowanie dzieci i młodzieży prowadzi w przyszłości do zaburzeń osobowości i cechuje się brakiem empatii, impulsywnością i egoizmem[25]. Może to

[22] Walka z dezinformacją w Internecie: eksperci apelują o większą przejrzystość platform internetowych. Komisja Europejska – Komunikat prasowy, Strasburg, 12 marca 2018 r., s. 2.

[23] *Cyberbullying – nękanie w sieci*, https://www.gov.pl/web/baza-wiedzy/cyberbullying---nekanie-w-sieci, [dostęp:10.01.2025].

[24] T. Majcherkiewicz, D. Żuchowska-Skiba, *Internet*..., s. 297-310.

[25] R.M. Jabłońska, *Człowiek w cyberprzestrzeni: wprowadzenie do psychologii Internetu*, Łódź 2018, s. 142.

powodować zaburzenia mózgu czyli psychopatii. Psychopaci nie są w stanie wykształcić mechanizmu, który rozróżniał by czyny niemoralne od akceptowanych społecznie. Są przekonani że postępują właściwie i tak właśnie powinni zrobić. Psychopata to osoba, która ma poważne braki w rozumieniu emocji, jest mocno impulsywna, egoistyczna, pozbawiona wyrzutów sumienia. W swoim zachowaniu jest pozbawiona hamulców, niezdolna do oceny emocjonalnej poziomu cierpienia innych ludzi.

Przed cyberbullyingiem trzeba i należy się bronić, przede wszystkim jednak należy reagować zgłaszając niestosowne, uwłaczające godności komentarze do administratorów stron lub moderatorów forów dyskusyjnych. Większość serwisów społecznościowych w swoich regulaminach również ma zapisy dotyczące cyberprzemocy. Ofiary cyberprzemocy powinny zachować kopię obraźliwego materiału, robiąc tzw. zrzut ekranu komputera. Jest to dowód na naruszenie godności osobistej, tym bardziej że cyberprzemoc w Polsce jest karalna. Obecny kodeks karny uznaje cyberprzemoc za czyn zabroniony, należy więc wszelkie przypadki cyberprzemocy, będące naruszeniem prawa zgłosić na policję lub do prokuratury[26].

Podsumowanie

Mimo wielu korzyści, jakie niesie ze sobą Internet należy pamiętać że każda nowa technologia może być nie tylko ułatwieniem, ale również nieść ze sobą zagrożenia, które autor starał się wymienić w niniejszym tekście. W dzisiejszych czasach, w dobie kulturowych przemian społecznych, napływu najnowszych technologii i wszechobecnej sieci, bez Internetu nie da się żyć i funkcjonować. Jednak brak ostrożności w korzystaniu z Internetu niesie ze sobą ryzyko cyberataku, cyberprzemocy, wykorzystania wizerunku czy phishingu. Zainfekowana sieć może wyłączyć z użytku serwery i podłączone do nich nośniki danych, jakimi są komputery. Dostępność Internetu to zachęta do szpiegostwa przemysłowego, wydobywania wrażliwych danych, stosowania hejtu. Atrakcyjność wirtualnego świata powoduje, że ogromnym problemem jest uzależnienie od Internetu, skutkujące rozpadem więzi społecznych, chorobami i dysfunkcją społeczną.

[26] *Cyberbullying – nękanie w sieci*, https://www.gov.pl/web/baza-wiedzy/cyberbullying---nekanie-w-sieci, [dostęp:10.01.2025].

Wykorzystując w pełni możliwości, jakie daje Internet, należy jednocześnie kłaść nieustanny, olbrzymi nacisk na edukację (zarówno młodzieży jak i seniorów), na promowanie programów nawiązujących do cyberbezpieczeństwa. Walka z zagrożeniami Internetu to wykorzystanie rozsądku, czujność i zasad cyberhigieny, rozumianej jako zbiór praktyk dążących do zabezpieczenia użytkowników, urządzeń, sieci i danych przed zagrożeniami, jakie niosą za sobą cyberataki[27].

Bibliografia

Boese A., *Fake newsy i inne fałszerstwa od średniowiecza do XXI wieku,* Warszawa 2018.

Garwol K., *Hejt w Internecie- analiza zjawiska*, „Edukacja-Technika-Informatyka" 2016, nr 4.

Jabłońska R.M., *Człowiek w cyberprzestrzeni: wprowadzenie do psychologii Internetu*, Łódź 2018.

Jankowska E., Korzan D., *Technologie elektroniczne wykorzystywane w nauczaniu języka angielskiego*, „Edukacja Otwarta" 2018, nr 2.

Kloch A., *Wędrówka do utopii*,, „Academia. Magazyn Polskiej Akademii Nauk" 2017, nr 1.

Kukliński A., *Hejt w Internecie, jako zagrożenie bezpieczeństwa człowieka,* „Kultura bezpieczeństwa. Nauka, praktyka, refleksje" 2018, nr 3.

Kwiatkowska E.M., *Rozwój Internetu rzeczy-szanse i zagrożenia,* „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2014, nr 3.

Majcherkiewicz T., Żuchowska-Skiba D., *Internet i nowe technologie komunikowania. Ich rola w procesie kształtowania środowiska młodzieży akademickiej,* [w:] *Akademicka społeczność informacyjna. na przykładzie środowiska akademickiego Akademii Górniczo-Hutniczej, Uniwersytetu Jagiellońskiego i Akademii Górniczo-Hutniczej*, L. Haber [red.], Kraków 2005.

Nicholas D., *Ocena potrzeb informacyjnych w dobie Internetu: idee, metody, środki,* Warszawa 2001.

Polańska K., *Informacja, jej wiarygodność i co z ich dla nas wynika*, [w:] *Informacja – dobra lub zła nowina,* A. Szewczyk [red.], Szczecin 2004.

Tomaszewska-Michalak M., *Fake news – wstępna analiza zjawiska*, „Przegląd Politologiczny" 2021, nr 1.

Wachowicz M.J., *Ujęcie teoretyczne pojęcia dezinformacji*, „Wiedza Obronna" 2019, nr 1-2.

Witkowski S., *Odporni na cyberataki? Poziom cyfrowego bezpieczeństwa Polski*, Warszawa 2023.

[27] *Cyberhigiena – jak zadbać o bezpieczeństwo w sieci?* https://balticad.eu/cyber-higiena-bezpieczenstwo-w-sieci, [dostęp:10.01.2025].

* * *

Digital Threats – an Overview of the Problem

Abstract

The history of the origin of the Internet dates back to the beginning of the second half of the 20th century. In September 1969, at the University of California in Los Angeles, during research for the military, the ARPANET network was created, which became the forerunner of today's Internet. In Poland, the Internet appeared exactly on 17 August 1991, as this is the date of the exchange of TCP/PP packets between our country and Denmark. Since then, there has been a rapid development of e-commerce solutions, wireless communication and a wide range of services provided over the Internet. This has made life much easier, but it also poses a number of risks, both in everyday life and in strategic management or in the area of state defence and civil defence. The aim of this article is to analyse the risks arising from irresponsible or uninformed use of web resources. The article addresses the risks arising from the use of the Internet, such as hate speech, manipulation, disinformation, cyberterrorism and cyberbullying. However, in doing so, it should be pointed out that the safe and wise development of information and communication technologies is an opportunity to improve the quality of life of societies, but on the condition of informed and responsible use. In this article, undertaking a study of the phenomenon described and the correlating interdependencies, the author used a behavioural, comparative method, and supplemented it with a historical approach, supplementing the research material with an analysis of the literature on the subject.

Keywords: Internet, disinformation, hate, fake news, manipulation, threats.