Patrycja Dobek
patriziaa.dk@gmail.com
Lotnicza Akademia Wojskowa

TECHNOLOGIE INFORMACYJNE A BEZPIECZEŃSTWO: ANALIZA WSPÓŁCZESNYCH ZAGROŻEŃ I DZIAŁAŃ PREWENCYJNYCH

https://doi.org/10.55676/asi.v6i2.42

Streszczenie

Celem artykułu było wskazanie wybranych współcześnie naukowo-technologicznych zagrożeń narażających bezpieczeństwo. Obecnie technologia informacyjna jest powszechnie dostępna, co jest źródłem wielu zagrożeń ściśle związanych z użytkowaniem systemów i sieci informatycznych. Przedstawiono działania Internetu jako medium współczesnych zagrożeń, ukazano także cyberbezpieczeństwo w XXI w. oraz trollowanie jako swego rodzaju atak występujący w sieci. Stało się więc oczywistym, iż nowoczesne technologie informacyjne i komunikacyjne są pełne zagrożeń.

Słowa kluczowe*: technologia, nauka, współczesność, zagrożenia, cyberbezpieczeństwo, Internet, trollowanie, sieci społecznościowe*

INFORMATION TECHNOLOGIES AND SECURITY: AN ANALYSIS OF CONTEMPORARY THREATS AND PREVENTIVE MEASURES

Abstract

The aim of the article was to showcase selected modern scientific and technological threats that pose a risk to security. With the widespread availability of information technology, numerous threats have emerged, many of which are associated with the use of information systems and networks. It presents the Internet as a medium for contemporary threats, as well as highlighting the significance of cyber security in the 21st century and the phenomenon of trolling as a form of online aggression. It is evident that modern information and communication technologies are fraught with a multitude of dangers.

Keywords*: technology, science, modern times, threats, cyber security, Internet, trolling, social networks*

1. Wstęp

Stosowanie nowych technologii wiąże się z wieloma zagrożeniami, a zwłaszcza z ich negatywnym wpływem na różne obszary działalności człowieka. Rozwój elektroniki, homogeniczne sieci informacyjne, upowszechnienie się urządzeń dostępowych, pojawienie się sieci społecznościowych, wykorzystanie sieci publicznych do przesyłania informacji do systemów przemysłowych – czynią z informacji kluczowy wyznacznik wiedzy i władzy[1]. Funkcjonowanie Internetu jest uznawane jako jedno z najważniejszych działań na przestrzeni ostatnich lat. Obecnie ludzie na całym świecie nie są w stanie wyobrazić sobie życia bez Internetu i powiązanych z nim przedsięwzięć. Wszechobecność i popularność Internetu wywarła ogromny wpływ na zmiany w codziennym funkcjonowaniu społeczeństwa. Należy więc pamiętać, aby w sposób odpowiedni, a przede wszystkim rozsądny, korzystać z istniejących walorów sieci.

W niniejszym artykule przedstawiono wyniki badań, które zostały przeprowadzone w formie kwestionariusza ankiety. W badaniu wzięły udział 84 osoby, w tym 54 kobiety – 64,3%, 29 mężczyzn – 34,5% oraz 1 osoba genderfluid (jest to tożsamość płciowa, odnosząca się do płci, która zmienia się w czasie) – 1,2%. Jeśli chodzi zaś o status kształcenia, to kwestionariusz został skierowany do

[1] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 11–12.

uczniów szkół średnich oraz do studentów, a przedział wiekowy, jaki zanotowano podczas badań, wyniósł od 16 do 44 lat. Do respondentów łącznie skierowano 25 pytań, które zostały posegregowane w trzy główne grupy:

- Internet – medium współczesnych zagrożeń;
- Cyberbezpieczeństwo w XXI w.;
- Trollowanie jako metoda ataku w Internecie.

Podstawowe pytanie badania brzmiało: Co dla Pani/Pana współcześnie stanowi najpoważniejsze zagrożenie bezpieczeństwa? Respondenci w każdej grupie oceniali poziom zagrożenia za pomocą 7-stopniowej skali Likerta, gdzie 7 oznaczało najwyższe zagrożenie, a 1 najmniejsze.

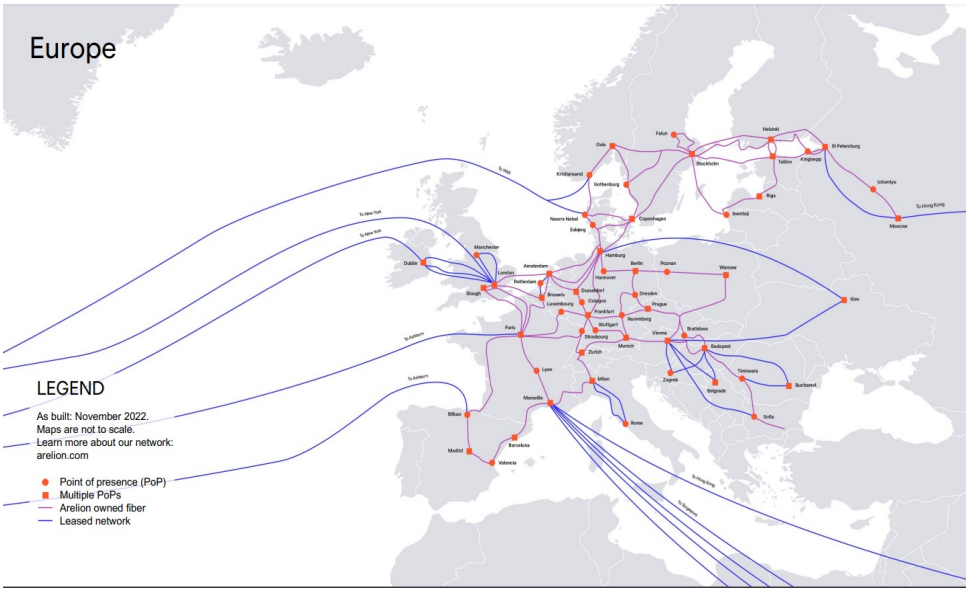
2. Internet jako źródło współczesnych zagrożeń bezpieczeństwa

W erze XXI w. można zauważyć związek pomiędzy rosnącym postępem technologicznym a ludzkim doświadczeniem[2]. Codziennie każdy człowiek jest świadkiem czynnych, a zarazem głębokich przemian społecznych, które praktycznie w większości są spowodowane działaniami technologicznymi. Współcześnie praktycznie nikt nie wyobraża sobie już życia bez technologii, Internetu, telefonu itp. Działania takie często prowadzą do różnorodnych zagrożeń, które odbijają się nie tylko na społeczeństwie, ale również na funkcjonowaniu całego kompleksu związanego z rozwijającą się techniką.

Internet, najprościej definiując, jest globalnym systemem połączonych komputerów na całym świecie, który pozwala ludziom komunikować się ze sobą oraz dzielić się informacjami[3]. Obejmuje kilka szerokopasmowych linii danych stanowiących *backbone* Internetu, który działa tak jak ludzki kręgosłup, potrafiący przenieść rozmaite sygnały do wielu mniejszych nerwów w organizmie – tak właśnie szkielet sieci jest w stanie przenieść zróżnicowane dane do mniejszych linii transmisyjnych[4]. Internet jest siecią rozległą, dlatego też opiera się na sieci szkieletowej, która służy do przesyłania danych na duże odległości (rys. 1). Ponadto sieć szkieletowa Internetu składa się z kilku połączeń, posiadających potężną przepustowość łączącą ze sobą cały szereg wielorakich węzłów na całym świecie[5]. Tak naprawdę Internet zapewnia szeroki zakres zasobów i usług informacyjnych, takich jak[6]:

- połączone ze sobą dokumenty hipertekstowe i aplikacje sieci World Wide Web (WWW);
- wszelkiego rodzaju media społecznościowe (aplikacje i witryny – np. Facebook, Instagram, Twitter);
- poczta elektroniczna (e-mail);
- telefonia.

[2] *Technologiczno-społeczne oblicza XXI wieku*, red. D. Gałuszka, G. Ptaszek, D. Żuchowska-Skiba, Kraków 2016, s. 13–14.
[3] B. Cieśleńska, M. Bruździński, *Obszary użytkowania Internetu we współczesnym obliczu sieci*, „Społeczeństwo. Edukacja. Język" 2016, t. 4, s. 22.
[4] *What is the Internet backbone?*, https://www.arelion.com/knowledge-hub/what-is-guides/what-is-the-internet-backbone [dostęp: 9.04.2023].
[5] https://techterms.com/definition/backbone [dostęp: 9.04.2023].
[6] J. Hofmokl, *Internet jako nowe dobro wspólne*, Warszawa 2009, s. 100–101.



Rys. 1. Europejska mapa szkieletów internetowych

Źródło: What is the Internet backbone?, https://www.arelion.com/knowledge-hub/what-is-guides/what-is-the-internet-backbone [dostęp: 9.04.2023].

Kształtowanie więzi społecznych może wynikać z prawidłowego przepływu informacji, przygotowując egzystencję jednostki na odpowiednim dla niej gruncie. Należy zachować równowagę w dostarczaniu odpowiedniej ilości informacji, ponieważ wszelkie zakłócenia w tym procesie mogą prowadzić do skutków związanych z nadmiarem bądź niedoborem informacji. Dlatego też taki postęp może spowodować brak jakiejkolwiek orientacji we współczesnym świecie[7]. Ponadto niewłaściwe korzystanie z Internetu może doprowadzić zarówno do różnorodnych chorób, jak i do treści, które są niepożądane wychowawczo. Należy mieć także na względzie czynny wzrost pojawiania się przestępczości w cyberprzestrzeni[8].

W obliczu zagrożeń związanych z korzystaniem z Internetu artykuł prezentuje wyniki analizy przeprowadzonych badań (wykres 1), w których do respondentów skierowano poniższe pytania:

- Czy dla Pani/Pana internetowa pornografia współcześnie stanowi poważne zagrożenie bezpieczeństwa?

Internetowa pornografia współcześnie rozwija się w błyskawicznym tempie. Tak naprawdę pornografia towarzyszy całej ludzkości już od początku jej historii, natomiast to właśnie w wyniku rozwoju Internetu przeszła ona swego rodzaju zmianę jakościową. Jeśli zaś chodzi o dostęp do pornografii, to jest on uznany za zagrożenie globalne[9]. Na kontakt z internetową pornografią jest

[7] M. Tryboń, I. Grabowska-Lepczak, M. Kwiatkowski, *Bezpieczeństwo człowieka w obliczu zagrożeń XXI wieku*, „Zeszyty Naukowe SGSP" 2011, nr 41, s. 200.

[8] I.A. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 13–15.

[9] M. Niedźwiedź, *Problematyka prawna dostępu do treści pornograficznych w Internecie ze względu na ochronę dzieci z perspektywy prawa unijnego*, „Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego" 2017, t. 15.

tak naprawdę narażona każda osoba, która korzysta z sieci. Pornografia przekazuje nie tylko brutalność, ale również przemoc oraz wulgarność.

- Czy dla Pani/Pana internetowy werbunek do grup terrorystycznych i przemocowych współcześnie stanowi poważne zagrożenie bezpieczeństwa?

Ukazujące się działania powiązane z grupami terrorystycznymi bądź przemocowymi są poważnym zagrożeniem dla stabilności nie tylko grup społecznościowych i kulturowych, ale również państwa, a tym bardziej dla różnorodnych organizacji międzynarodowych. Werbunki, które mają przede wszystkim pozyskać nowych osobników, dotyczą działań związanych zarówno z psychomanipulacją, jak i indoktrynacją[10]. Poświęcenie się wyłącznie jednej idei prowadzi do podjęcia wszelakich działań o jakimkolwiek charakterze.

- Czy dla Pani/Pana poznawanie osób w celu handlu ludźmi współcześnie stanowi poważne zagrożenie bezpieczeństwa?

Poznawanie osób w celu handlu ludźmi stanowi poważne zagrożenie bezpieczeństwa. Sytuacje takie odbywają się z naprawdę różnorodnych względów, m.in. zmuszanie do usług seksualnych, pozyskiwanie dawców organów czy siły roboczej itp. Działania kierowane są w celu wykorzystywania człowieka bez względu na wiek czy też płeć[11]. Wszelkie takie czynności zaburzają podstawowe prawo, które dotyczy decydowania o sobie.

- Czy dla Pani/Pana współcześnie cyberseks stanowi poważne zagrożenie bezpieczeństwa?

Wirtualny stosunek odbierany jest jako zagrożenie, które w rzeczywistości nie jest postrzegane za dość poważne. Istotnym argumentem, który może wpływać na takie twierdzenie, to fakt, iż współcześnie znaczna część rzeczy oraz działań jest zależna od eksploracji nowoczesnych technik, natomiast przede wszystkim główną rolę pełni Internet. Naturalnie istnieją zarówno zwolennicy, jak i przeciwnicy takich metod, jednakże cyberseks prowadzi niestety do wielu kontrowersji etycznych, a co za tym idzie, występuje cały szereg niebezpieczeństw[12].

- Czy dla Pani/Pana współcześnie wyłudzanie pieniędzy stanowi poważne zagrożenie bezpieczeństwa?

Wyłudzanie jest niebezpiecznym oraz nielegalnym zjawiskiem, które głównie ma na celu kradzież danych osobowych bądź też wprowadzenie złośliwego oprogramowania do komputera, który w danym momencie staje się celem. Takie sytuacje często są stosowane poprzez wiadomości tekstowe wysyłane na numer telefonu komórkowego, jak również poprzez wiadomość e-mail[13]. Działania mające na celu wszelkie wyłudzenia współcześnie są jednymi z poważniejszych zagrożeń. Ponadto z dnia na dzień coraz bardziej ewoluują w różnorodne złożone formy. Dlatego też w każdej sytuacji, która bezpośrednio wiąże się z jakimkolwiek działaniem w Internecie, należy pamiętać, aby zachować zdrowy rozsądek.

[10] M. Jankowska, *Psychomanipulacja jako technika werbunku wykorzystywania przez sekty oraz ich fasadowe organizacje*, „Warmińsko-Mazurski Kwartalnik Naukowy, Nauki Społeczne" 2012, nr 4, s. 163–164.
[11] J. Rubiś-Kulczycka, *Handel ludźmi jako forma współczesnego niewolnictwa*, „Zeszyty Naukowe Uczelni Jana Wyżykowskiego. Studia z Nauk Społecznych" 2016, nr 9, s. 28–29.
[12] O. Sawajner, *Zalety i zagrożenia rozpowszechniania cyberseksu*, http://www.psychologia.net.pl/artykul.php?level=391 [dostęp: 10.04.2023].
[13] *Co to jest smishing i jak się przed nim chronić?*, https://www.omegasoft.pl/blog/co-to-jest-smishing-i-jak-sie-przed-nim-chronic/ [dostęp: 10.04.2023].

- Czy dla Pani/Pana współcześnie uzależnienie od Internetu stanowi poważne zagrożenie bezpieczeństwa?

We współczesnym świecie uzależnienie od Internetu nieustannie przybiera na sile, w szybkim tempie pozyskując nowych użytkowników. Niestety dotychczas zjawisko to nie zostało spójnie zdefiniowane wraz z odpowiednio określającymi przepisami, dotyczącymi jego diagnostyki. Nadużywanie funkcjonowania w Internecie prowadzi do wielu negatywnych skutków, które są w stanie zaburzyć całokształt działań człowieka. Według psycholog Kimberly S. Young można wyróżnić pięć podstawowych rodzajów uzależnień od sieci komputerowej: uzależnienie od komputera (*computer addiction*); erotomania internetowa (*cybersexual addiction*); socjomania internetowa (*cyber-relationship addiction*); przeciążenie informacyjne (*information overload*) oraz uzależnienie od sieci internetowej (*net compulsions*)[14]. Problem powyższego zjawiska wystąpił, gdy dostęp do sieci rozpowszechnił się na skalę masową.

- Czy dla Pani/Pana wpływ Internetu na zdrowie psychiczne współcześnie stanowi poważne zagrożenie bezpieczeństwa?

Nadmierne korzystanie z Internetu prowadzi do różnorodnych problemów, które powiązane są w sposób bezpośredni ze zdrowiem psychicznym człowieka[15]. Szybkie przekazywanie dużej ilości informacji w sieci sprawia, że mózg człowieka staje się przeciążony, co może doprowadzić do negatywnych odczuć. W ten sposób umiejętność zapamiętywania staje się coraz słabsza, co prowadzi również do braku koncentracji. W takich chwilach często pojawia się poczucie przytłoczenia. Co istotne, działania takie mogą prowadzić do silnych stanów lękowych, a co gorsza – do depresji.

- Czy dla Pani/Pana wyizolowanie społeczne współcześnie stanowi poważne zagrożenie bezpieczeństwa?

Współcześnie wyizolowanie dotyka najczęściej młodzieży, dlatego też istotnym aspektem jest to, aby w razie zauważenia przejawów takiej sytuacji, sprawdzić, co się dzieje z daną osobą. Osoby wyizolowane często czują się samotne, co negatywnie wpływa na ich samoocenę. Ponadto towarzyszy im odczucie, że są, z jakiegoś względu, odłączone od świata rzeczywistego[16]. Niestety przez występującą globalizację oraz rozwój technologii liczba zagubionych i wyizolowanych osób wzrasta. Izolacja społeczna często ma wpływ m.in. na: emocje, zachowania społeczne, poziom stresu czy sen.

- Czy dla Pani/Pana rezygnacja z rozrywek (innych niż te w sieci) lub ich zawężanie współcześnie stanowi poważne zagrożenie bezpieczeństwa?

Rezygnując z rozrywek w świecie rzeczywistym, nie tylko zatraca się samego siebie, lecz również tracą na wartości znajomości, które były utrzymywane. Należy rozróżnić czas poświęcany w wirtualnym świecie i w tym rzeczywistym. Jest to dość istotny aspekt, gdyż przez takie zachowania zawężamy swój światopogląd oraz różnorodne zainteresowania, które są zatracane przez czas spędzany wyłącznie w sieci. Powinno się mieć na uwadze, że kolejne pokolenia będą funkcjonowały w czasach, gdy technologia będzie na jeszcze wyższym poziomie niż teraz.

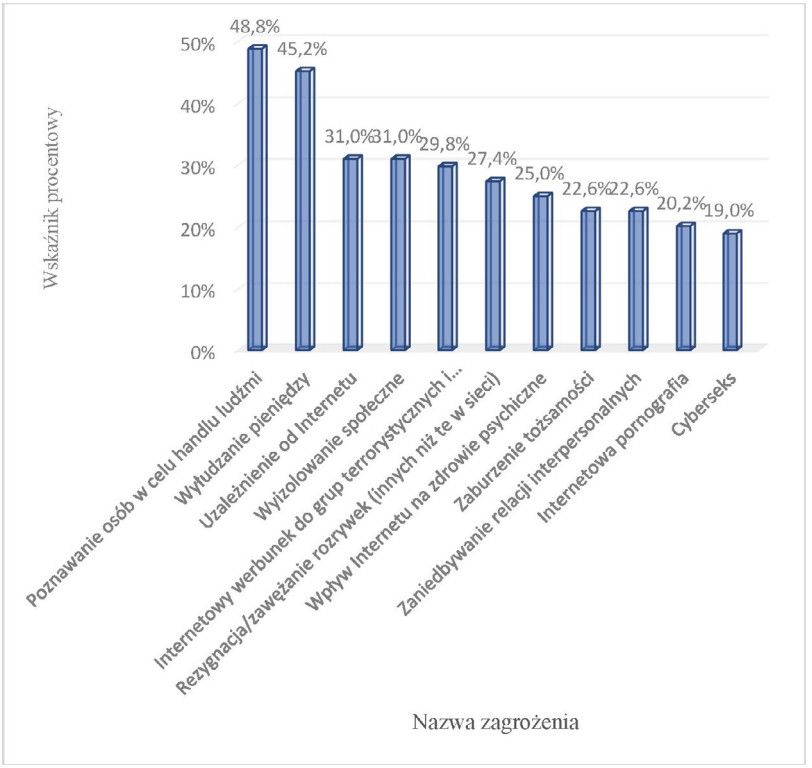
[14] K.S. Young, *Caught in the Net: How to Recognize the Signs of Internet Addiction – and A Winning Strategy for Recovery*, New York 1998.
[15] Ł. Stawikowski, *Uzależnienie od internetu – objawy i leczenie siecioholizmu*, https://www.medicover.pl/o-zdrowiu/uzaleznienie-od-internetu-objawy-i-leczenie-siecioholizmu,6339,n,192 [dostęp: 10.04.2023].
[16] *Izolacja społeczna – definicja i sposoby jej przezwyciężania*, https://www.edulider.pl/rozwoj/izolacja-spoleczna-definicja-i-sposoby-jej-przezwyciezania [dostęp: 10.04.2023].

- Czy dla Pani/Pana zaburzenie tożsamości współcześnie stanowi poważne zagrożenie bezpieczeństwa?

Jest to dość ważne zjawisko, gdyż współcześnie osoby funkcjonujące w Internecie posiadają szeroki zakres możliwości konstruowania zupełnie odmiennej tożsamości. Zjawiska takie są związane z faktem, że najgłębsza koncentracja współzależna jest z własną osobą, która silnie potrzebuje być zauważona. Jednakże zaburzenia tożsamości występują często po traumatycznych i bolesnych przeżyciach. Osoba z zaburzeniem tożsamości do zinternalizowania zdarzeń naciskających z zewnątrz jest w stanie doświadczać swego rodzaju poczucia emocjonalnego rozregulowania, które prowadzi do dysocjacji osobowości[17].

- Czy dla Pani/Pana współcześnie zaniedbywanie relacji interpersonalnych stanowi poważne zagrożenie bezpieczeństwa?

Zaniedbywanie relacji interpersonalnych prowadzi do poważnych problemów występujących w relacjach międzyludzkich. Wszelkie zaniechania mogą doprowadzić do trudności związanych z kształtowaniem stosunków z osobami, z którymi dana jednostka utrzymywała relację przez długi czas. Głównymi przeszkodami w występujących relacjach interpersonalnych są nieadaptacyjne strategie radzenia sobie. Problemy takie będą cały czas nawracać, jeśli nie podejmie się odpowiednich kroków, by je zwalczyć.



Wykres 1. Internet – medium współczesnych zagrożeń
Źródło: opracowanie własne.

[17] W. Orlof, K.M. Wilczyńska, N. Waszkiewicz, *Dysocjacyjne zaburzenie tożsamości (osobowość mnoga) – powszechniejsze niż wcześniej sądzono*, „Psychiatria" 2018, t. 15, nr 4, s. 229.

2. Cyberbezpieczeństwo w XXI wieku

Globalna możliwość preferencji Internetu stała się dość ważnym aspektem w ciągu ostatnich lat. Z tego powodu bardzo ważne są działania związane bezpośrednio z cyberbezpieczeństwem, gdyż są one w stanie zmniejszyć ryzyko potencjalnych zagrożeń płynących ze stron sieci internetowych. Najprościej cyberbezpieczeństwo można zdefiniować jako swego rodzaju strategie lub procedury, które są stosowane przez osoby, grupy społecznościowe, przedsiębiorstwa itp., by osłabiać wszelkie niechciane działania[18]. Jak podaje (Mini)Słownik BBN cyberbezpieczeństwo to:

> transsektorowy obszar bezpieczeństwa, obejmujący proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego elementów (struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej oraz będących w ich dyspozycji systemów teleinformatycznych i zasobów informacyjnych)[19].

Nadrzędnym celem cyberbezpieczeństwa jest ukazanie czynności, które są powiązane bezpośrednio z projektowaniem oraz zarządzaniem bezpieczeństwem odpowiednich systemów informatycznych, jak również dopilnowanie osób, które są odpowiedzialne za sfery poprawnego funkcjonowania. Ponadto podczas wdrażania systemów informatycznych cyberbezpieczeństwo powinno być zawsze brane pod uwagę jako jedno z pierwszych elementów, gdyż tworzy pewną podstawę utrzymującą resztę działań. Należy jednak pamiętać, iż cyberbezpieczeństwo to zupełnie co innego niż bezpieczeństwo informacji (zawiera ono szerszy zakres wykonywanych czynności).

Kolejnym ważnym aspektem jest to, że cyberbezpieczeństwo stało się nierozłącznym elementem funkcjonowania całej ludzkości[20]. Jest tak, gdyż współcześnie rozmaite przedmioty technologiczne są spójne z codziennymi działaniami praktycznie każdego człowieka – mowa głównie o telefonach komórkowych, laptopach, tabletach itd. Głównie na cyberbezpieczeństwo stawiają firmy, które nie mogą pozwolić sobie na jakiekolwiek błędy. Stosowane procedury względem bezpieczeństwa powinny być wzmacniane i opierane w szczególności na dobranych środkach technicznych. Kluczowym kontekstem jest w tym momencie wiedza, na skutek której będzie istniała możliwość zminimalizowania szkodzących działań.

Najistotniejsze standardy IT względem cyberbezpieczeństwa powinny być realizowane za pomocą:

- NIST (ang. *National Institute of Standards and Technology*) SP 800-115 – przewodnik techniczny do prowadzenia testów bezpieczeństwa;
- OSSTMM (ang. *Open Source Security Testing Methodology Manual*) – recenzowany podręcznik służący do testowania i analizy zabezpieczeń;
- ISSAF (ang. *Information Systems Security Assessment Framework*) – tzw. metodyka OISSG (ang. *Open Information Systems Security Group),* opierająca się na weryfikacji strategii bezpieczeństwa;
- OWASP (ang. *The Open Web Application Security Project*) – metodyka dotycząca prowadzenia testów penetracyjnych;
- WASC (ang. *Web Application Security Consortium*) – opracowywanie oraz szerzenie norm bezpieczeństwa w Internecie[21].

---

[18] K. Wojciechowska, *Cyberbezpieczeństwo – definicja*, https://isportal.pl/cyberbezpieczenstwo-definicja/ [dostęp: 11.04.2023].
[19] Biuro Bezpieczeństwa Narodowego, *(Mini)Słownik BBN: Propozycje nowych terminów z dziedziny bezpieczeństwa,* http://katedrawiss.uwm.edu.pl/sites/default/files/download/202005/minislownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.pdf [dostęp: 11.04.2023].
[20] *Cyberbezpieczeństwo wyzwaniem XXI wieku*, red. T. Dębowski, Łódź–Wrocław 2018, s. 34–25.
[21] J. Krawiec, P. Górny, *Cyberbezpieczeństwo – podejście systemowe*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia ASzWoj" 2016, nr 2, s. 12.

Mając na względzie występujące współcześnie działania oraz ryzyko potencjalnych zagrożeń wypływających z sieci internetowych przeciwko cyberbezpieczeństwu, poniżej przedstawiono wyniki analizy przeprowadzonych badań (wykres 2). Do respondentów skierowano poniższe pytania:

- Czy dla Pani/Pana współcześnie ataki *ransomware* stanowią poważne zagrożenie bezpieczeństwa?

Takie ataki powiązane są z ograniczeniem jakiegokolwiek dostępu do systemu komputerowego bądź uniemożliwiają odczyt danych zawartych w danym urządzeniu. Ponadto takie działania wymagają zapłacenia okupu, by zlikwidować założoną wcześniej blokadę[22]. Głównym celem tzw. cyberprzestępców poprzez powyższy atak jest chęć wyłudzenia w większości przypadków pieniędzy, w zamian za co miałby zostać przywrócony stan pierwotny danej aparatury. Jednakże nie zawsze przestępcy internetowi po uzyskaniu okupu usuwają nałożoną wcześniej blokadę.

- Czy dla Pani/Pana współcześnie ataki *phishingowe* stanowią poważne zagrożenie bezpieczeństwa?

Ataki *phishingowe* to metoda oszustwa, która dotyczy bezpośrednio przestępcy podszywającego się pod zupełnie kogoś innego (dotyczy to również firm i różnorodnych instytucji). Główny cel takich działań dotyczy przede wszystkim wyłudzenia zarówno prywatnych, jak i poufnych informacji lub „zaatakowania" określonego urządzenia szkodliwym oprogramowaniem[23]. Większość takich przedsięwzięć odbywa się poprzez wysyłanie wiadomości lub linków do stron internetowych na konta e-mail oraz na różnorodne konta społecznościowe.

- Czy dla Pani/Pana współcześnie ataki hakerskie stanowią poważne zagrożenie bezpieczeństwa?

Działaniami takimi kierują różne motywy, które mogą dotyczyć przede wszystkim uzyskania rozgłosu czy po prostu wywołania zamieszania na większą skalę[24]. Hakerzy często pragną również pozyskać różnorodne informacje w celu późniejszego uzyskania okupu. Osoby powiązane z takimi działaniami są również nazywane *crackerami*[25]. Jednakże oni skupiają się głównie na łamaniu zabezpieczeń serwerów oraz oprogramowania.

- Czy dla Pani/Pana współcześnie *spyware* stanowi poważne zagrożenie bezpieczeństwa?

Współcześnie każdy użytkownik Internetu musi być świadomy, że jest narażony na zagrożenie, które występuje w postaci *spyware*. Są to zagrożenia, które pozostają całkowicie niezauważalne, dlatego też powszedni użytkownik może nie być świadomy występującego ryzyka. Najprościej mówiąc, *spyware* jest definiowane jako szkodliwe oprogramowanie, które jest w stanie monitorować kompletną aktywność danego urządzenia[26]. Dzieje się tak, gdyż działa ono zwykle w tle, dlatego też jest w stanie przez dłuższy czas zostać niezauważone. Działania takie mają głównie na celu uzyskać poufne dane użytkownika, m.in. loginy i hasła, PESEL itp.

---

[22] *Ataki ransomware – niezwykle skuteczna broń przestępców*, https://testarmy.com/pl/blog/ataki-ransomware-niezwykle-skuteczna-bron-przestepcow/ [dostęp: 11.04.2023].

[23] *Czym są ataki phishingowe?*, https://www.trendmicro.com/pl_pl/what-is/phishing/phishing-attacks.html [dostęp: 11.04.2023].

[24] *Hakerzy i hakowanie 101*, https://pl.malwarebytes.com/hacker/#:~:text=Hakerstwo%20odnosi%20si%C4%99%20do%20dzia%C5%82a%C5%84,tablety%2C%20a%20nawet%20ca%C5%82e%20sieci [dostęp: 11.04.2023].

[25] „Hakerzy, którzy niszczą cudze pliki lub całe dyski twarde – nazywa się ich crakerami lub po prostu wandalami", zob. K.D Mitnick, W.L. Simon, *The Art of Deception: Controlling the Human Element of Security*, Indianapolis 2002.

[26] https://www.veracode.com/security/spyware#:~:text=Spyware%20is%20any%20software%20that,this%20data%20to%20other%20parties [dostęp: 12.04.2023].

- Czy dla Pani/Pana współcześnie VoIP stanowi poważne zagrożenie bezpieczeństwa?

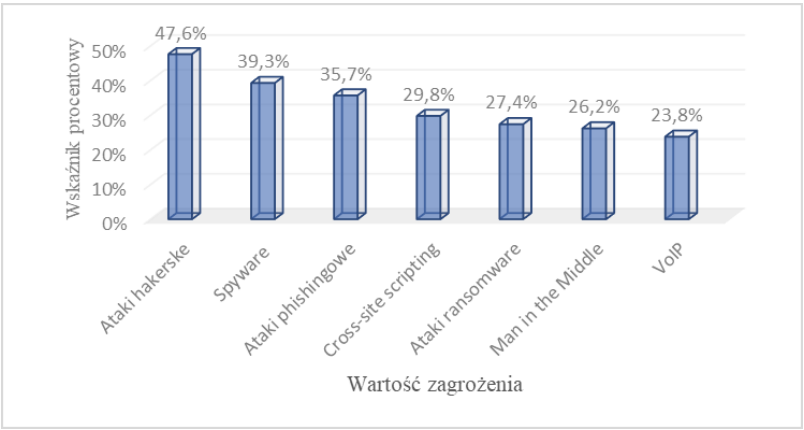
VoIP popularnie jest określany mianem internetowej telefonii. Jest to technika, która umożliwia przesyłanie dźwięków mowy za pomocą sieci, wykorzystując protokół IP lub przesyłanie poprzez łącza internetowe[27]. Jednakże największą wadą, a zarazem występującym zagrożeniem ze strony VoIP, jest brak jakichkolwiek standardów odnoszących się bezpośrednio do zabezpieczeń przed podsłuchem. Ponadto występuje wysoka podatność ataków typu DoS na bramki VoIP.

- Czy dla Pani/Pana współcześnie *cross-site scripting* stanowi poważne zagrożenie bezpieczeństwa?

XSS (również takie oznaczenie przyjmuje dane zagrożenie) jest dość istotnie zagrażającym działaniem, które ukazuje się na łączach internetowych. Jest to swego rodzaju luka, występująca zazwyczaj w internetowych aplikacjach. Ponadto jednostki atakujące są w stanie wykorzystać lukę w zabezpieczeniach skryptów, które ukazują się pomiędzy lokacjami w celu ominięcia jakichkolwiek kontroli dostępu[28].

- Czy dla Pani/Pana współcześnie *Man in the Middle* stanowi poważne zagrożenie bezpieczeństwa?

Działania *Man in the Middle* to ataki kryptologiczne, które polegają przede wszystkim na podsłuchu oraz różnorodnej modyfikacji wiadomości pomiędzy np. dwoma jednostkami bez ich wiedzy. Należy mieć na względzie, że to jedne z poważniejszych ataków aktywnych w Internecie[29]. Istotnym aspektem jest także to, że działania takie są zarówno próbą odczytu wszelkich informacji zaszyfrowanych, jak i próbami dotyczącymi różnorodnych oszustw.



Wykres 2. Cyberbezpieczeństwo w XXI w.
Źródło: opracowanie własne.

[27] M. Sikorski, *Internet jako determinanta rozwoju sektora małych i średnich przedsiębiorstw*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej w Płocku. Nauki Ekonomiczne" 2018, t. 28.
[28] https://owasp.org/www-community/attacks/xss/#:~:text=Cross%2DSite%20Scripting%20(XSS),to%20a%20different%20end%20user. [dostęp: 12.04.2023].
[29] P. Szmaj, *Atak Man in the middle. Na czym polega i jak się przed nim bronić?*, https://geek.justjoin.it/atak-man-in-the-middle-na-czym-polega-i-jak-sie-przed-nim-bronic/ [dostęp: 12.04.2023].

3. Trollowanie jako metoda ataku w Internecie

Współcześnie Internet zawiera w sobie swego rodzaju różnorodność, która posiada zarówno zalety, jak i wady. Z perspektywy czasu można zauważyć, iż działania powiązane bezpośrednio z siecią internetową zmieniają całkowicie całokształt porozumiewania się pomiędzy ludźmi, a więc jednocześnie w tym kontekście następuje modyfikacja stylu komunikacji.

Zagłębiając się w internetowe style komunikowania, można natknąć się na wiele osób, grup bądź społeczności, które prowadzą wielorakie działania na arenie całego Internetu, a jednym z nich jest właśnie tzw. trollowanie. Jeśli chodzi o samą genezę, jak również znaczenie powyższego wyrazu, to czasownik *troll* wywodzi się ze starofrancuskiego *troller*, który jest terminem myśliwskim, natomiast jeśli mamy na myśli rzeczownik *troll* to pochodzi on z mitologii i oznacza potwora[30]. Ponadto trolle to także stworzenia, które ukazują się w skandynawskich bajkach i są przedstawiane jako sprytne, podstępne, a zarazem bardzo psotne.

Obecnie trollowanie pochodzi z języka angielskiego – *trolling for fish*, a oznacza metodę łowienia ryb na haczyk i tak właśnie działają dzisiejsze trolle, gdyż „zarzucają one haczyk" na swoją przynętę w celu sprowokowania i doprowadzenia do kłótni[31].

> Znaczenie terminu było wyrażone w Internecie w późnych latach osiemdziesiątych XX wieku, ale pierwszy znany przykład pochodzi z 1992 r. Pierwsze, niezwiązane z Internetem, wykorzystanie *trollingu* w kontekście umyślnej działalności prowokacyjnej udokumentowano w lotnictwie armii amerykańskiego w 1972 r. w Wietnamie[32].

Dzisiaj trollowanie określane jest jako zachowanie chuligańskie, a przede wszystkim patologiczne. Działania takie odbywają się zazwyczaj poprzez opublikowanie prowokujących, dygresyjnych, a także niezwiązanych z tematem wiadomości w określonej społeczności internetowej, m.in. forum, grupa dyskusyjna, blog, czat oraz serwisy społecznościowe. Głównym zamiarem takich czynności jest sprowokowanie czytelników do wyrażania reakcji emocjonalnych i normalizacja dyskusji tangencjalnej. Ponadto trollowanie można utożsamiać z nękaniem w Internecie, dlatego też w środowisku internetowym używa się terminu *troll* na oznaczenie osoby, która wybitnie stara się z pomocą podżegających postów, komentarzy i wiadomości krzywdzić innych. Trollem jest również osoba, która w sposób agresywny reaguje wtedy, gdy ktoś z danej grupy społecznościowej próbuje załagodzić wcześniej zaostrzoną sytuację. W następstwie tego, im bardziej zaistniały spór pomiędzy ludźmi wzrasta, tworząc coraz to większą kłótnię, tym troll jest bardziej zadowolony i dumny z siebie[33]. „*Trollem* może być również *lamer*, czyli użytkownik, który słabo zna temat, ale za wszelką cenę próbuje udowodnić, że jest inaczej. Taka osoba często dużo dyskutuje i udaje profesjonalistę, używając zwrotów bardzo oczywistych"[34]. Wskutek czego często zostaje demaskowana przez świadomych i dojrzałych użytkowników, natomiast następstwem takich działań jest zablokowanie danej osoby przez administratora określonej strony.

Poniżej przedstawiono wyniki analizy przeprowadzonych badań, związanych bezpośrednio z trollowaniem w Internecie (wykres 3). Do respondentów skierowano poniższe pytania:

---

[30] D. Jachyra, *Trollowanie – antyspołeczne zachowania w Internecie, sposoby wykrywania i obrony*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Informatica" 2011, nr 28, s. 253.
[31] Tamże, s. 260.
[32] Tamże, s. 254.
[33] *Trolle w internecie. Jak manipulują informacją w sieci?*, https://www.omegasoft.pl/blog/trolle-w-internecie-jak-manipuluja-informacja-w-sieci/ [dostęp: 12.04.2023].
[34] Tamże, s. 255.

- Czy dla Pani/Pana współcześnie nieprawdziwe treści stanowią poważne zagrożenie bezpieczeństwa?

Nieprawdziwe treści to informacje, które są przedstawione w sposób niezgodny z rzeczywistością i nie posiadają jakiegokolwiek potwierdzenia bezpośrednio dotyczącego działań w stanie faktycznym[35]. Takie treści często prowadzą do różnego rodzaju nieporozumień, kłótni, a także do niepożądanych działań.

- Czy dla Pani/Pana współcześnie działania prowokacyjne stanowią poważne zagrożenie bezpieczeństwa?

Głównym celem prowokacji jest spowodowanie reakcji m.in. na osobie, która jest uznawana za ofiarę danego przedsięwzięcia, zazwyczaj niekorzystnie wpływającego na nią lub na osoby, grupy czy też organizacje z nią powiązane[36]. Działania prowokacyjne zazwyczaj prowadzone są przez jedną osobę, która jest odpowiedzialna za wszystkie wykonywane manewry i jest ona nazywana prowokatorem. To właśnie takie osoby zachęcają innych do popełnienia czynu, który jest całkowicie zabroniony. Często takie zachowania mają na celu skierowanie postępowania karnego przeciwko określonej osobie. Prowokatorzy najpierw zachęcają jednostkę do działań, natomiast później osobiście informują odpowiednie służby o sytuacjach, które w danym momencie się odgrywają.

- Czy dla Pani/Pana współcześnie spamowanie stanowi poważne zagrożenie bezpieczeństwa?

Spamem współcześnie określane są niechciane wiadomości elektroniczne, których główną cechą jest masowe rozsyłanie treści do przypadkowych, nieznanych odbiorców[37]. Należy mieć również na względzie, że spam istniał praktycznie od samego początku pojawienia się Internetu. Osobę bezpośrednio zajmującą się spamowaniem określa się mianem spamera. To właśnie takie osoby często przesyłają e-maila posiadającego wirusa (najczęściej spełniającego rolę typu konia trojańskiego), który po otworzeniu wiadomości samoczynnie instaluje się na komputerze, telefonie czy też tablecie i jest w stanie przesłać spamerowi wszelkie dane użytkownika, jak również cenne informacje.

- Czy dla Pani/Pana współcześnie brak znajomości netykiety stanowi poważne zagrożenie bezpieczeństwa?

Netykieta to swego rodzaju zbiór zasad i zobowiązań, które dotyczą odpowiedniego zachowania obowiązującego w Internecie. Na ten moment nikt oficjalnie nie zajmuje się karaniem osób, które nie przestrzegają netykiety, aczkolwiek osoby ciągle narażające się i łamiące zasady mogą zostać wyrzucone, zablokowane przez określonego administratora bądź zgłoszone do odpowiedniego działu[38]. Istotnym aspektem jest również to, że odpowiednie stosowanie netykiety jest w stanie zapewnić prawidłową komunikację w Internecie.

- Czy dla Pani/Pana współcześnie żądania wobec innych użytkowników stanowią poważne zagrożenie bezpieczeństwa?

---

[35] *Rozpoznawanie nieprawdziwych informacji*, https://www.gov.pl/web/baza-wiedzy/rozpoznawanie-nieprawdziwych-informacji [dostęp: 12.04.2023].
[36] S. Pikulski, *Podstawowe zagadnienia taktyki kryminalistycznej*, Białystok 1997, s. 93–96.
[37] *Co to jest spam i jak się przed nim chronić?*, https://kapitalni.org/pl/artykuly/co-to-jest-spam-i-jak-sie-przed-nim-chronic [dostęp: 14.04.2023].
[38] R. Lorens, *Netykieta, czyli jak być kulturalnym w internecie…*, https://www.mac.pl/aktualnosci/netykieta-czyli-jak-byc-kulturalnym-w-internecie [dostęp: 14.04.2023].

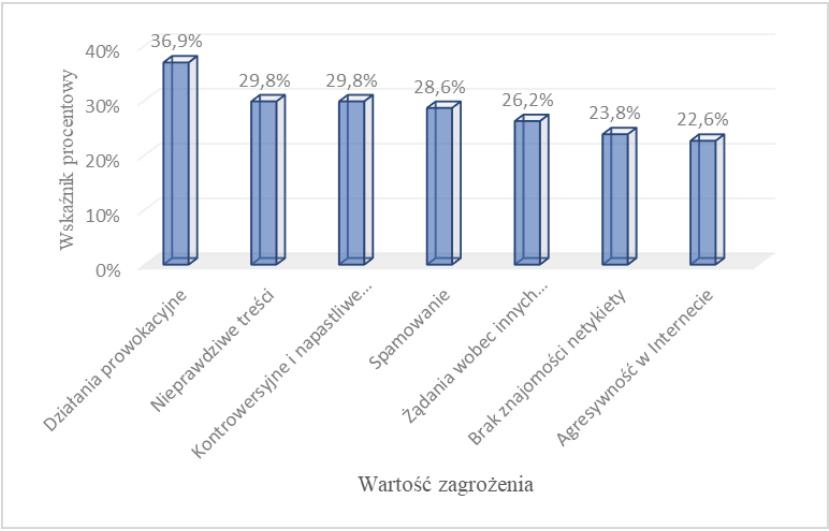
Działania takie z roku na rok stają się coraz bardziej powszechne, natomiast osoby korzystające z przeróżnych platform mogą nie zdawać sobie z tego sprawy. Zarówno indywidualne jednostki, jak i grupy pod pretekstem lub zwykłym naciskiem zmuszają innych użytkowników do działań, które mogą być np. niedozwolone bądź nawet karalne. Presja wywierana na osobę narażoną na określone żądanie jest równie istotnym aspektem. Wobec takich osób często są stosowane wyłudzenia np. danych osobistych i majątkowych, wykorzystując wcześniej pozyskane fotografie lub filmy, które niekoniecznie okazują się prawdziwe – w większości sytuacji w celu zastraszenia stosowany jest tzw. fotomontaż.

- Czy dla Pani/Pana współcześnie agresywność w Internecie stanowi poważne zagrożenie bezpieczeństwa?

Należy mieć na względzie, że ówcześnie Internet niesie za sobą wiele niespokojnych, wręcz nieodpowiednich dla użytkowników wartości, których wpływ i znaczenie stale się rozszerzają. Aktualnie nie można bezpośrednio wskazać głównej przyczyny agresywności w sieci, gdyż na ten stan składa się wiele czynników, które łącznie tworzą tzw. ciąg przyczynowo-skutkowy. Jednym z takich czynników jest przede wszystkim anonimowość, która daje większości ludzi pewną swobodę. Kolejną przyczyną może być także występująca przemoc słowna, która daje poczucie swego rodzaju bezkarności oraz możliwość znieważania innych.

- Czy dla Pani/Pana współcześnie kontrowersyjne i napastliwe przekazy stanowią poważne zagrożenie bezpieczeństwa?

Określone zagrożenie dotyczy głównie zamierzonych ataków na dane jednostki, a także grupy społecznościowe. Ponadto kontrowersyjne i napastliwe przekazy są uznawane za złamanie podstawowych zasad dotyczących netykiety. W Internecie częściej uaktywniają się osoby, które są skłonne do obrażania innych. Myśląc, że są całkowicie anonimowe, nie zwracają uwagi na sposób, w jaki odnoszą się do użytkowników czy na konsekwencje swoich działań. Natomiast ówcześnie znaczną część społeczności nie dziwi już kontrowersyjny nieparlamentarny język, który jest używany w sieci.



Wykres 3. Trollowanie jako metoda ataku w Internecie
Źródło: opracowanie własne.

5. Wnioski

Internet jest obecnie uważany za źródło różnorodnych zagrożeń. Konieczne jest zwrócenie uwagi na wszelkie potencjalne szkodliwe działania wynikające z posiadania globalnej sieci, ponieważ nieodpowiednie korzystanie może prowadzić do negatywnych skutków i naruszenia prawa, a nawet do poważnych incydentów.

Cyberbezpieczeństwo w erze XXI w. jest ważnym obszarem, który powinien być intensywnie rozwijany w celu zapewnienia najlepszych możliwych zabezpieczeń w czasach Internetu. Wszelkiego rodzaju przedsięwzięcia powiązane bezpośrednio z cyberbezpieczeństwem powinny być realizowane w sposób rzetelny oraz kompetentny, aby dane znajdujące się na urządzeniach elektronicznych były odpowiednio zabezpieczone. Cyberbezpieczeństwo często jest określane jako systemy lub techniki odporne na niepożądane działania pochodzące z sieci. Takie działania mają głównie na celu ochronę oraz zabezpieczenie urządzeń technologicznych, np. poprzez programy antywirusowe, natomiast podstawą podczas korzystania z Internetu jest własna czujność. Należy mieć także na względzie, iż cyberbezpieczeństwo jest nierozłącznym elementem działalności i rozwoju całej ludzkości. Współcześnie technologia jest wręcz spójna z człowiekiem, dając mu jednocześnie możliwość rozwoju. Warto jednak posiadać jakąkolwiek wiedzę dotyczącą wielokształtności, jaką potrafi przybrać Internet.

W kontekście komunikacji w Internecie istnieje wiele terminów odnoszących się do tego zagadnienia. Niemniej jednak, zarówno w sieci, jak i w życiu codziennym, możemy natknąć się na osoby, które celowo chcą wyrządzić krzywdę innym. Dlatego też na takie osoby oraz ich zachowanie w Internecie istnieje określenie – troll (osoba) i trollowanie (zachowanie). Należy mieć na względzie, że trollowanie charakteryzuje się głównie zachowaniem antyspołecznym, które odbywa się na różnych czatach, blogach, a także serwisach społecznościowych. Troll podczas swoich ataków skupia uwagę głównie na jednej osobie bądź wydarzeniu i wykonuje odpowiednie manewry, by skutecznie upokorzyć wcześniej wytypowany cel. Kontrowersja i napastliwość to jedne z głównych działań trollowania, gdyż im bardziej troll ośmieszy daną jednostkę lub doprowadzi do kłótni grupę społecznościową, tym bardziej będzie z siebie zadowolony. Równie istotnym aspektem jest to, że działania stosowane przez trolli w powszechnej opinii wynikają z braku wiedzy na temat kultury w Internecie i stanowią złamanie podstawowych zasad określanych jako netykieta.

Podsumowując, dzisiejsze środowisko internetowe, które jest pełne zagrożeń, wymaga odpowiedniej uwagi i ochrony. Cyberbezpieczeństwo ma dziś ogromne znaczenie i powinno być intensywnie rozwijane, aby jak najlepiej chronić dane i urządzenia elektroniczne. Ważna jest również osobista czujność i znajomość zasad netykiety, aby uniknąć niechcianych zachowań ze strony trolli i tych, którzy świadomie starają się skrzywdzić innych. Internet z jednej strony daje nam możliwość rozwoju i komunikowania się na poziomie globalnym, lecz z drugiej strony wymaga od nas świadomej odpowiedzialności i wynikających z niej zagrożeń. Warto pamiętać, że cyberbezpieczeństwo stanowi integralny element rozwoju człowieka, dlatego należy podchodzić do niego z najwyższą powagą.

BIBLIOGRAFIA

Artykuły i monografie

Cieśleńska B., Bruździński M., *Obszary użytkowania Internetu we współczesnym obliczu sieci*, „Społeczeństwo. Edukacja. Język" 2016, t. 4.

Cyberbezpieczeństwo wyzwaniem XXI wieku, red. T. Dębowski, Łódź–Wrocław 2018.

Hofmokl J., *Internet jako nowe dobro wspólne*, Warszawa 2009.

Jachyra D., *Trollowanie – antyspołeczne zachowania w Internecie, sposoby wykrywania i obrony*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Studia Informatica" 2011, nr 28.

Jankowska M., *Psychomanipulacja jako technika werbunku wykorzystywania przez sekty oraz ich fasadowe organizacje*, „Warmińsko-Mazurski Kwartalnik Naukowy, Nauki Społeczne" 2012, nr 4.

Jaroszewska I.A., *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017.

Krawiec J., Górny P., *Cyberbezpieczeństwo – podejście systemowe*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej" 2016, nr 2.

Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.

Mitnick K., Simon W.L., *The Art of Deception: Controlling the Human Element of Security*, Indianapolis 2002.

Niedźwiedź M., *Problematyka prawna dostępu do treści pornograficznych w Internecie ze względu na ochronę dzieci z perspektywy prawa unijnego*, „Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego" 2017, t. 15.

Orlof W., Wilczyńska K.M., Waszkiewicz N., *Dysocjacyjne zaburzenie tożsamości (osobowość mnoga) – powszechniejsze niż wcześniej sądzono*, „Psychiatria" 2018, t. 15, nr 4.

Pikulski S., *Podstawowe zagadnienia taktyki kryminalistycznej*, Białystok 1997.

Rubiś-Kulczycka J., *Handel ludźmi jako forma współczesnego niewolnictwa*, „Zeszyty Naukowe Uczelni Jana Wyżykowskiego. Studia z Nauk Społecznych" 2016, nr 9.

Sikorski M., *Internet jako determinanta rozwoju sektora małych i średnich przedsiębiorstw*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej w Płocku. Nauki Ekonomiczne" 2018, t. 28.

Technologiczno-społeczne oblicza XXI wieku, red. D. Gałuszka, G. Ptaszek, D. Żuchowska-Skiba, Kraków 2016.

Tryboń M., Grabowska-Lepczak I., Kwiatkowski M., *Bezpieczeństwo człowieka w obliczu zagrożeń XXI wieku*, „Zeszyty Naukowe SGSP" 2011, nr 41.

Young K.S., *Caught in the Net: How to Recognize the Signs of Internet Addiction – and A Winning Strategy for Recovery*, New York 1998.

Źródła internetowe

Ataki ransomware – niezwykle skuteczna broń przestępców, https://testarmy.com/pl/blog/ataki-ransomware-niezwykle-skuteczna-bron-przestepcow/ [dostęp: 11.04.2023].

Biuro Bezpieczeństwa Narodowego, *(Mini)Słownik BBN: Propozycje nowych terminów z dziedziny bezpieczeństwa*, http://katedrawiss.uwm.edu.pl/sites/default/files/download/202005/minislownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.pdf [dostęp: 11.04.2023].

Co to jest smishing i jak się przed nim chronić?, https://www.omegasoft.pl/blog/co-to-jest-smishing-i-jak-sie-przed-nim-chronic/ [dostęp: 10.04.2023].

Co to jest spam i jak się przed nim chronić?, https://kapitalni.org/pl/artykuly/co-to-jest-spam-i-jak-sie-przed-nim-chronic [dostęp: 14.04.2023].

Czym są ataki phishingowe?, https://www.trendmicro.com/pl_pl/what-is/phishing/phishing-attacks.html [dostęp: 11.04.2023].

Hakerzy i hakowanie 101, https://pl.malwarebytes.com/hacker/#:~:text=Hakerstwo%20odnosi%20si%C4%99%20do%20dzia%C5%82a%C5%84,tablety%2C%20a%20nawet%20ca%C5%82e%20sieci [dostęp: 11.04.2023].

Lorens R., *Netykieta, czyli jak być kulturalnym w internecie…*, https://www.mac.pl/aktualnosci/netykieta-czyli-jak-byc-kulturalnym-w-internecie [dostęp: 14.04.2023].

Rozpoznawanie nieprawdziwych informacji, https://www.gov.pl/web/baza-wiedzy/rozpoznawanie-nieprawdziwych-informacji [dostęp: 12.04.2023].

Sawajner O., *Zalety i zagrożenia rozpowszechniania cyberseksu*, http://www.psychologia.net.pl/artykul.php?level=391 [dostęp: 10.04.2023].

Stawikowski Ł., *Uzależnienie od internetu – objawy i leczenie siecioholizmu*, https://www.medicover.pl/o-zdrowiu/uzaleznienie-od-internetu-objawy-i-leczenie-siecioholizmu,6339,n,192 [dostęp: 10.04.2023].

Szmaj P., *Atak Man in the middle. Na czym polega i jak się przed nim bronić?*, https://geek.justjoin.it/atak-man-in-the-middle-na-czym-polega-i-jak-sie-przed-nim-bronic/ [dostęp: 12.04.2023].

Trolle w internecie. Jak manipulują informacją w sieci?, https://www.omegasoft.pl/blog/trolle-w-internecie-jak-manipuluja-informacja-w-sieci/ [dostęp: 12.04.2023].

What is the Internet backbone?, https://www.arelion.com/knowledge-hub/what-is-guides/what-is-the-internet-backbone [dostęp: 9.04.2023].

Wojciechowska K., *Cyberbezpieczeństwo – definicja*, https://isportal.pl/cyberbezpieczenstwo-definicja/ [dostęp: 11.04.2023].

https://owasp.org/www-community/attacks/xss/#:~:text=Cross%2DSite%20Scripting%20(XSS),to%20a%20different%20end%20user [dostęp: 12.04.2023].

https://techterms.com/definition/backbone [dostęp: 9.04.2023].

https://www.edulider.pl/rozwoj/izolacja-spoleczna-definicja-i-sposoby-jej-przezwyciezania [dostęp: 10.04.2023

https://www.veracode.com/security/spyware#:~:text=Spyware%20is%20any%20software%20that,this%20data%20to%20other%20parties [dostęp: 12.04.2023].