Beata Zajęcka
Uniwersytet Jana Długosza w Częstochowie
ORCID: 0000-0002-7765-4067

Marek Kopiec
Uniwersytet Jana Długosza w Częstochowie
ORCID: 0009-0001-0172-0136

DOI: 10.24917/20838972.21.11

Aspekty etyczne niebezpieczeństw w cyberprzestrzeni

Wprowadzenie

Czym tak naprawdę jest Internet? To nasz przyjaciel czy może wróg? To my go tworzymy czy on kreuje nas i przejmuje nad nami władzę? Wielu z nas niejednokrotnie zadaje sobie takie pytania dopiero wtedy, gdy staje w obliczu tego potężnego medium, rządzącego się swoimi prawami i tętniącego własnym wirtualnym życiem.

Stale rosnąca popularność, wszechstronność, nowoczesność i multimedialność to tylko jedne z licznych przymiotów cechujących internetowy cyberświat. Z dnia na dzień, z minuty na minutę medium to przeobraża się, rozprzestrzenia, obejmuje coraz to głębsze pokłady ludzkiej egzystencji, wkracza również w etyczne aspekty zachowań człowieka. Przez krótkie lata swojego istnienia Internet zdążył już utworzyć swego rodzaju interaktywną relację, bowiem „rozwija możliwości człowieka i jest produktem tego rozwoju”[1]. Sieć internetowa daje możliwość podłączenia się w zasadzie z dowolnego miejsca na Ziemi w dowolnym czasie. Ważne jest też, iż komunikacja ta może mieć charakter multimedialny – może odbywać się za pomocą obrazu, dźwięku i tekstu. Ponadto Internet nie ma wyznaczonych

1 B. Aouil, *Komunikowanie się w Internecie – narzędzia, specyfika i własności*, [w:] *Komunikacja społeczna w świecie wirtualnym*, red. M. Wawrzak-Chodaczek, Wydawnictwo Adam Marszałek, Toruń 2008, s. 11.

godzin otwarcia, działa 24 godziny na dobę. Bez przerwy możliwy jest dostęp do informacji zgromadzonych na stronach internetowych, forach dyskusyjnych, czatach, cały czas możemy korzystać z komunikatorów czy poczty elektronicznej itd.[2] W dzisiejszych czasach trudno się bez Internetu obejść. Jego brak w niektórych dziedzinach życia staje się nieraz barierą, przez którą trudno osiągnąć założony cel. Brak dostępu do Internetu może prowadzić do wykluczenia cyfrowego, bo to właśnie dostęp, umiejętność i sposób korzystania twórczego czy odtwórczego ma wpływ na zwiększenie lub zmniejszenie szans życiowych użytkownika[3]. Sieć internetowa łączy ze sobą różne cechy, m.in. radia, telewizji, prasy, dlatego też wygodniejszym jest dla współczesnego człowieka korzystanie ze środka przekazu zawierającego w jednym miejscu to wszystko, co jest potrzebne, a przede wszystkim wszystko to jest dostępne w telefonie, komputerze czy tablecie.

Internet wyróżnia się spośród tradycyjnych mediów, choć tak samo jak one jest nośnikiem informacji, wiedzy, środkiem przekazu, gromadzenia danych i informacji. Rzeczywistość wirtualna niewątpliwie stała się medium o charakterze ponadnarodowym, a nawet ponadkontynentalnym. Internet jest obecnie nie tylko narzędziem pracy czy rozrywki. Stał się też naturalnym tłem życia codziennego[4]. Miejsce, czas czy forma w cyberprzestrzeni nie istnieją – świat rzeczywistości wirtualnej daje nieograniczone możliwości swoim użytkownikom, tak jak i rzeczywistość prawdziwa[5]. Czy istnieje zatem jeszcze granica dzieląca te dwa światy: rzeczywistości realnej i rzeczywistości wirtualnej? Jakie etyczne wyzwania towarzyszą użytkownikom Internetu? Czy jesteśmy bezpieczni w cyberprzestrzeni?

„Cyberpojęcia" – wyjaśnienie wybranych definicji

Istotnym elementem wpływającym na bezpieczeństwo podczas korzystania z zasobów i możliwości sieci Internet oraz właściwego korzystania z narzędzi, które oferuje nam współczesny świat, jest realne podnoszenie świadomości. Świadomości rozumianej jako umiejętność korzystania ze współczesnych zasobów technologicznych, a także ich bezpiecznego używania. Może odnosić się to do różnych aspektów: wiedzy o tym, jak korzystać z takich urządzeń, jak komputer, smartfon, tablet oraz innych urządzeń i aplikacji

2 C. Guerreschi, *Nowe uzależnienia*, Wydawnictwo Salwator, Kraków 2006.

3 B. Zajęcka, *Internet – przyjaciel czy wróg współczesnej młodzieży?*, „Prace Naukowe Akademii im. Jana Długosza w Częstochowie. Seria Pedagogika", t. XXI, s. 209–220.

4 J.A. Bargh, K.Y.A. McKenna, *Internet a życie społeczne*, [w:] *Internet a psychologia: możliwości i zagrożenia*, red. W.J. Paluchowski, Difin, Warszawa 2009, s. 25–45.

5 M. Szpunar, *Społeczności wirtualne jako nowy typ społeczności – eksplikacja socjologiczna*, „Studia Socjologiczne" 2004, nr 173(2), s. 95–130.

służących do komunikacji czy robienia zakupów, jak również do zagrożeń związanych z używaniem Internetu i innych technologii. Jak twierdził jeden z najsłynniejszych hackerów Kevin Mitnick „System bezpieczeństwa jest tak silny jak jego najsłabsze ogniwo – człowiek”[6]. Wciąż rozwijające się nowe technologie pociągają za sobą ryzyko popełnienia błędu, którego skutki mogą być dotkliwe w świecie nie tylko wirtualnym, ale także realnym.

Użytkownik Internetu powinien mieć umiejętność korzystania z narzędzi technologicznych w sposób bezpieczny i odpowiedzialny. Obejmuje to zrozumienie, jak chronić prywatność i swoje dane osobowe, jak unikać zagrożeń cybernetycznych, jak korzystać z mediów społecznościowych i innych platform online w sposób etyczny. Taka świadomość jest szczególnie ważna w dzisiejszych czasach, kiedy technologia jest coraz bardziej powszechna i wpływa na wiele aspektów naszego życia. Właściwa profilaktyka w tym zakresie może pomóc ludziom uniknąć błędów, czyli pułapek i zagrożeń związanych z technologią, a jednocześnie wskaże, jak wykorzystać jej zalety w sposób efektywny. To od użytkowników Internetu i poziomu ich świadomości zależy bezpieczeństwo korzystania ze współczesnych technologii. Każdy użytkownik bez względu na wiek, płeć czy wykształcenie może stać się osobą poszkodowaną, a nawet nieumyślnym sprawcą niewłaściwego działania w sieci.

Bardzo szybki rozwój Internetu sprawił, że świat wkroczył w nową erę, a przed użytkownikami sieci otworzyły się zupełnie nowe możliwości. Niestety, rozwój nowoczesnych technologii ma też swoją ciemną stronę, czego przejawem jest bardzo dynamiczny rozwój przestępczości w nowej wirtualnej rzeczywistości. Czym jest **cyberprzestępczość**? Ogólnie uważa się, że cyberprzestępczość jest jednym z cyberzagrożeń, które obejmują „nieuprawnione zachowania skierowane na uzyskanie dostępu, pozyskanie, manipulowanie lub utratę integralności, poufności i dostępności danych, aplikacji czy systemu komputerowe”[7]. Chociaż wyraz „cyberprzestępczość” nie należy w obowiązującym stanie prawnym do katalogu polskich wyrażeń ustawowych, niewątpliwie odnosi się do jednego z największych zjawisk przestępczych dzisiejszych czasów[8]. Pod pojęciem cyberprzestępczości rozumie się czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takim sieciom i systemom. W ten sposób pojęcie to zostało zdefiniowane przez

6 K. Mitinck, *Człowiek to najsłabsze ogniwo*, https://itwiz.pl/jak-skutecznie-zabezpieczyc-najslabsze-ogniwo-bezpieczenstwie/ (dostęp: 16.05.2023).

7 J. Kosiński, *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015, s. 14.

8 M. Siwicki, *Cyberprzestępczość*, Warszawa 2013.

Komisję Wspólnot Europejskich. Definicja cyberprzestępstwa została w Polsce określona w Rządowym Programie Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016 oraz powtórzona w Polityce Ochrony Rzeczypospolitej Polskiej z 2013 roku. Cyberprzestępstwo zostało w nich określone jako „czyn zabroniony popełniany w obszarze cyberprzestrzeni"[9] (na marginesie wskazać należy, że w obecnie obowiązującej Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 nie pojawia się definicja cyberprzestępstwa)[10].

Od samego początku Internet służył także do celów przestępczych. Skoro zaistniało zjawisko określane mianem cyberprzestępczości, to trzeba się przed nim chronić. Stąd też bardzo istotnym elementem współczesnego świata jest **cyberbezpieczeństwo** mieszczące się w ramach bezpieczeństwa informacji. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 utożsamia pojęcie cyberbezpieczeństwa z bezpieczeństwem sieci i systemów informatycznych oraz bezpieczeństwem teleinformatycznym. Traktuje je jako synonimy oznaczające „odporność systemów teleinformatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informacyjne"[11]. Niestety żaden system, żadne oprogramowanie nie będzie nigdy wystarczająco skuteczne bez ingerencji człowieka. Prostym tego przykładem jest pozostawienie alarmu w domu bez aktywacji – to my sami musimy ten alarm uruchomić, aby był on skuteczny. Sytuacja ta znajduje swoje odzwierciedlenie w zakresie cyberbezpieczeństwa. Komputer, chociaż ma zainstalowany system zabezpieczeń, nie chroni przed zagrożeniami a jedynie może wspierać użytkownika przed nimi. Pomimo automatycznej aktualizacji bazy wirusów konieczne jest systematyczne, „ręczne" jej aktualizowanie. Odnosi się to także do pozostałego oprogramowania zainstalowanego na danym urządzeniu.

Bezpośrednim naruszeniem bezpieczeństwa jest atak – w sieci nosi on nazwę **cyberatak** i jest „rozumiany jako każdy rodzaj ofensywnego działania w Internecie osób lub organizacji, którego celem mogą być systemy

9 *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016*, pkt 1.1. Definicje, Warszawa 2010, s. 6.

10 Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*, https://www.dziennikustaw.gov.pl/M2019000103701.pdf (dostęp: 29.09.2023).

11 C. Banasiński, *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, [w:] *Cyberbezpieczeństwo – zarys wykładu*, red. C. Banasiński i in., Wolters Kluwer, Warszawa 2018, s. 31.

informatyczne, sieci komputerowe, komputery lub inne urządzenia osobiste"[12]. Cyberatak ma na celu zniszczenie danych, zmodyfikowanie ich lub uzyskanie nieuprawnionego dostępu do nich. Może on przybierać różne formy, takie jak podsyłanie wirusów i trojanów, phishing czy DDoS (Distributed Denial of Service). Cyberataki stanowią poważne zagrożenie dla firm, organizacji i prywatnych użytkowników, ponieważ mogą prowadzić do kradzieży poufnych informacji, zniszczenia lub modyfikacji danych oraz zakłóceń systemów informatycznych. Są one często przeprowadzane przez hakerów, cyberprzestępców. Aby chronić się przed cyberatakami, należy stosować odpowiednie środki bezpieczeństwa, takie jak oprogramowanie antywirusowe i zapora sieciowa, silne hasła. Nie powinno się również klikać w podejrzane linki. W przypadku wykrycia ataku należy szybko działać i podjąć odpowiednie kroki, takie jak odłączenie systemu od sieci, zmiana haseł i zawiadomienie odpowiednich służb lub ekspertów ds. bezpieczeństwa. W obliczu ciągle rosnącego zagrożenia cyberatakiem ważne jest, aby zarówno firmy, jak i prywatni użytkownicy byli świadomi ryzyka i podejmowali odpowiednie środki ostrożności. Pracownicy zatrudnieni w firmach powinni uczestniczyć w szkoleniach z zakresu cyberbezpieczeństwa w celu zdobycia umiejętności rozpoznawania podejrzanych e-maili, wiadomości i stron internetowych oraz zdobycia wiedzy, jak postępować w przypadku wykrycia anomalii lub zaistniałego incydentu.

Charakterystyka najczęściej występujących zagrożeń w cyberświecie

W związku z intensywnym rozwojem Internetu i nowych technologii zagrożenie w cyberprzestrzeni znacznie wzrosło. Skutki często odczuwalne są w świecie zarówno wirtualnym, jak i rzeczywistym, a ich przyczyną jest nikła świadomość zagrożeń lub jej całkowity brak. Raport *Threat Landscape 2022* przygotowany przez Agencję UE ds. Cyberbezpieczeństwa (ENISA), wskazuje na osiem głównych grup zagrożeń. Są to zagrożenia ransomware, malware, związane z socjotechniką, związane z danymi, dla dostępności – ataki typu „odmowa usługi", związane z dostępnością Internetu, dezinformacją oraz z łańcuchem dostaw[13].

12 *Cyberatak* [hasło], https://sjp.pwn.pl/sjp/cyberatak;5606168.html (dostęp: 16.05.2023).

13 *Raport Threat Landscape 2022*, https://www.europarl.europa.eu/news/pl/headlines/society/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia (dostęp: 29.09.2023).

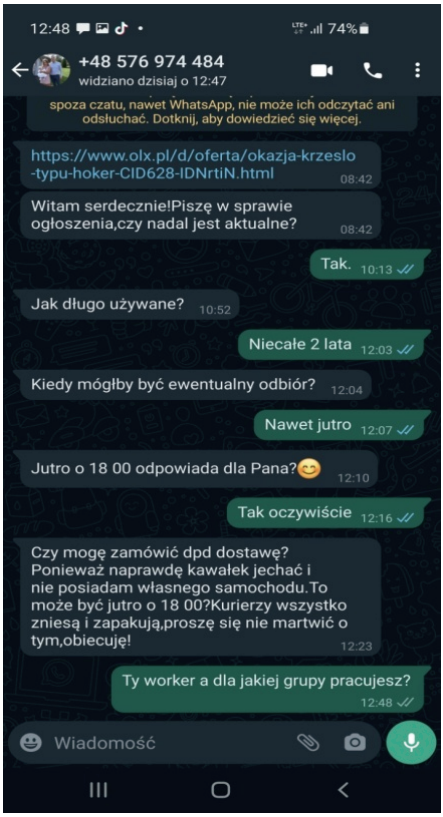
✓ Ransomware

Ataki typu ransomware (ang. ransom – 'okup') w 2022 roku zajmowały czołowe miejsce wśród wszystkich cyberzagrożeń. Stają się one coraz bardziej złożone, niejednokrotnie cyberprzestępcy korzystają w nich z innych technik pośredniczących, np. socjotechnik. Jest to rodzaj oprogramowania (w tym przypadku wirusa) używanego w przestępczości internetowej. Wirus przenika do wnętrza atakowanego komputera i szyfruje dysk należący do użytkownika. Następnie wirus umieszcza w komputerze notatkę, często wyświetlaną samoistnie na ekranie. Notatka ta zawiera instrukcję dotyczącą tego, co musi zrobić właściciel plików w celu ich odzyskania (odszyfrowania). Zwykle sprawca domaga się przelania pieniędzy na konto portfela kryptowalut, a w zamian obiecuje wysłanie klucza oraz instrukcji, jak odszyfrować dane[14]. Dodatkowo szantaż ten bywa poparty groźbą upublicznienia wykradzionych wcześniej wrażliwych danych.



Rys. 1. Komunikat złośliwego oprogramowaniem typu ransomware – WannaCry
Źródło: K. Frankowicz, *WannaCry Randsomware*, https://cert.pl/posts/2017/05/wannacry-ransomware/ (dostęp: 16.05.2023).

14 T. Pączkowski, *Słownik cyberbezpieczeństwa*, Szkoła Policji w Katowicach, Katowice 2017.



Rys. 2. Zrzut ekranu przedstawiający korespondencję ze sprawcą usiłowania oszustwa

Źródło: opracowanie własne – link nadesłany za pośrednictwem komunikatora WhatsApp.

Jak wynika z danych cytowanych przez ENISĘ, średnia wartość okupu zapłaconego w atakach ransomware podwoiła się z 71 000 euro w 2019 roku do 150 000 euro w 2020 roku. Natomiast w 2021 roku osiągnęła wartość 18 miliardów euro, czyli 57 razy więcej niż w 2015 roku[15].

Nie bez znaczenia pozostają również innego rodzaju ataki, czy też przestępstwa mające na celu wyłudzenie pieniędzy. Mogą one prowadzić do utraty środków pieniężnych na skutek klasycznego oszustwa, np. podczas robienia zakupów w sieci internetowej, czy też do innych szkód z wykorzystaniem socjotechnik. Utrata gotówki następuje zazwyczaj na skutek braku świadomości w zakresie:

15 *Raport Threat Landscape…*

- właściwego zabezpieczenia sprzętowo-programistycznego (np. ustawienie pinów, haseł, aktualizacje programów i aplikacji, stosowanie programów antywirusowych itp.),
- właściwego odczytywania adresów URL (stron WWW), adresów e-mail (zwłaszcza tych niewidocznych),
- logowania do bankowości elektronicznej za pomocą nadesłanych linków np. za pośrednictwem aplikacji WhatsApp czy poprzez SMS,
- inwestowania w kryptowaluty (w efekcie reklam wykorzystujących wizerunki znanych osób, tj. polityków, celebrytów czy sportowców – tzw. SCAM).

✓ Malware – złośliwe oprogramowanie

Określenie „malware" powstało z połączenia dwóch angielskich słów *malicious* oraz *software* i oznacza 'złośliwe oprogramowanie', czyli takie oprogramowanie, którego celem jest uszkodzenie programu, urządzenia komputerowego, serwera lub sieci komputerowej lub wywołanie innych skutków niż zamierzone przez posiadacza danych. Istnieje wiele różnych rodzajów malware, a każdy z nich może mieć inne możliwości. Oprogramowanie to może m.in. uzyskiwać zdalny dostęp do systemu informatycznego, zapisywać i wysyłać dane z tego systemu osobom trzecim bez wiedzy i zgody użytkownika, wyłączać środki bezpieczeństwa lub w inny sposób wpływać na integralność danych i systemu. Do malware zalicza się wirusy, robaki, konie trojańskie, backdoory, rootkity, keyloggery czy spyware[16]. Parlament Europejski wskazuje, iż w 2020 roku i na początku 2021 roku liczba incydentów związanych ze złośliwym oprogramowaniem globalnie spadła z powodu pandemii COVID-19, jednak wyraźnie wzrosła pod koniec 2021 roku, głównie z powodu powrotu ludzi do biur[17].

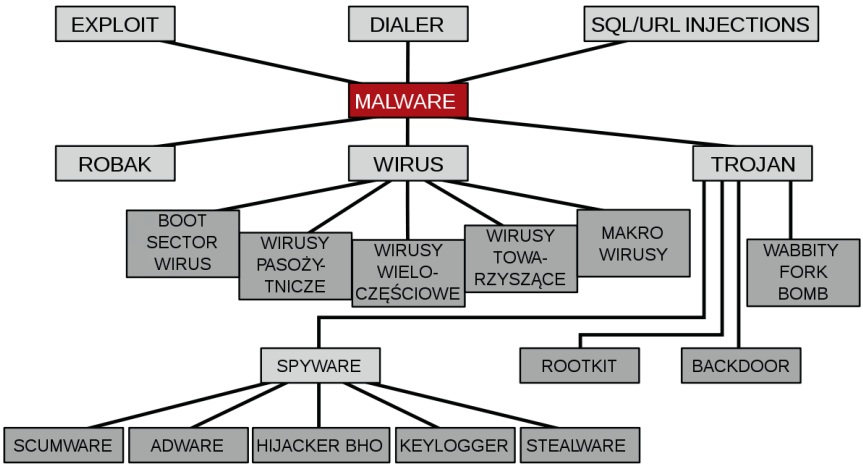
„Wzrost liczby incydentów związanych ze złośliwym oprogramowaniem przypisuje się również tzw. cryptojackingowi (potajemnemu wykorzystywaniu komputera ofiary do nielegalnego wydobywania kryptowalut) oraz złośliwemu oprogramowaniu atakującemu tzw. internet rzeczy, czyli urządzenia podłączone do Internetu, takie jak routery lub kamery" [18]. Według ENISY, w pierwszym półroczu 2022 roku było więcej ataków na urządzenia podłączone do Internetu niż w poprzednich czterech latach[19].

16 J. Kosiński, *Paradygmaty cyberprzestępczości*...

17 *Cyberbezpieczeństwo: główne i nowe zagrożenia*, https://www.europarl.europa.eu/news/pl/headlines/society/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia (dostęp: 17.05.2023).

18 Tamże.

19 *Raport Threat Landscape 2022*..., s. 50.



Rys. 3. Rodzaje złośliwego oprogramowania

Źródło: https://pl.wikipedia.org/wiki/Z%C5%820%C5%9Bliwe_oprogramowanie (dostęp: 16.05.2023).

✓ Atak z wykorzystaniem socjotechnik

Inżynieria społeczna (socjotechnika) od wielu lat była przedmiotem badań nauk społecznych. Rozumiana była ona jako umiejętność skutecznego oddziaływania na innych, a także jako „ogół metod i działań indywidualnych lub grupowych, których celem jest uzyskanie pożądanego zachowania jednostek lub grup społecznych”[20]. Tak ugruntowane stanowisko teoretyczne podlegało licznym zmianom, niemniej przetrwało i utrwaliło się w polskiej myśli socjologicznej. Od niedawna jednak inżynieria społeczna stała się przedmiotem nauki o bezpieczeństwie oraz informatyki. W informatyce socjotechniką określa się sztukę manipulacji ludźmi w celu nakłonienia ich do podjęcia określonych działań lub ujawnienia poufnych informacji. Niewątpliwie duża część ataków skierowanych na uzyskanie środków pieniężnych następuje z wykorzystaniem socjotechnik. Przykładem mogą być oszustwa, oszustwa internetowe oraz kradzieże środków pieniężnych znajdujących się na rachunkach bankowych[21]. Europol wskazuje, iż zarówno przedstawiciele organów ścigania, jak i sektora prywatnego uznają

20 A. Podgórecki, *Socjotechnika: praktyczne zastosowania socjologii*, Wydawnictwo Książka i Wiedza, Warszawa 1968, s. 33.

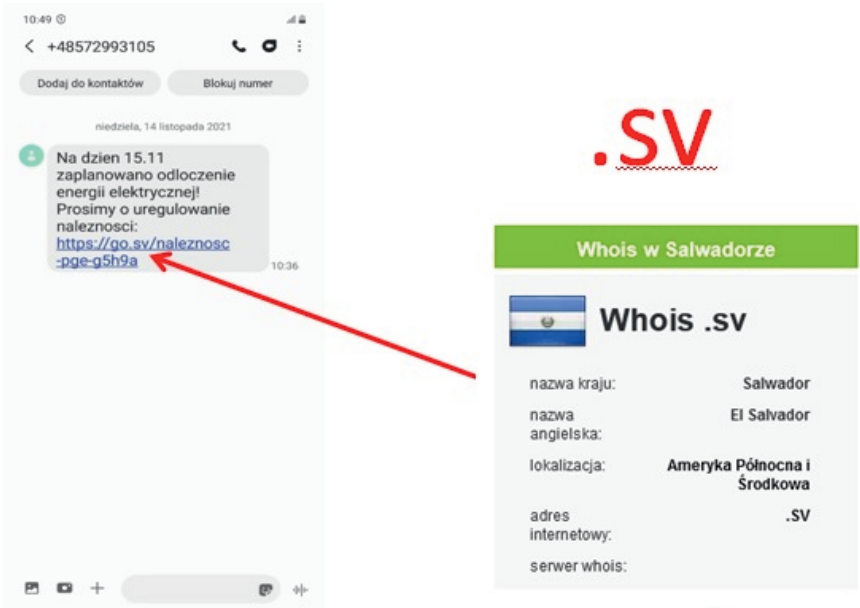
21 A. Gryszczyńska, *Wykorzystanie COVID-19 w scenariuszach ataków opartych na socjotechnice*, „Rocznik Bezpieczeństwa Morskiego – Przestępczość Teleinformatyczna 2020” 2021, s. 141–145.

wykorzystanie inżynierii społecznej za podstawowe zagrożenia i czynnik ułatwiający popełnienie przestępstw internetowych. Znaczne różnice występują w poziomie zaawansowania ataków i atakujących. Niestety z uwagi na nieodpowiednie środki bezpieczeństwa lub niewystarczającą wiedzę i umiejętności nawet słabo przeprowadzone ataki bardzo często kończą się sukcesem cyberprzestępców. Jednocześnie następuje wzrost ilościowy i jakościowy tych ataków, a ich sprawcy stosują strategie łączące socjotechnikę z wykorzystywaniem narzędzi, systemów i luk w zabezpieczeniach oraz fałszywych tożsamości i współpracy z innymi cyberprzestępcami[22].

Czy prywatność w Internecie to tylko mit? Każdy z nas ma na pewno choć jedno konto w sieci. Może to być konto na portalu społecznościowym, w sklepie internetowym czy też służące do obsługi bankowości elektronicznej. Jako użytkownicy zakładamy różne blokady i hasła, czujemy się pewni, że skoro zabezpieczyliśmy nasze konta, to nic nam nie grozi. Niestety to błąd. Hakerzy, czyli osoby włamujące się do sieci i systemów komputerowych, nie pozwalają nam spokojnie funkcjonować w sieci i burzą naszą prywatność. Bardzo poważnym zagrożeniem naszej prywatności i bezpieczeństwa jest **phishing**, który należy do najczęstszych ataków socjotechnicznych. Jest to atak wykorzystujący inżynierię społeczną w celu wyłudzenia poufnych informacji i zasobów, które następnie są szyfrowane. Cyberprzestępcy za pomocą phishingu mogą wyłudzić nasze dane osobowe, numery kont bankowych, kart kredytowych i inne poufne informacje. Jak wynika ze wspomnianego powyżej raportu CERT, w 2020 roku wzrosła liczba ataków phishingowych wykorzystujących motyw fałszywych bramek płatności. Najczęściej były to wiadomości SMS z panelem informującym o potrzebie dopłaty oraz linkiem do fałszywej bramki płatności wykorzystującej wizerunek firmy eCard. Cyberprzestępcy wykorzystują skracanie nazw domen internetowych dotyczących np. dopłaty do przesyłki firmy kurierskiej, opłat za energię elektryczną czy gaz. W kwietniu 2020 roku fałszywy panel eCard, który do tej pory wyłudzał tylko dane do kont bankowych, został poszerzony o możliwość płatności blikiem. Takie zachowanie z pewnością było spowodowane wzrostem popularności tej metody płatniczej[23].

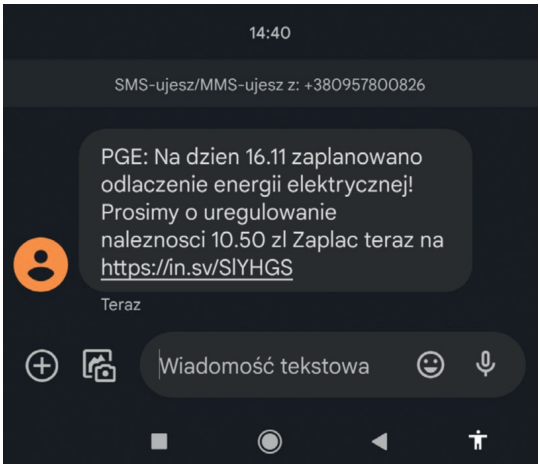
22 *Internet Organised Crime Threat Assessment (IOCTA)*, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020 (dostęp: 18.05.2023).

23 *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działań CERT Polska 2021*, Państwowy Instytut Badawczy NASK, Warszawa 2022, s. 55.



Rys. 4. Phishingowa wiadomość SMS zawierająca link w domenie .sv
Źródło: opracowanie własne – link nadesłany za pośrednictwem SMS.

Inna wersja tego ataku, sugerująca uregulowanie należności prąd pod groźbą odłączenia energii elektrycznej.



Rys. 5. Wiadomość SMS sugerująca konieczność dopłaty za prąd
Źródło: *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działań CERT Polska 2021*, Państwowy Instytut Badawczy NASK, Warszawa 2022, s. 55.

Innym rodzajem ataków jest przejmowanie kont na Facebooku. Najczęstszym celem tego ataku są grupy otwarte mające dużą liczbę członków, zazwyczaj lokalne (miejskie, gminne) lub handlowe, typu „sprzedam/wymienię/oddam". W 2019 roku jako phishing sklasyfikowano 3516 incydentów[24], natomiast w 2021 roku odnotowano ich prawie pięć razy więcej, tj. 18 852[25].

Wśród ataków z użyciem socjotechnik można również wyróżnić takie, które są ukierunkowane na konkretne osoby (*spearphishing*), na osoby decyzyjne, kierowników jednostek organizacyjnych (*whaling*) oraz takie, w których do wyłudzenia danych dochodzi podczas rozmowy telefonicznej (*vishing*) lub za pośrednictwem wiadomości SMS (*smishing*). Istnieje jeszcze więcej ataków opartych na tej technice. Należą do nich *Business Email Compromise* (*BEC*), *SIM swapping*, a także oszustwa nigeryjskie. Występują również takie ataki, które wymagają większej wiedzy, umiejętności i zaangażowania sprawców, np. *spoofing* i *pharming*[26]. Przestępcy coraz częściej atakują też giełdy kryptowalut i właścicieli portfeli cyfrowych.

✓ Zagrożenia bezpieczeństwa danych

Kolejna grupa zagrożeń dotyczy **bezpieczeństwa danych**. Zagrożenia te związane są z atakowaniem źródeł danych dla uzyskania nieautoryzowanego dostępu lub ujawnienia ich. Wyróżnia się dwie główne grupy ataków. Do pierwszej należą naruszenia bezpieczeństwa danych, gdzie na ogół są to zamierzone ataki cyberprzestępców. Drugą grupę stanowią tzw. wycieki danych, które na ogół nie są zamierzone, powstają na skutek stosowania niewłaściwej polityki bezpieczeństwa i związanych z nią procedur bezpieczeństwa. Oczywiście pieniądze są głównym motorem działań sprawców. Szpiegostwo stanowi zaledwie 10% wszystkich ataków[27].

✓ Zagrożenia dostępności danych

Inną grupą niepożądanych działań są te związane z **zagrożeniami dla dostępności**. Są to ataki typu „odmowa dostępności", które uniemożliwiają użytkownikom dostęp do danych lub usług. Ataki typu DoS (z ang. *Denial of Service* – Odmowa Dostępu) są jednymi z najbardziej krytycznych zagrożeń dla systemów informatycznych. Ich zakres i złożoność są coraz większe. Jedną z powszechnych form ataku jest przeciążenie infrastruktury sieciowej i uniemożliwienie dostępu do systemu. Wszystkie statystyki zespołów CERT na całym świecie pokazują ciągły wzrost ataków DoS. A wszystko przez to,

24 Tamże, s. 9.

25 Tamże, s. 91.

26 A. Gryszczyńska, *Wykorzystanie COVID-19…*

27 *Cyberbezpieczeństwo: główne i nowe zagrożenia…*

że stały się bardzo tanie. Ataki typu „odmowa usługi" coraz częściej uderzają w sieci komórkowe i podłączone urządzenia, czyli atakują „internet rzeczy". Są także często używane w cyberwojnie rosyjsko-ukraińskiej[28].

✓ Zagrożenia dla dostępności

Istotnym zagrożeniem jest również brak dostępu do Internetu. „Takie zagrożenia obejmują fizyczne przejmowanie i niszczenie infrastruktury internetowej, co zaobserwowano na okupowanych terytoriach ukraińskich od czasu rosyjskiej inwazji, a także aktywne cenzurowanie serwisów informacyjnych lub mediów społecznościowych"[29].

✓ Dezinformacja

Pomyślmy, jeżeli każdy użytkownik Internetu może udostępniać informacje, to czy zawsze będą one prawdziwe? Należy pamiętać, że niestety nie. Dla osób świadomie korzystających z Internetu jego interakcyjność to prawdziwa skarbnica wiedzy umożliwiająca rozwój osobisty. Jednak osoby poruszające się w wirtualnym świecie w poszukiwaniu aktualnych informacji nie zawsze potrafią rozróżnić fakty od nieprawdziwych danych. Niepożądanym zjawiskiem dla współczesnego świata jest **dezinformacja**, czyli informacja wprowadzająca w błąd. „Rosnące wykorzystanie mediów społecznościowych i mediów internetowych doprowadziło do nasilenia kampanii rozpowszechniających dezinformację (celowo sfałszowane informacje) i informacje wprowadzające w błąd (udostępnianie błędnych informacji)"[30]. Celem tych kampanii jest rozpowszechnianie informacji rodzących nienawiść do innych nacji czy religii, bądź też budzenie strachu i niepewności. Warto także wspomnieć o nowej i wciąć rozwijającej się technologii *deepfake*. Daje ona możliwość tworzenia fałszywych nagrań audio, wideo lub zdjęć, które są prawie nie do odróżnienia od tych prawdziwych. Jak mało teraz trzeba, żeby za pomocą dostępnych aplikacji zniszczyć komuś życie. Narażone na niebezpieczeństwo są zwłaszcza dzieci i młodzież.

✓ Rozwój i dynamika zagrożeń

Współcześnie kategorii i rodzajów nowych zagrożeń związanych ze światem wirtualnym jest bardzo wiele i wraz z rozwojem technologicznym wciąż pojawiają się nowe. Wśród nich warto wymienić te związane z kradzieżą tożsamości, na co najczęściej narażone są osoby tworzące loginy i hasła

28 *Rodzaje ataków*, https://dataspace.pl/blog/dos-rodzaje-atakow-cz-1/ (dostęp: 19.05.2023).

29 *Cyberbezpieczeństwo: główne i nowe zagrożenia*...

30 Tamże.

z prostych ciągów znaków, np. używając imion swoich dzieci, dat urodzin, nazw instytucji czy firm wraz z dodanymi znakami „1" lub „@1"[31].

Innym zagrożeniem są cyberprzestępstwa popełniane zarówno na skutek celowych działań, jak i te dokonywanych z uwagi na brak wystarczającej świadomości, wiedzy, znajomości obowiązujących przepisów, w tym także błędne przeświadczenie o niekaralności czynu. Mogą one przybierać wiele form, w zależności od charakteru tych działań i ich konsekwencji. Przykłady takich działań to: cyberprzemoc, hakerstwo, oszustwa komputerowe, rozpowszechnianie nielegalnych treści. Natomiast do czynów często popełnianych z uwagi na wskazane powyżej braki czy też „błędy", można zaliczyć przestępstwa z zakresu ochrony praw autorskich, kopiowanie czy udostępnianie filmów, muzyki (np. za pośrednictwem protokołu p2p) oraz sprzedaży towarów objętych regulacjami ustaw szczególnych (np. zwierząt i roślin objętych konwencją CITES).

Media elektroniczne tworzą z jednej strony przestrzeń wolności dla jednostki, z drugiej zaś strony ta wolność jest często niewłaściwie rozumiana. Współcześnie szczególnie niebezpiecznym zjawiskiem jest seksting, czyli forma komunikacji elektronicznej, w której przekazem jest seksualnie sugestywny obraz lub treść. Termin powstał na początku XXI wieku jako zrost angielskich słów: *sex* i *texting*. Zjawisko to nie ogranicza się jedynie do dzieci i młodzieży, jednak dla tej grupy wiekowej stanowi najpoważniejsze zagrożenie, przede wszystkim z uwagi na jego konsekwencje. Istnieje również niebezpieczeństwo, iż materiały przesyłane w prywatnych wiadomościach mogą zostać upublicznione[32]. Jak wynika z badań ogólnopolskich prowadzonych na reprezentatywnej grupie badawczej, zjawisko sekstingu jest akceptowalne wśród młodych użytkowników Internetu. Co piąty z nich (18,6%) nie widzi nic złego w takim zachowaniu. Ponadto rodzice większości badanych nie kontrolują, czy ich dzieci oglądają treści pornograficzne w Internecie. Taką odpowiedź wskazało w ankiecie 59,9% nastolatków. Z większością z nich (58,5%) rodzice nigdy nie przeprowadzili żadnej rozmowy na temat oglądania pornografii w Internecie i ewentualnych konsekwencji kontaktu z takimi materiałami[33]. Młodzi ludzie poddają się powszechnemu trendowi seksualizacji wszystkich sfer życia. Wydaje im się, że jeżeli chcą być postrzegani jako atrakcyjni, muszą pokazać coś więcej niż inni. Wpływa to negatywnie na ich samoocenę oraz zaburza budowanie trwałych,

31 J. Kosiński, *Paradygmaty cyberprzestępczości*...

32 Ł. Wojtasik, *Seksting*, [w:] *Bezpieczeństwo dzieci online. Kompendium dla rodziców, nauczycieli i profesjonalistów*, red. A. Wrzesień-Gandolfo, Warszawa 2014.

33 R. Lange i in., *Nastolatki wobec pornografii cyfrowej. Trajektorie użytkowania. Raport z badań ogólnopolskich*, Państwowy Instytut Badawczy NASK, Warszawa 2022, s. 30–33.

wartościowych relacji. Młodzież często nie ma świadomości, jakie ryzyko podejmuje i jakie mogą być konsekwencje wysyłania przez Internet swoich nagich zdjęć. Podczas gdy seksting może być dla dorosłych sposobem na odkrywanie swojej seksualności i intymności, może również wiązać się z potencjalnym ryzykiem, zwłaszcza, jeśli treści są udostępniane bez zgody wszystkich zaangażowanych stron. Powinniśmy być świadomi, że w Internecie nic nie ginie.

✓ Etyczne aspekty w cyberprzestrzeni

Jak podkreślano powyżej, nieodłącznym elementem codzienności współczesnego człowieka są liczne interakcje online. Komunikacja z innymi członkami społeczeństwa, również w aspekcie międzynarodowym, dostęp do najbardziej aktualnych informacji z różnych zakątków świata to dobra, z którymi mamy na co dzień do czynienia, ale ich istnienie i nadmierne lub niewłaściwe wykorzystywanie mogą prowadzić do etycznych dylematów. Dyskusja o problemach etycznych związanych ze stosowaniem nowych technologii toczy się od lat.

Najpierw jednak należy poznać znaczenie słowa „netykieta". Powstało ono z dwóch angielskich słów: *net* ('sieć') oraz *etiquette* ('etykieta'), które po połączeniu oznaczają „etykietę sieciową". Netykieta na ogół definiowana jest jako zbiór reguł właściwego i zgodnego z ogólnie przyjętymi zasadami etyki i prawa postępowania internautów w cyberprzestrzeni[34]. Zagadnienia etyczne, na które wskazują praktycy, to wolność, gdy jest oddzielona od odpowiedzialności, natychmiastowość reakcji, która często jest emocjonalną reakcją oderwaną od rozumu i woli, anonimowość użytkowników czy ignorancja części internautów[35].

Głównym założeniem netykiety jest okazywanie szacunku innym użytkownikom Internetu stanowiącym jedną społeczność, w myśl zasady „traktuj innych tak, jak sam chciałbyś być traktowany". Powyższą zasadę powinniśmy stosować w praktyce zarówno „w życiu" offline, jak i online. Istnieje jeszcze kilka innych prostych reguł, o których warto pamiętać. Jedną z nich jest poprawność pisowni polegająca na przestrzeganiu zasad ortografii i interpunkcji oraz niestosowaniu wulgaryzmów. Kolejną bardzo ważną regułą jest przestrzeganie regulaminu danego portalu, forum czy czatu. Większość regulaminów wskazuje działania niepożądane, za popełnienie których użytkownik może ponieść rozmaite konsekwencje. Dbając o właściwe zachowanie się w Internecie, nie należy pisać wiadomości wielkimi literami,

34 J. Kulesza, *Ius Internet. Między prawem a etyką*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2010, s. 24.

35 Ks. A. Domaszk, *Konferencja naukowa „Etyczne i prawne wyzwania Internetu"*, „Prawo Kanoniczne: Kwartalnik Prawno-Historyczny" 2010, nr 53/3–4, s. 373–376.

gdyż taka forma oznacza krzyk. Inne równie istotne zasady netykiety to m.in. nieprowokowanie pozostałych użytkowników do niepotrzebnych i nieuzasadnionych kłótni, zwane trollingiem, niespamowanie, czyli nierozsyłanie niechcianych wiadomości, reagowanie na krzywdzenie innych w Internecie (na zjawisko zwane hejtem), szanowanie cudzej własności intelektualnej, uważanie na *fake newsy* oraz dbanie o własny wizerunek[36].

Niezależnie od powyższego, podkreśla się również osamotnienie oraz cyberuzależnienie jako problemy etyczne towarzyszące człowiekowi w wirtualnym świecie. Co ciekawe i godne odnotowania wraz ze wzrastającą liczbą kontaktów w świecie wirtualnym narastają poczucie osamotnienia i bycia niezrozumianym oraz wynikająca z tego izolacja[37].

W przedmiocie cyberuzależnienia wskazuje się już nie tylko na zagadnienie nadmiernego korzystania z gier komputerowych, ile na uzależnienia od sprawdzania wiadomości tekstowych, tablic swoich kont w mediach społecznościowych i wszechogarniającej manii robienia zdjęć. Kiedyś mówiło się o dzieciach zamkniętych w swoich pokojach i wpatrzonych w monitory, dziś mówimy już nie tylko o młodych ludziach i nie tylko o korzystaniu z cybersieci w swoim pomieszczeniu. Za sprawą rozwoju technologii (smartfony, wi-fi, łącze radiowe) w każdym niemal miejscu i o każdej porze ludzie są „zalogowani", życie w świecie wirtualnym toczy się równolegle, jak gdyby w pewnym oderwaniu od tego, co dzieje się w przestrzeni fizycznej[38].

Warto wspomnieć jeszcze o zagadnieniach dotyczących dbania o bezpieczeństwa danych i systemów informatycznych. Ataki hakerów, kradzieże tożsamości i inne cyberzagrożenia są nie tylko nielegalne, ale także naruszają etykę w cyberprzestrzeni. Rozprzestrzenianie wpisów, wiadomości, kanałów informacyjnych, w których przekazywane dane okazują się nieprawdziwe lub przeinaczone (*fake news*) jest również nieetyczne i w przyszłości będzie coraz większym zagrożeniem etycznym, z którym będzie musiało zmierzyć się społeczeństwo jako grupa, a także poszczególne jednostki[39]. Nieetyczne są bez wątpienia cyberprzemoc i przybierający na sile w ostatnich latach patostreaming (w szczególności groźny dla dzieci

36 *Netykieta, czyli* savoir-vivre *w internecie*, https://www.gov.pl/web/baza-wiedzy/netykieta-czyli-savoir-vivre-w-internecie (dostęp: 19.05.2023).

37 A. Jucewicz, *Człowiek „w sieci" jako problem etyczny*, „Nurt SVD" 2022, t. 151, nr 1, s. 36–50.

38 M. Trusewicz-Pasikowska, *Tożsamość wirtualna – droga do wyzwolenia czy zniewolenia?*, [w:] *Co nas wyzwala, co nas zniewala? Młodzi o wolności*, red. A. Kampka i in., Warszawa 2018, s. 179.

39 *Rozpoznawanie nieprawdziwych informacji*, https://www.gov.pl/web/baza-wiedzy/rozpoznawanie-nieprawdziwych-informacji (dostęp: 28.09.2023).

i młodzieży). Agresywne przekazy medialne na ogół skierowane są na zysk finansowy i dalece odbiegają od zasad etyki internetowej.

Promowanie etyki w cyberprzestrzeni wymaga edukacji i podnoszenia świadomości wśród użytkowników Internetu, aby zrozumieli, które zachowania są akceptowalne, a które nie.

Wnioski

Żyjemy w czasach rozwoju informacyjnego, a technologia stała się nieodłącznym elementem naszego życia. Jeszcze kilka lat temu dzieci uczyły się zachowań dzięki obserwacji rodziców i przysłuchiwanie się rozmowom – w ten sposób nabywały umiejętności niezbędnych do kształtowania zdrowych relacji międzyludzkich. Niepotrzebne były żadne urządzenia, ludziom wystarczało ich wzajemne towarzystwo[40]. Wskutek dynamicznego rozwoju technologicznego i zmian społeczno-kulturowych wszystko inne również zaczęło ulegać przemianom. Zauważyć należy, iż rodzący się w naszych czasach człowiek jest człowiekiem cybermedialnym – od najmłodszych lat wychowywanym przed ekranem telewizora, laptopa, z telefonem komórkowym w ręku, czyli rozwija się w towarzystwie technologii cyfrowej. Jak zmierzyć się z zagrożeniami czyhającymi pod przykrywką świata wirtualnego?

Niestety nigdy nie będziemy w stanie poznać wszystkich zasobów sieci i zniwelować związanych z tym problemów. Świat zmierza w kierunku postępu. Internet, a zwłaszcza nadmiar informacji, powodują konieczność trafnej oceny i wyboru między tym, co wartościowe, potrzebne, przydatne, etyczne, a tym, co bezużyteczne, nieprawdziwe, złe czy szkodliwe. Mimo dynamicznego rozwoju systemów zabezpieczeń informatycznych liczba przestępstw popełnianych w cyberprzestrzeni stale rośnie. Profilaktyka jest niezbędnym narzędziem do zapobiegania cyberzagrożeniom. Aby jednak dała ona zadowalający rezultat, musi być prowadzona na kilku płaszczyznach. W obliczu rosnącej liczby incydentów to właśnie czynnik ludzki odgrywa decydującą rolę. Franklin Ramón Chang, były dyrektor ds. badań w NSA, już w 2012 roku twierdził, że kwestie cyberbezpieczeństwa muszą być rozpatrywane na gruncie zarówno nauk ścisłych, jak i społecznych[41]. W obszarze cyberprzestępczości nieustannie następują dynamiczne zmiany kształtujące holistyczne podejście do niej, uwzględniające wszystkie aspekty pozwalające zrozumieć zachodzące procesy. Cyberprzestępcy coraz częściej stosują w atakach pewne formy psychologicznej manipulacji z wykorzystaniem różnorakich socjotechnik, przed którymi nie chronią użytkowników systemy

40 S. Kozak, *Patologia cyfrowego dzieciństwa i młodości*, Difin, Warszawa 2014.

41 F.R. Chang, *Guest Editor's Column*, „The Next Wave" 2012, nr 19(4), s. 1–2.

zabezpieczeń informatycznych. Jednym z największych wyzwań stojących obecnie przed cyberpsychologią jest edukowanie i zwiększanie świadomości użytkowników w zakresie psychologicznych aspektów cyberbezpieczeństwa. Istotnym jest także zrozumienie procesów odpowiedzialnych m.in. za podejmowanie decyzji czy ocenę zagrożenia[42]. Nie należy zapominać również o etycznych zagrożeniach wynikających ze świata wirtualnego, stanowiących zwłaszcza niebezpieczeństwo dla dorastających dzieci i młodzieży, ale też i dla każdego użytkownika Internetu. Haker w znaczeniu potocznym bardzo często kojarzony jest z cyberprzestępcą. Nie każdy jednak cyberprzestępca, wykorzystujący chociażby powyżej przytoczone rodzaje ataków, jest hakerem, i nie każdy haker postępuje nieetycznie. *White hat'a* to miano, którym określa się **etycznych hakerów**, czyli ekspertów bezpieczeństwa sieci i komputerów często specjalizujących się w testach penetracyjnych, zabezpieczeniu systemów informatycznych. Nawet jeśli działanie etycznych hakerów ma niekiedy nieetyczny charakter, to na pierwszym planie należy postawić cel ich działań, którym jest podnoszenie i zapewnianie cyberbezpieczeństwa. Zatem wspomniany cel, motywacja oraz skutek są odmienne od sfery intencjonalnej przestępców[43], których motorem działania jest korzyść osobista kosztem krzywdy innych ludzi.

W artykule zaprezentowano tylko zarys problematyki dotyczącej wielu płaszczyzn i aspektów współczesnego świata. Świata, w którym pierwsze skrzypce grają nowe technologie. Jednak to od nas samych zależy, jak ten świat będzie wyglądał. Dlatego też konieczne jest ciągłe podnoszenie świadomości w celu zapobiegania, likwidacji lub niwelowania skutków niewłaściwego i nieetycznego korzystania z nowych technologii.

Bibliografia

Aouil B., *Komunikowanie się w Internecie – narzędzia, specyfika i własności*, [w:] *Komunikacja społeczna w świecie wirtualnym*, red. M. Wawrzak-Chodaczek Wydawnictwo Adam Marszałek, Toruń 2008, s. 11–40.

Banasiński C., *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, [w:] *Cyberbezpieczeństwo – zarys wykładu*, red. C. Banasiński i in., Wolters Kluwer, s. 21–65.

Bargh J.A., McKenna K.Y.A, *Internet a życie społeczne*, [w:] *Internet a psychologia: możliwości i zagrożenia*, red. W.J. Paluchowski, Difin, Warszawa 2009, s. 25–45.

42 P. Zegarow, *Psychologiczne aspekty cyberbezpieczeństwa*, Państwowy Instytut Badawczy NASK, Warszawa 2019.

43 A. Haręża, *Doktryna Hakerów – mit czy rewolucja? Uwagi na temat natury informacji, entropii cyberprzestrzeni i postawy awangardy rewolucji postindustrialnej*, „CBKE e-Biuletyn" 2005, nr 1, s. 13–14, https://www.bibliotekacyfrowa.pl/Content/23674/Doktryna_Hakerow.pdf (dostęp: 9.10.2024).

Chang F.R, *Guest Editor's Column*, „The Next Wave" 2012, nr 19(4), s. 1–2.
Cyberatak [hasło], https://sjp.pwn.pl/sjp/cyberatak;5606168.html (dostęp: 16.05.2023).
Cyberbezpieczeństwo: główne i nowe zagrożenia, https://www.europarl.europa.eu/news/pl/headlines/society/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia (dostęp: 17.05.2023).
Domaszk A., *Konferencja naukowa „Etyczne i prawne wyzwania Internetu"*, „Prawo Kanoniczne: Kwartalnik Prawno-Historyczny" 2010, nr 53/3–4, s. 373–376.
Gryszczyńska A., *Wykorzystanie COVID-19 w scenariuszach ataków opartych na socjotechnice*, „Rocznik Bezpieczeństwa Morskiego. Przestępczość teleinformatyczna 2020" 2021, s. 137–161.
Guerreschi C., *Nowe uzależnienia*, Wydawnictwo Salwator, Kraków 2006.
Haręża A., *Doktryna hakerów – mit czy rewolucja? Uwagi na temat natury informacji, entropii cyberprzestrzeni i postawy awangardy rewolucji postindustrialnej*, „CBKE e-Biuletyn" 2005, nr 1, s. 13–14, https://www.bibliotekacyfrowa.pl/Content/23674/Doktryna_Hakerow.pdf (dostęp: 9.10.2024).
Internet Organised Crime Threat Assessment (IOCTA), https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020 (dostęp: 18.05.2023).
Jucewicz A., *Człowiek „w sieci" jako problem etyczny*, „Nurt SVD" 2022, t. 151, nr 1, s. 36–50.
Kosiński J., *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015.
Kozak S., *Patologia cyfrowego dzieciństwa i młodości*, Difin, Warszawa 2014.
Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działań CERT Polska 2021, Państwowy Instytut Badawczy NASK, Warszawa 2022.
Kulesza J., *Ius Internet. Między prawem a etyką*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2010.
Lange R., Błażej M., Konopczyński F., Ładna A., *Nastolatki wobec pornografii cyfrowej. Trajektorie użytkowania. Raport z badań ogólnopolskich*, Państwowy Instytut Badawczy NASK, Warszawa 2022.
Netykieta, czyli savoir-vivre *w internecie*, https://www.gov.pl/web/baza-wiedzy/netykieta-czyli-savoir-vivre-w-internecie (dostęp: 19.05.2023).
Mitinck K., *Człowiek to najsłabsze ogniwo*, https://itwiz.pl/jak-skutecznie-zabezpieczyc-najslabsze-ogniwo-bezpieczenstwie/(dostęp: 16.05.2023).
Pączkowski T., *Słownik cyberbezpieczeństwa*, Szkoła Policji w Katowicach, Katowice 2017.
Podgórecki A., *Socjotechnika: praktyczne zastosowania socjologii*, Wydawnictwo: Książka i Wiedza, Warszawa 1968.
Raport Threat Landscape 2022, https://www.europarl.europa.eu/news/pl/headlines/society/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia (dostęp: 29.09.2023).
Rodzaje ataków, https://dataspace.pl/blog/dos-rodzaje-atakow-cz-1/ (dostęp: 19.05.2023).
Rozpoznawanie nieprawdziwych informacji, https://www.gov.pl/web/baza-wiedzy/rozpoznawanie-nieprawdziwych-informacji (dostęp: 28.09.2023).

Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016, Warszawa 2010.

Siwicki M., *Cyberprzestępczość*, C.H. Beck, Warszawa 2013.

Szpunar M., *Społeczności wirtualne jako nowy typ społeczności – eksplikacja socjologiczna*, „Studia Socjologiczne" 2004, nr 173(2), s. 95–130.

Trusewicz-Pasikowska M., *Tożsamość wirtualna – droga do wyzwolenia czy zniewolenia?*, [w:] *Co nas wyzwala, co nas zniewala? Młodzi o wolności*, red. A. Kampka i in., Wydawnictwo SGGW, Warszawa 2018.

Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*, https://www.dziennikustaw.gov.pl/M2019000103701.pdf (dostęp: 29.09.2023).

Wojtasik Ł., *Seksting*, [w:] *Bezpieczeństwo dzieci online. Kompendium dla rodziców, nauczycieli i profesjonalistów*, red. A. Wrzesień-Gandolfo, Polskie Centrum Programu Safer Internet, Warszawa 2014, s. 91–97.

Zajęcka B., *Internet – przyjaciel czy wróg współczesnej młodzieży?*, „Prace Naukowe Akademii im. Jana Długosza w Częstochowie. Seria Pedagogika" 2012, t. XXI, s. 209–220.

Zegarow P., *Psychologiczne aspekty cyberbezpieczeństwa*, Państwowy Instytut Badawczy NASK, Warszawa 2019.

Aspekty etyczne niebezpieczeństw w cyberprzestrzeni

Streszczenie

Artykuł porusza problematykę świadomości użytkowników Internetu na temat zagrożeń, które mogą napotkać podczas korzystania z sieci. Wirtualna rzeczywistość stała się nieodłącznym elementem współczesnego świata, a intensywny rozwój technologii informacyjnych przyniósł nie tylko liczne korzyści, ale również wiele zagrożeń. W artykule zaprezentowano najczęstsze zagrożenia związane z cyberprzestrzenią oraz metody zapobiegania im. Podkreślono etyczne aspekty cyberprzestrzeni oraz rolę rodziców, nauczycieli, a także instytucji edukacyjnych w kształtowaniu świadomości młodych użytkowników w zakresie bezpiecznego korzystania z nowych technologii.

Słowa kluczowe: cyberatak, cyberbezpieczeństwo, cyberprzestępczość, netykieta, świat wirtualny

Beata Zajęcka – pedagog specjalny w zakresie resocjalizacji, dr, adiunkt w Katerze Nauk o Wychowaniu Uniwersytetu Jana Długosza w Częstochowie. Autorka wielu publikacji koncentrujących się na problematyce zachowań ryzykownych dzieci i młodzieży, a także na resocjalizacji instytucjonalnej nieletnich i dorosłych sprawców czynów karalnych.

Marek Kopiec – pedagog, mgr, asystent w Katerze Nauk o Wychowaniu Uniwersytetu Jana Długosza w Częstochowie, emerytowany funkcjonariusz Policji zajmujący się cyberbezpieczeństwem. W swojej działalności naukowej skupia się na

problemach społecznych współczesnego świata, zwłaszcza tych związanych z nowymi technologiami. Jest współorganizatorem ogólnopolskiej konferencji naukowej „Pedagogiczne i Techniczne Aspekty Cyberbezpieczeństwa". Swoje działania koncentruje także na profilaktyce związanej z podnoszeniem świadomości w korzystaniu z nowych technologii.

Ethical Aspects Dangers in Cyberspace

Abstract

This article addresses the issue of Internet users' awareness of the risks they may encounter when using the web. Virtual reality has become an inseparable element of the modern world and the intensive development of information technology has brought not only numerous benefits but also a number of threats. The article presents the most common cyber threats and methods of their prevention. The ethical aspects of cyberspace and the role of parents, teachers and educational institutions in shaping the awareness of young users of the safe use of new technologies are highlighted.

Keywords: cyberattack, cybercrime, cybersecurity, netiquette, virtual world

Beata Zajęcka – special pedagogue in the field of re-socialisation, PhD, assistant professor in the Department of educational sciences at Jan Dlugosz University in Czestochowa. Author of numerous publications focusing on risk behaviour of children and adolescents as well as institutional rehabilitation of juvenile and adult offenders.

Jan Dlugosz – pedagogue, MA, assistant in the Department of educational sciences at Jan Dlugosz University in Czestochowa, retired police officer dealing with cyber security. In his scientific activity, he focuses on social problems of the modern world, especially related to new technologies. He is the co-organiser of the national scientific conference 'Pedagogical and Technical Aspects of Cyber Security'. He also focuses his activities on prevention related to raising awareness in the use of new technologies.