Cyberbezpieczeństwo

teoretycznie i empirycznie
w naukach o bezpieczeństwie

Redakcja naukowa:
Robert, Adam Janczewski

Recenzenci:
dr hab. inż. Halina Świeboda
dr hab. inż. Krzysztof Wysocki

Redakcja naukowa
dr inż. Robert Janczewski

Redakcja techniczna, opracowanie graficzne, projekt okładki
dr inż. Robert Janczewski

Forma i treść przedstawionych materiałów odpowiada wersji przekazanej przez ich autorów.

Wydawca:
Wydawnictwo BP
bartlomiej@paczek.eu
tel. 887-021-030
Gdynia

ISBN
978-83-65763-50-1

Książkę sfinansowało
Morskie Centrum Cyberbezpieczeństwa

Spis treści

WSTĘP

Cyberbezpieczeństwo stanowi zagadnienie wieloaspektowe. Jego znaczenie w społeczeństwach, które swoje funkcjonowanie uzależniły od sieci i systemów teleinformatycznych wciąż rośnie. Zagadnieniu temu poświęconych zostało wiele spotkań roboczych, konferencji naukowych oraz wysiłków badawczych. Zarówno praktycy jak i teoretycy prowadzą dyskusje na temat bezpieczeństwa samych sieci i systemów teleinformatycznych oraz bezpieczeństwa instytucji, w których teleinformatyka stanowi kluczowy i fundamentalny zasób.

Cyberbezpieczeństwo cechuje się wielowymiarowością. Na rynku wydawniczym polskim i zagranicznym istnieje bogata literatura, prezentująca problemy cyberbezpieczeństwa wielu wymiarach od technicznych po społeczne i psychologiczne. Obszar ulega dynamicznym zmianom, wymaga ciągłych badań i innowacyjnego spojrzenia, i dociekania złożonych, i zmiennych zagrożeń. Niniejsza monografia stanowi wynik naukowych rozważań nad problematyką cyberbezpieczeństwa podchorążych Marynarki Wojennej w Gdyni. Jest próbą usystematyzowania wiedzy w oparciu o analizę i krytykę piśmiennictwa oraz metody empiryczne (np. sondaż diagnostyczny), które wzbogacają niniejsze opracowanie o unikalne wyniki.

Monografia przeznaczona jest zarówno dla specjalistów zajmujących się cyberbezpieczeństwem, jak i dla każdego użytkownika sieci i systemów teleinformatycznych. Jest źródłem cennych informacji dla wojskowych, jak i tych osób, które nie są związane z wojskowością. Należy jednak mieć na uwadze, że treści niniejszej publikacji, ze względu na dynamikę zmian jakie dokonują się w przedmiotowym obszarze, z czasem ulegną dezaktualizacji a aktualizację wyznaczą nowe badania naukowe. Monografię poświęcono problemom dezinformacji, socjotechnice, audytom i certyfikacji, białemu wywiadowi ujmując treści badań z różnych punktów dociekań. Wobec tak zróżnicowanego podejścia to zagrożenia i problemy cyberbezpieczeństwa stworzyły ramy dla pracy. Zasadniczym wyzwaniem była chęć prezentacji naukowego dorobku w tym obszarze podchorążych Marynarki Wojennej w Gdyni. W mnogości cyberzagrożeń ale również działań w zakresie cyberbezpieczeństwa autorzy starają się odpowiedzieć na pytanie jaki jest aktualnie stan bezpieczeństwa i zagrożeń cyberprzestrzeni.

Zagadnienia pozostające w zakresie tematu niniejszej publikacji ujęto i zaprezentowano w poszczególnych rozdziałach przedstawiając wiele aspektów cyberbezpieczeństwa umożliwiających poznanie ich natury i charakteru.

Martyna Bukacka w rozdziale pierwszym zatytułowanym *Dezinformacja jako element wojny hybrydowej* zaprezentowała wyniki swoich badań nad dezinformacją jako elementem wojny hybrydowej. Przedmiotem badań były działania dezinformacyjne we współczesnych konfliktach zbrojnych, działaniach terrorystycznych i występujących poniżej progu wojny. Autorka

umiejscowiła dezinformację wśród działań w czasie wojny hybrydowej. Szczególną uwagę skupiła na analizie rodzajów dezinformacji, jej użycia we współczesnych konfliktach oraz kroków, które są podejmowane w celu przeciwdziałania dezinformacji. W pracy uporządkowano pojęcia dotyczące dezinformacji oraz wojny hybrydowej.

Manuela Chamera w rozdziale drugim *Socjotechnika a cyberprzestępczość na wybranych przykładach* w oparciu o wyniki własnych badań opisała zależności między socjotechniką a cyberprzestępczością. Przedstawiła podstawowe pojęcia z zakresu cyberprzestępczości. Zaprezentowała szereg elementarnych pojęć związanych z socjotechniką i cyberprzestępczością. W pracy opisuje uwarunkowania oraz doświadczenia praktyczne w zakresie wykorzystania socjotechniki w cyberprzestępczości. Szczególną uwagę skupiła na analizie klasyfikacji ataków w cyberprzestrzeni oraz przedstawieniu podstawowych typów ataków wykorzystujących inżynierię społeczną. W pracy przedstawiono także istotę sposobów obrony przed atakami.

Szymon Cydejko w rozdziale trzecim zatytułowanym *Audyt i certyfikacja wojskowych systemów teleinformatycznych* przedstawił wyniki swoich rozważań nad istotą audytu i certyfikacji wojskowych systemów teleinformatycznych. Opracowanie zawiera zagadnienia z zakresu polityki bezpieczeństwa informacji, procesu akredytacji systemów teleinformatycznych oraz dokumentacji bezpieczeństwa teleinformatycznego. Rozważania w tym zakresie uzupełnia prezentacja oprogramowania narzędziowego stosowanego w audycie oraz analiza aktów prawnych i standardów z zakresu bezpieczeństwa teleinformatycznego. Autor szczególną uwagę skupił na wykazaniu, iż audyt jest procesem wysoce rygorystycznym, bazującym na ściśle określonych normach i standardach.

Marlena Dymowska w rozdziale *Inżynieria społeczna w atakach hakerskich* zaprezentowała wyniki swoich dociekań naukowych na taki właśnie temat. Opracowanie dotyczy technik inżynierii społecznej, jakimi posługują się współcześni cyberprzestępcy w swoich atakach. W pracy wyjaśniono definicje, które odnoszą się do tematu. Przedstawiono podstawowe pojęcia z zakresu socjotechniki i reguł wywierania wpływu, które stosowane są w życiu codziennym oraz przez socjotechników. Zwrócono uwagę na podział zagrożeń występujących w Internecie oraz jakie skutki mogą nieść za sobą zbyt szybkie podejmowanie decyzji w sieci. Omówiono negatywny wpływ zagrożeń na ludzkie zachowanie i psychikę. W pracy ustalano możliwe sposoby obrony przez cyberatakami. Praca koncentruje się na zagadnieniu stosowania technik socjotechnicznych w atakach hakerskich. Wskazuje w jaki sposób atakujący dzięki wykorzystaniu inżynierii społecznej dokonują czynów zabronionych i atakują użytkowników Internetu.

Bartłomiej Gostkowski w rozdziale piątym *Świadomość studentów Akademii Marynarki Wojennej w Gdyni na temat zagrożeń wynikających z użytkowania cyberprzestrzeni* przedstawił wyniki własnych badań świadomości studentów Akademii Marynarki Wojennej w Gdyni na temat zagrożeń

wynikających z użytkowania cyberprzestrzeni. Praca prezentuje poziom świadomości studentów Akademii Marynarki Wojennej w Gdyni na temat cyberzagrożeń w oparciu o analizę wyników badań przeprowadzonych metodą sondażu diagnostycznego, techniką ankiety, z wykorzystaniem kwestionariusza ankiety jako narzędzia badawczego. Praca zawiera analizę pojęcia cyberprzestrzeni, charakterystykę cyberzagrożeń oraz wyniki badań empirycznych przeprowadzonych w grudniu 2020 roku.

Dawid Jutrzenka Trzebiatowski w rozdziale szóstym *Bezpieczeństwo informacji niejawnych w systemach teleinformatycznych Sił Zbrojnych Rzeczypospolitej Polskiej* na podstawie wyników własnych badań opisał bezpieczeństwo informacji niejawnych w systemach teleinformatycznych Sił Zbrojnych Rzeczypospolitej Polskiej. Przedmiotem badań były zasady funkcjonowania systemu zarządzania bezpieczeństwem informacji niejawnych. W swojej pracy autor zaprezentował również wymagania bezpieczeństwa stawiane wojskowym sieciom telekomunikacyjnym oraz stosowane środki ochrony w świetle potencjalnych zagrożeń. Autor szczególną uwagę skupił na analizie obowiązujących uwarunkowań formalno- prawnych i zbudowanym, w oparciu o nie, systemie ochrony systemów teleinformatycznych Sił Zbrojnych Rzeczypospolitej Polskiej.

Marcin Kaźmierczak w rozdziale siódmym *Biały wywiad internetowy* w oparciu o wyniki własnych badań opisał biały wywiad internetowy. W opracowaniu zawarł zagadnienia związane z białym wywiadem, jego definicje, sposoby działania oraz wykorzystania, potencjał i zagrożenia. Autor dokonał charakterystyki białego wywiadu w sektorze prywatnym i publicznym. Szczególną uwagę skupił na możliwościach praktycznego wykorzystania OSINT na przykładzie wybranych narzędzi, takich jak: OsintFramework, Maltego oraz Oryon OSINT Browser. Stanowi to wartościowy wkład poznawczy w obszar cyberbezpieczeństwa.

Aleksandra Pawlikowska (Łuka) w rozdziale ósmym *Narzędzia i techniki dezinformacji wykorzystywane przez Federację Rosyjską w cyberprzestrzeni* opierając się o swoje dociekania naukowe przedstawiła narzędzia i techniki dezinformacji wykorzystywane przez Federację Rosyjską w cyberprzestrzeni. W pracy przedstawiła istotę dezinformacji oraz metody dezinformacji stosowane przez Rosję. Autorka umieściła, także opis czynności i działań podejmowanych w celu przeciwdziałania oraz zwalczania tego zjawiska. Dodatkowo autorka sprecyzowała cele Federacji Rosyjskiej związane z polityką zagraniczną w zakresie przedmiotu swoich dociekań naukowych.

Kacper Pirch w rozdziale dziewiątym *Socjotechnika jako cyberzagrożenie* zaprezentował socjotechnikę jako cyberzagrożenie. Dokonał analizy, dlaczego działania cyberprzestępców oraz działalność militarna przenoszona jest do cyberprzestrzeni oraz zaprezentował podział cyberzagrożeń ze względu na zagrożenia techniczne oraz nietechniczne. Scharakteryzował działanie najbardziej rozpowszechnionych metod, które wykorzystywane są do pozyskiwania danych szczególnej kategorii. Ponadto, zaprezentował socjotechnikę jako

cyberzagrożenie opierając si na definicję inżynierii społecznej metodykę działania cyberprzestępców posługujących się tym narzędziem. W rozdziale tym również przedstawiono cykl socjotechniczny opracowany przez Kevina Mitnicka.

Kuba Wojnicki w rozdziale dziesiątym *Cyberzagrożenia w aspekcie bezpieczeństwa narodowego* analizował cyberzagrożenia w aspekcie bezpieczeństwa narodowego. Treść opracowania stanowi prezentacja wyników własnych badań nad cyberzagrożeniami mogącymi wpłynąć niekorzystnie na bezpieczeństwo narodowe. Autor przybliżył pojęcia związane z cyberprzestrzenią i jej bezpieczeństwem, aspekty cyberterroryzmu skierowanego przeciwko infrastrukturze krytycznej państwa oraz wojny informacyjnej. Autor szczegółowo opisał popularne cyberataki dotykające państwo, ale także obywateli jako użytkowników sieci i systemów teleinformatycznych. W pracy uporządkowano pojęcia dotyczące cyberbezpieczeństwa i cyberprzestępczości.

Rozdział jedenasty autorstwa **Jakuba Zambrowskiego** zatytułowany *Incydenty w cyberprzestrzeni* stanowi prezentację wyników własnych badań incydentów w cyberprzestrzeni. Autor pracy przedstawia cyberprzestrzeń jako wymiar fizyczny, wirtualny oraz ludzki. Przybliża pojęcia z zakresu cyberbezpieczeństwa oraz przedstawia kluczowe dokumenty normatywne oraz akty prawne dotyczące cyberprzestrzeni w perspektywie Rzeczypospolitej Polskiej oraz Unii Europejskiej. Charakteryzuje incydent jako wykorzystanie podatności systemu teleinformatycznego oraz naruszenie atrybutów bezpieczeństwa. Autor prezentuje wyniki swoich badań studium przypadku - ataku Stuxnet. W pracy omówił także złośliwe oprogramowanie statystycznie najczęściej wykorzystywane w okresie ostatnich lat.

dr inż. Robert Janczewski

bsmt pchor. Martyna BUKACKA

DEZINFORMACJA JAKO ELEMENT WOJNY HYRYDOWEJ

Streszczenie

Niniejsze opracowanie dotyczy działań dezinformacyjnych w wojnie hybrydowej oraz we współczesnych konfliktach zbrojnych jako jednych z najbardziej niebezpiecznych, współczesnych zagrożeń. Dezinformacja jest wyjaśniona, zostały podane jej rodzaje i przykłady oraz została umiejscowiona w walce informacyjnej, cyberprzestrzeni. Przedstawiono również pojęcia wojny hybrydowej oraz jej specyfikę. Ponadto, przytoczono przykłady jej wykorzystania w działaniach terrorystycznych oraz agresji poniżej progu wojny. Zawiera również ocenę zagrożenia przez Ministerstwo Obrony Narodowej. Regularnie przeciwdziała dezinformacji, opracowując i wdrażając plany działania oraz kształcąc młodych ludzi w tym kierunku. Rezultatem niniejszej pracy jest osiągnięcie celu, czyli udowodnienie, że dezinformacja jest elementem wojny hybrydowej.

Słowa kluczowe:
wojna hybrydowa, dezinformacja, walka informacyjna, cyberprzestrzeń, współczesne konflikty, agresja poniżej progu wojny, terroryzm

Abstract

Disinformation as an element of hybrid warfare

The article concerns disinformation activities in hybrid war and in contemporary armed conflicts as one of the most dangerous contemporary threats. Disinformation is explained, types and examples are given, and it has been placed in the information warfare, cyberspace. The concepts of hybrid war and its specificity are also presented. Moreover, examples of its use in terrorist activities and aggression below the threshold of war were presented. It also includes a threat assessment by the Ministry of National Defense. It regularly counteracts disinformation by developing and implementing action plans and educating young people in this direction. The result of the work is the achievement of the goal, i.e., proving that disinformation is an element of hybrid war.

Keywords:
hybrid warfare, disinformation, information warfare, terrorism, cyberspace, modern conflicts.

Wstęp

Dezinformacja stanowi jedno z najbardziej niebezpiecznych działań wojny hybrydowej. Informacja oraz jej manipulacja w dzisiejszych czasach jest bardzo ważnym składnikiem konfliktów oraz czynnikiem, który ma ogromny wpływ na przewagę nad przeciwnikiem. Celem niniejszego rozdziału jest umiejscowienie dezinformacji wśród działań wojny hybrydowej. Szczególnej analizie zostały poddane rodzaje dezinformacji, użycie jej we współczesnych konfliktach oraz kroki, które są podejmowane w kierunku jej przeciwdziałania. Ponadto, celem pracy jest uporządkowanie pojęć dotyczących dezinformacji oraz wojny hybrydowej. Przedmiotem badań są działania dezinformacyjne we współczesnych konfliktach zbrojnych, działaniach terrorystycznych i występujących poniżej progu wojny.

Pojęcie oraz rodzaje dezinformacji

Dezinformację można ująć w wielu aspektach. Słownik języka polskiego podaje definicję w ogólnym pojęciu jako „wprowadzenie kogoś w błąd przez podanie mylących lub fałszywych informacji”[1].

Dezinformacja w dokumencie doktrynalnym Ministerstwa Obrony Narodowej jest wyjaśniona jako „wszelkie przedsięwzięcia mające na celu wprowadzenie przeciwnika w błąd poprzez manipulowanie, działania pozorujące i preparowanie dowodów, prowokujące działania szkodzące jego własnym interesom”[2]. Jej celem jest manipulacja percepcją poprzez stosowanie środków decydentów przeciwnika, manipulacja zachowaniami, uzyskiwanie zamierzonych reakcji. Powinna być realizowana przy pełnym wsparciu innych działań. Dezinformacja może mieć kluczowe znaczenie przy osiągnięciu sukcesu podczas prowadzenia operacji[3]. Można wyróżnić cztery rodzaje dezinformacji: wojskowa, polityczna, ekonomiczna oraz naukowo-techniczna[4].

Rodzaj **dezinformacji wojskowej** to „zamierzone przekazywanie przygotowanych (fałszywych) informacji, pogłosek, specjalnie opracowanych dokumentów oraz demonstrowanie działań wojsk, których celem jest wprowadzenie w błąd przeciwnika w odniesieniu do prawdziwych zamierzeń, planów i przedsięwzięć o znaczeniu militarnym”[5]. „Obiektami dezinformacji wojskowej są: przeciwnik, wojska własne i otoczenie, które stanowi płaszczyznę kontaktów obu stron”[6].

Dezinformacja polityczna jest „prowadzona w sferze wewnętrznej i zewnętrznej (zagranicznej) przez centralne kierownictwo państwa. W polityce wewnętrznej elementem jest własne społeczeństwo. Dezinformacja w tym zakresie

[1] https://sjp.pwn.pl/sjp/dezinformacja;2554971.html, dostęp: 07.12.2020 r.
[2] Słownik terminów i definicji NATO, AAP (2015), str. 128, cyt. za: DD 3.10(A), *Operacje informacyjne*, Ministerstwo Obrony Narodowej, Centrum Doktryn i Szkolenia Sił Zbrojnych, Bydgoszcz 2017, str. 2-15.
[3] Tamże.
[4] A. Żebrowski, *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2016, s. 447.
[5] http://wiedzaobronna.edu.pl/index.php/wo/article/view/39/39, dostęp 12.12.2020 r.
[6] A. Żebrowski, *Walka informacyjna…*, dz. cyt., s. 447.

służy kształtowaniu pożądanych postaw, opinii i zachowań współobywateli (…). Natomiast dezinformacja w polityce zagranicznej ma za zadanie tworzenie pozytywnego wizerunku własnego państwa na arenie międzynarodowej”[7]. Przykładem tego rodzaju dezinformacji może być stanowisko Republiki Turcji, która zapiera się dokonania ludobójstwa na ludności Ormiańskiej w celu manipulacji wydarzeniami historycznymi oraz próby uzyskania lepszego wizerunku swojego państwa, a także prowokacja gliwicka z 31 sierpnia 1939 roku.

Dezinformacja ekonomiczna „ma na celu wprowadzenie przeciwnika w błąd co do stanu rzeczywistych osiągnięć ekonomiczno-gospodarczych, dotyczących możliwości obronnych państwa”[8], właśnie na tym polegał projekt Wunderwaffe – *cudownabroń III Rzeszy*.

Dezinformacja naukowo-techniczna polega na zatajeniu przed potencjalnym przeciwnikiem swoich osiągnięć w różnych dziedzinach, m.in.: innowacyjnych odkryć z zakresu zdolności obronnej państwa[9]. Zilustrowaniem tej dezinformacji jest wysłanie w kosmos przez Związek Socjalistycznych Republik Radzieckich Sputnika 1.

Dezinformacja w walce informacyjnej

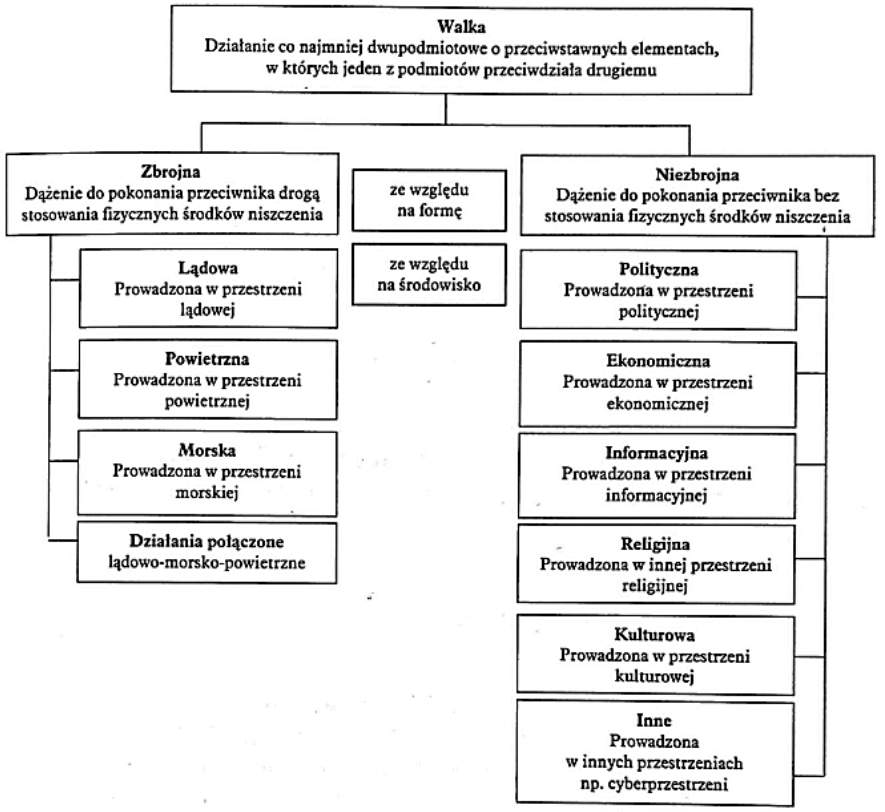
Piotr Sienkiewicz definiuje walkę informacyjną jako „całokształt działań ofensywnych i defensywnych koniecznych do uzyskania przewagi informacyjnej nad przeciwnikiem i osiągnięcia zamierzonych celów militarnych (politycznych)”[10]. Wyodrębnił on również cztery jej cechy:

- jej głównym celem jest uzyskanie supremacji informacyjnej,
- przeciwnik jest w niej ciężki do zidentyfikowania, pozostaje on niewidoczny,
- polem walki jest cyberprzestrzeń,
- czas to czynnik krytyczny[11].

Walka informacyjna jest takim sposobem walki, w którym informacja stanowi broń (narzędzie walki) oraz cel ataku[12].

Ogólna walka dzieli się na zbrojną oraz niezbrojną. Rysunek 1.1 przedstawia ujęcie walki informacyjnej w pełnym wymiarze walki. Jest ona elementem walki niezbrojnej, prowadzi się ją w przestrzeni informacyjnej.

[7] Tamże.
[8] Tamże.
[9] Tamże.
[10] P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, [w:] L. S. Haber, *Społeczeństwo informacyjne – wizja czy rzeczywistość*, Akademia Górniczo-Hutnicza, Kraków 2004, s. 375, cyt. za: P. Dela, *Teoria walkiw cyberprzestrzeni*, Akademia Sztuki Wojennej, Warszawa 2020, s. 18.
[11] Tamże.
[12] T. R. Aleksandrowicz, *Podstawy walki informacyjnej*, Editions Spotkania, Warszawa 2016, s. 129.



Źródło: A. Żebrowski, *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego* s. 91 na podstawie L. Ciborowski, *Mechanizmy i przestrzenie walki informacyjnej*, [w:] G. Nowacki (red.), *Informacja w walce zbrojnej*, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2002, s. 53.

Rysunek 1.1. Miejsce walki informacyjnej w ogólnej przestrzeni walki

W walce informacyjnej przeciw zorganizowanym strukturom, szczególnie państwom i ich centralnym ośrodkom decyzyjnym, jako jedną z zastosowanych metod wyróżnia się implementację u przeciwnika mechanizmów umożliwiających samosterowanie, w tym dezinformację[13]. Manipulacja to nierozłączne narzędzie dezinformacji. W walce informacyjnej ma ona na celu wpojenie ludziom, że walczą o swoje własne interesy, bądź realizują wzniosłe cele. W rzeczywistości jednak, działają oni w zupełnie przeciwnym kierunku. Manipulacja kieruje często ludźmi w ten sposób, aby myśleli, że ich działania są samowolne oraz niezależne[14].

[13] https://socjocybernetyka.files.wordpress.com/2010/08/totalna-wojna-informacyjna.pdf, s. 5, dostęp: 11.12.2020 r.
[14] http://www.autonom.edu.pl/publikacje/kossecki_jozef/elementy_wojny_informacyjnej-ocr.pdf, s. 1,
dostęp: 11.12.2020 r.

Walka informacyjna ma zastosowanie nie tylko w sferze militarnej, ale także w polityce, gospodarce i kulturze. Istotną jest umiejętność selekcji i analizy informacji. Zważając na wydarzenia związane z działaniami dezinformacyjnymi, należy poddać ocenie daną informację w różnych kontekstach, choć jej rozpoznanie jest bardzo skomplikowanym zabiegiem. Charakterystyczne jest np. w białym wywiadzie nadawanie odpowiednich ocen dla informacji i jej źródła, w celu lepszego określenia jej przydatności[15].

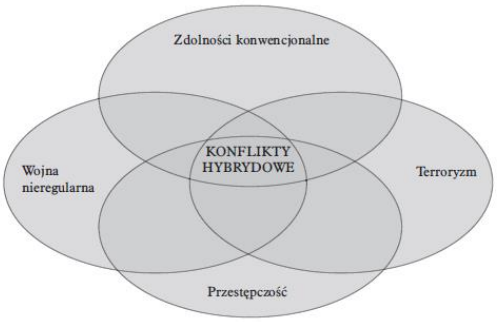
Pojęcie wojny hybrydowej

Wojnę hybrydową od wojen konwencjonalnych różni jej specyfika. Ewolucja wojen związana jest z rozwojem technologii i człowieka. Czynnikiem, który nie ulega zmianie jest podłoże konfliktów. Postęp mass mediów przyczynił się do większych możliwości rozwoju oraz przekazywania informacji[16]. Wojna hybrydowa łączy w sobie konwencjonalne techniki prowadzenia konfliktów z nowoczesnymi metodami.

Łaciński termin „hybryda" oznacza mieszańca, który powstał poprzez skrzyżowanie dwóch różniących się genetycznie gatunków, odmian czy ras[17]. Hybrydowość w ogólnym ujęciu oznacza zestawienie ze sobą odmiennych części, które nie muszą być ze sobą powiązane. Definicja przytoczona w (mini)słowniku Biura Bezpieczeństwa Narodowego reguluje wojnę hybrydową w następujący sposób: „wojna łącząca w sobie jednocześnie różne możliwe środki i metody przemocy, w tym zwłaszcza zbrojne działania regularne i nieregularne, operacje w cyberprzestrzeni oraz działania ekonomiczne, psychologiczne, kampanie informacyjne (propaganda) itp."[18].

Rysunek 2.1 przedstawia składowe złożonego konfliktu hybrydowego, który jest odzwierciedleniem przytoczonych wyżej definicji. Jego elementami są: zdolności konwencjonalne, wojna nieregularna, terroryzm, przestępczość[19].

[15] https://www.app.college.police.uk/app-content/information-management/management-of-police-information/collection-and-recording/, dostęp 11.12.2020.
[16] https://repozytorium.ukw.edu.pl/bitstream/handle/item/4197/Proba%20wyjasnienia%20pojecia%20i%2 0istoty%20wojen%20hybrydowych.pdf?sequence=1&isAllowed=y, s. 261, dostęp: 11.12.2020 r.
[17] M. Banasik, *Wojna hybrydowa i jej konsekwencje dla bezpieczeństwa euro atlantydzkiego*, Wydawnictwo Difin, Warszawa 2018, s. 63.
[18] https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbnpropozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html, dostęp 20.12.2020.
[19] https://www.ce.uw.edu.pl/pliki/pw/4-2015_hajduk.pdf, s. 137, dostęp: 11.12.2020 r.



Źródło: J. Hajduk, T. Stępniewski, *Wojna hybrydowa Rosji z Ukrainą: uwarunkowania i instrumenty*, https://www.ce.uw.edu.pl/pliki/pw/4-2015_hajduk.pdf, dostęp: 11.12.2020 r.

Rysunek 2.1. Zakres konfliktów hybrydowych według Franka Hoffmana

Specyfika wojen hybrydowych

Wojna hybrydowa cechuje się skrytością intencji oraz nieprzewidywalnością działań. Według pułkownika Grygi podstawą wojny hybrydowej jest sparaliżowanie wnętrza państwa przeciwnika, używając przy tym przede wszystkim środków niemilitarnych, a w mniejszej części militarnych. W wojnie konwencjonalnej zastosowanie tych dwóch elementów wygląda odwrotnie. Wojnę hybrydową prowadzi się bez jej oficjalnego wypowiedzenia[20]. Głównym polem bitwy staje się tutaj umysł człowieka, działania dezinformacyjne, psychologiczne, wpływanie na społeczeństwo oraz jego elity[21].

Źródłami siły wojny hybrydowej mogą stać się:

- idee,
- perswazja elit i opozycjonistów,
- brak obaw społeczności i walczących o konsekwencje działań,
- pewność w swoich działaniach i poglądach,
- metoda swobodnego prowadzenia działań taktycznych[22].

Przytoczone wyżej podpunkty są czynnikami, przez które wojna hybrydowa nabiera wielkości i intensywności działań. Idee zawsze były, są i będą powodem narastania konfliktów. Ludzie dla swoich poglądów są w stanie oddać życie oraz je odebrać. Umiejętność wpływania liderów oraz buntowników na społeczeństwo powoduje wywołanie rozpoczęcia realizacji zamierzonych przez nich działań. W przypadku, kiedy obywatele nie boją się możliwych konsekwencji i kar lub nie są ich świadomi oraz nie są wrażliwi na cierpienia, narastanie konfliktu jest nieuniknione.

[20] https://www.defence24.pl/wojska-specjalne-a-zagrozenia-hybrydowe-cz-1- czym-tak-naprawde-jest-wojna-hybrydowa-raport, dostęp: 02.01, 2021 r.
[21] https://depot.ceon.pl/bitstream/handle/123456789/9904/Banasik,%20Parafianowicz.pdf?sequence=1&is Allowed=y, s. 14, dostęp: 20.12.2020 r.
[22] W. J. Nemeth, *Future war and Chechnya*., s. 62, cyt. za: M. Banasik, *Wojna hybrydowa i jej konsekwencje dla bezpieczeństwa euro atlantydzkiego*, Wydawnictwo Difin, Warszawa 2018, s. 61.

Pewność o słuszności swoich działań jest ważnym elementem wzrastania w sile wojny hybrydowej. W przypadku niedopuszczenia do siebie racji odmiennego stanowiska nie ma szansy na zaprzestanie konfliktu. Decentralizacja taktyki, czyli swoboda działań polega na możliwości przeprowadzania operacji, wykonywania ruchów w różny sposób. Nie muszą być konsultowane ze scentralizowaną władzą.

Tabela 1.1 przedstawia analizę dwóch metod prowadzenia wojny hybrydowej oraz przykładowych sposobów ich wykorzystania. Działania te odbywają się w odmiennych etapach konfliktu oraz w niejednakiej skali[23].

Tabela 1.1

Metody prowadzenia wojny hybrydowej

MILITARNE	NIEMILITARNE
- konwencjonalne działania zbrojne - działania nieregularne - akty terroryzmu	- presja ekonomiczna - duża aktywność służb specjalnych - działania ofensywne w cyberprzestrzeni - wielokierunkowe działania dyplomatyczne

Źródło: Opracowanie własne na podstawie: Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, https://www.abw.gov.pl/download/1/1925/skoneczny pdf, dostęp: 20.12.2020 r.

Cyberprzestrzeń jako wymiar walki w wojnie hybrydowej

Cyberprzestrzeń obok lądu, morza, powietrza oraz przestrzeni kosmicznej stanowi piąty wymiar walki. Ataki w jej obszarze mogą uderzyć bezpośrednio w elity polityczne oraz kluczowe elementy bezpieczeństwa państwa. Jest to bardzo niebezpieczna i ciężka do odparcia ataku strefa. Konflikty w jej zakresie, prowadzone równocześnie z konwencjonalnymi już trwają, a w przyszłości mogą stanowić podstawową płaszczyznę prowadzenia wojen[24].

W dzisiejszych czasach technologia jest na tyle rozwinięta, że bazując na technikach używanych w zakresie cyberprzestrzeni możliwa staje się kontrola nowoczesnego uzbrojenia, jej destrukcja oraz przekierowanie przeciw osobie z niej korzystającej. Przez dezinformację, która bezsprzecznie jest częścią cyberprzestrzeni w walce informacyjnej istnieje możliwość pozbawienia przeciwnika wizerunku wśród swojego własnego społeczeństwa oraz innych państw całego świata[25].

[23] https://www.abw.gov.pl/download/1/1925/skoneczny.pdf, s. 46, dostęp: 20.12.2020 r.
[24] P. Dela, *Teoria walki w cyberprzestrzeni*, Akademia Sztuki Wojennej, Akademia Sztuki Wojennej, Warszawa 2020, s. 22.
[25] Tamże.

Centrum Doskonalenia Cyberobrony w Tallinie na rzecz NATO stworzyło następującą definicję cyberprzestrzeni: „zależny od czasu zbiór połączonych systemów informacyjnych oraz ludzi/użytkowników wchodzących w interakcje z tymi systemami”[26].

Najważniejszym elementem w cyberprzestrzeni jest informacja, a wszystkie jej zagrożenia są z nią powiązane[27]. Walka informacyjna w cyberprzestrzeni wywołuje konflikt[28]. Można, więc stwierdzić, iż skoro walka informacyjna jest elementem wojny hybrydowej to cyberprzestrzeń z pewnością jest jej wymiarem.

Dezinformacja we współczesnych konfliktach zbrojnych

„Wojna jest Tao wprowadzania w błąd. Jeśli zatem jesteś zdolny, udawaj mało zdolnego. Gdy podrywasz swoje wojska do działania, udawaj bierność. Jeżeli twój cel jest bliski, zachowuj się tak, jakby był odległy. A gdy jest odległy, udawaj, że jest bliski”[29]. Powyższy cytat Sun-Tzu, autora pierwszego podręcznika sztuki wojennej i pierwszego realisty w teorii stosunków międzynarodowych oraz prakseologa współczesnego biznesu, który żył i tworzył 2500 lat temu nie uległ dewaluacji.

Współczesne konflikty zbrojne są tymi, które rozpoczęły się pod koniec dwudziestego wieku. Cechują się asymetrią, nieregularnością, dużą ilością podmiotów biorących w nich udział oraz próbami rozstrzygnięcia konfliktu przez niezaangażowanych, wyznaczonych prawem międzynarodowym[30]. Jako przełom w filozofii prowadzenia wojen uznaje się rozpad ZSRR, zakończenie procesu dekolonizacji oraz militaryzację społeczeństwa. W konfliktach hybrydowych zdecydowanie zanika granica między obywatelami a żołnierzami, traci się poziom działań strategicznych, operacyjnych i taktycznych oraz różnicę pomiędzy operacjami ofensywnymi i defensywnymi[31].

Niezależnie od tego, w którym miejscu toczą się konflikty, zawsze mają wpływ na społeczność światową. Powodem tego są stosunki i relacje międzypaństwowe oraz przyrost liczby uchodźców. Środki maskowego przekazu (telewizja, Internet) spowodowały, że wojny oraz informacje o nich posiadają cechy natychmiastowości i globalności[32]. Żyje nimi cały Świat.

---

[26] R. Ottis, P. Lorents, *Cyberspace: definition and Implications, Cooperative Cyber Defense Center of Exellence*, Tallin 2010, cyt za: P. Dela, *Teoria walki w cyberprzestrzeni*, Akademia Sztuki Wojennej, Warszawa 2020, s. 34.

[27] P. Dela, *Teoria walki…,* dz. cyt., s. 34.

[28] http://www.abw.gov.pl/download/1/2170/TomaszRAleksandrowicz.pdf, s. 15, dostęp: 11.12.2020 r.

[29] https://graduacja.lazarski.pl/fileadmin/user_upload/dokumenty/student/Sun_Tzu_sztuka_wojny.pdf, s. 11, dostęp: 30.12.2020 r.

[30] I. Denysiuk, M. Osypowicz, *Współczesne oblicze konfliktów zbrojnych – nowe zjawisko a kontynuacja nurtu działań partyzanckich*, Oficyna Wydawnicza ASPRA-JR, Siedlce 2018, s. 340.

[31] Tamże.

[32] https://www.znak.com.pl/ksiazka/wspolczesne-konflikty-zbrojne-los-robert-reginia-zacharski-jacek44116, dostęp: 30.12.2020 r.

Klasycznym przykładem dezinformacji jako elementem wojny hybrydowej jest aneksja Krymu przez Rosję. Agresja zaczęła się od działań nieregularnych polegających na wykorzystaniu na dużą skalę funkcjonariuszy rosyjskich służb specjalnych oraz żołnierzy jednostek specjalnych SPECNAZ, pod postacią „lokalnych oddziałów samoobrony". Oddziały te inspirowały niezadowolenie miejscowej ludności, dezinformowały i manipulowały opinią, co ułatwiło przejęcie kontroli nad budynkami administracji rządowej, infrastrukturą krytyczną oraz jednostkami wojskowymi. Dezinformacja była na tyle skuteczna, że wojsko, aparat państwowy i społeczeństwo zostały sparaliżowane i stały się niezdolne do stawiania oporu. Zdezorientowana była też światowa opinia publiczna, ponieważ dopiero 25 marca, czyli blisko miesiąc od aneksji Rada Europy, a później ONZ wydały oświadczenie potępiające agresję[33].

Pierwszą w historii wojnę internetową wywołał konflikt w Kosowie w czasie, którego użyto całego wachlarza środków. Internet był narzędziem propagandy, komunikacji, demonizowania i dyskredytacji przeciwnika (dezinformacja), cyberataków, Denial of Service (DoS), Denial of Service (DDoS), e-mail bombingu, włamywania się na konta i portale internetowe itp. Internet wspierał oficjalną narrację propagandową obu stron. Serbowie wysyłali codziennie pocztą elektroniczną tysiące wiadomości e-mailowych do mediów, środowisk opiniotwórczych i rządów z apelami o zaprzestanie ataków z powietrza. Znaczna część e-maili miało charakter antykoalicyjny, a inne wyolbrzymiały skutki ataków, które powodowały natowskie samoloty. Londyński korespondent *Washington Post* Tom Reid, twierdził, że był adresatem do 50 elektronicznych wiadomości dziennie od serbskich profesorów z różnych uniwersytetów i aktywistów z prośbą o apel, by wstrzymać bombardowania. „Pamiętaj, że pod twoimi bombami giną ludzie"[34].

Dezinformacja w działaniach terrorystycznych

Terroryzm to „różnie umotywowane, najczęściej ideologicznie, planowane i zorganizowane działania pojedynczych osób lub grup, podejmowane z naruszeniem istniejącego prawa w celu wymuszenia od władz państwowych i społeczeństwa określonych zachowań i świadczeń, często naruszające dobra osób postronnych; działania te są realizowane z całą bezwzględnością, za pomocą różnych środków (nacisk psychiczny, przemoc fizyczna, użycie broni i ładunków wybuchowych), w warunkach specjalnie nadanego im rozgłosu i celowo wytworzonego w społeczeństwie lęku"[35], natomiast wojna hybrydowa stanowi mieszankę metod klasycznie militarnych, przede wszystkim nieregularnych (niekonwencjonalnych) działań zbrojnych (partyzantka, sabotaż, dywersja, akty terrorystyczne), ale zawiera też elementy

[33] https://www.abw.gov.pl/download/1/1925/skoneczny.pdf, s. 46, dostęp: 20.12.2020 r.
[34] W. Smolski, *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państw*, [w:] P. Fiktus, H. Malewski, M. Marszał (red.), *Rodzinna Europa. Europejska myśl polityczno-prawna u progu XXI wieku*, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2015, s. 481.
[35] https://encyklopedia.pwn.pl/haslo/terroryzm;3986796.html, dostęp: 20.12.2020 r.

walki informacyjnej (propaganda, dezinformacja), ekonomicznej oraz cybernetycznej. W tym sensie jest znacznie bardziej złożoną, wielowymiarową i wielosektorową następczynią wojny asymetrycznej, która może być prowadzona nie tylko przez dane państwo lub blok państw, lecz także przez organizacje pozapaństwowe, szczególnie terrorystyczne, takie jak Daesh[36]. Powyższe definicje są najbardziej obrazowe, bo wskazują na różnice i podobieństwa, a także definiują części wspólne terroryzmu i wojny hybrydowej, ponieważ często te formy walki interferują.

Dezinformacja w działaniach asymetrycznych stosowanych przez terrorystów jest skutecznym narzędziem walki i pozyskania zwolenników. Służy też manipulacji i odwróceniu uwagi od faktycznych zamiarów i dążeń. Dużą niewiadomą i obiekt wielu teorii spiskowych stanowi wsparcie ISIS przez Rosję. Nigdy nie było na to oczywistych dowodów, tak jak w przypadku niemalże oficjalnego wsparcia ze strony Kataru, Arabii Saudyjskiej czy nawet USA. Są jednak ślady w danych wywiadów o infiltrowaniu środowiska „dżihadystów". W 2016 r. prezydent Czeczenii, Ramzan Kadyrow nieoczekiwanie przyznał, że w szeregach ISIS służą „czeczeńskie siły specjalne". Prezydent Kadyrow oświadczył również o utworzeniu rozbudowanej sieci agentów w strukturach ISIS, gdzie wysłano elitę jego jednostek. Zadaniem czeczeńskich siły specjalnych jest gromadzenie danych o strukturach, potencjale terrorystów, wskazywaniu celów ataku i ocena ich skuteczności. Zdaniem znawców tematu występują dwa powody takiego działania. Po pierwsze Czeczeni stanowiący istotną część bojowników ISIS, po powrocie do kraju będą poważnym zagrożeniem dla interesów Rosji i Kadyrowa. Po drugie, Rosja prowadziła wielostopniową dezinformację w strukturach ISIS, jak i działać na niekorzyść USA oraz jej sojuszników[37].

Określenie działań dezinformacyjnych poniżej progu wojny

Agresja poniżej progu wojny (agresja podprogowa) to „działania wojenne, których rozmach i skala są celowo ograniczane i utrzymywane przez agresora na poziomie poniżej dającego się w miarę jednoznacznie zidentyfikować progu regularnej, otwartej wojny. Celem agresji podprogowej, jest osiąganie przyjętych celów z jednoczesnym powodowaniem trudności w uzyskaniu konsensusu decyzyjnego w międzynarodowych organizacjach bezpieczeństwa"[38].

Każdy konflikt może mieć kilka faz, co zależy od jego rodzaju oraz tła. Bezsprzecznym jest to, że konflikty międzynarodowe na skalę kontynentalną, a nawet lokalną rzadko wybuchną niespodziewanie. Narastaniu konfliktu towarzyszy wiele symptomów. Bardziej prawdopodobnym jest to, że konflikt będzie eskalował powoli– a wraz z nim będzie się zmieniać sytuacja międzynawowa. Użyte adekwatne środki polityczne oraz ekonomiczne doprowadzą do jego eskalacji, przygaszenia lub

[36] D. Niedzielski, *Zagrożenia hybrydowe. Podstawowe informacje i zdolności Sił Zbrojnych RP*, „Kwartalnik Bellona", nr 2/2016, s. 37.
[37] P. Mazur, M. Targ. *Geopolityczne i ekonomiczne korzyści zaangażowania się Rosji w konflikt syryjski*, „Przegląd Geopolityczny", nr 25/2018, s. 126.
[38] hhtps://www.bbn.gov.pl/pl/wydarzenia/6671,Juz-jutro-konferencja-BBN-i-AON-nt-zagrozenhybrydowych.html, dostęp 01.01.2021 r.

całkowitego zażegnania sporu. Pierwszą zdefiniowaną fazą jest sprzeczność interesów, bazującą zwykle na przesłankach historycznych lub obecnych działaniach rządów. Jej rozwiązywaniu służy zwykle mediacja i polityka zagraniczna. Drugą fazą są zazwyczaj spory, powstające, wówczas, kiedy zewnętrzne lub wewnętrzne napięcia będące spowodowane konfliktem interesów wymkną się spod kontroli i nadzoru mediatorów i obserwatorów, a wówczas dochodzi do retorsji drugiej strony. To jest faza ostrzegawcza. Wtedy państwo lub sojusz państw, stosując adekwatne ich zdaniem środki, mogą przyczynić się wzrostu napięć międzynarodowych i doprowadzić do sytuacji zagrożenia porządku, stabilizacji i pokoju. Trzecią fazą jest kryzys, powstający zwykle wówczas, kiedy strony sporu w celu osiągnięcia swoich rozbieżnych interesów, stosują narzędzia i środki w postaci embarga celnego, izolacji ekonomicznej, protekcjonizmu politycznego, a nawet posuwają się do demonstracji siły militarnej oraz groźby interwencji zbrojnej. Następną fazą jest konfrontacja, która nie jest jeszcze jednoznaczna z rozpoczęciem wojny. Nadal możliwy jest kompromis, na przykład, kiedy dojdzie do ugody lub jedna ze stron ugnie się naciskom lub da się przekonać mediacjom. Do otwartej wojny w fazie konfrontacji dochodzi wówczas, kiedy zawiodą wszelkie środki zaradcze, a sytuacja wejdzie w tryb niekontrolowanej inercji. Ostatnią fazą jest zazwyczaj pokojowe uregulowanie konfliktu. Zazwyczaj strona trzecia (mediator) ma decydujący wpływ na zakończenie konfliktu[39]. Agresja poniżej progu wojny jest stosowana zazwyczaj w drugiej, trzeciej i czwartej fazie potencjalnego konfliktu. Dezinformacja służy tu do deformacji niewygodnych faktów, pozyskaniu sojuszu, protekcji oraz pośrednio zdobyciu zaufania, bądź uzasadnienia własnych działań.

Utworzenie wojsk obrony cyberprzestrzeni

Niezbędność utworzenia Wojsk Obrony Cyberprzestrzeni podkreślił Piotr Dela w „Teorii walki w cyberprzestrzeni". Uważa, że niezbędna jest implementacja dowództwa, które będzie na równi z innymi rodzajami sił zbrojnych[40]. Stworzył on swoją propozycję struktury takiego dowództwa oraz wskazał możliwość stworzenia cyberbroni, która ma być zaprojektowana typowo do wyrządzania szkód[41].

Dyrektor Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni generał brygady Karol Molenda na posiedzeniu Komisji Obrony Narodowej oświadczył, że Wojska Obrony Cyberprzestrzeni osiągną pełną gotowość operacyjną w 2025 roku[42]. Jest to bardzo ważne, w kontekście budowania nowych zdolności SZ RP do działań zaczepnych i obronnych w cyberprzestrzeni. Niezbędnym krokiem w stronę implementacji nowego rodzaju sił zbrojnych jest pozyskanie wykwalifikowanej kadry oraz zespołów. Większość z nich jest już w szeregach armii. Służą oni jednak w różnych jednostkach, posiadających inną specyfikę niż ich specjalizacja.

---

[39] https://rsawl.awl.edu.pl/images/Archiwum/2011/nr_2/10justyna_szkola.pdf, dostęp: 13.01.2021 r.
[40] P. Dela, *Teoria walki…*, dz. cyt., s. 133.
[41] Tamże.
[42] https://www.cyberdefence24.pl/dyrektor-ncbc-wojska-obrony-cyberprzestrzeni-z-pelna-zdolnosciaoperacyjna-do-2025, dostęp 17.01.2021 r.

Program Cyber.mil ministerstwa obrony narodowej

Ministerstwo Obrony Narodowej, świadome zagrożeń związanych ze wzrostem brutalnych działań w cyberprzestrzeni, skierowanych w najważniejsze instytucje państwowe oraz społeczeństwo cywilne, wprowadziło specjalny program o nazwie CYBER.MIL. Ta strategia daje możliwość kształcenia oraz nabierania świadomości młodych osób w zakresie całego cyberbezpieczeństwa. Uczniowie między innymi zdobywają wiedzę w obszarze technicznym, uczą się kryptografii, jej genezy oraz operowania bezpieczeństwem danych i informacji, zarządzają ryzykiem. Zajęcia przeprowadzane są zasadą wiązania teorii z praktyką[43]. Program kierowany jest dla młodzieży licealnej oraz uczących się w technikach. Na oficjalnej stronie CYBER.MIL podkreślone zostało, że współczesne działania i konflikty przybierają charakteru hybrydowego, a cyberataki stanowią znaczący element[44].

Bazując na Zarządzeniu Ministra Obrony Narodowej w sprawie wdrożenia „Programu CYBER.MIL z klasą, koncepcja ta jest rozwojowym, prognostycznym projektem, który w przyszłości z pewnością posłuży się do nabycia wykwalifikowanych specjalistów z zakresu cyberbezpieczeństwa. Osoby, które po jego ukończeniu zdecydują się na wstąpienie do szkół oficerskich stanowić będą podstawę przyszłych Wojsk Obrony Cyberprzestrzeni. Podsumowując, program ten jest przełomowym krokiem w przód. Został opracowany dla ambitnych uczniów z umysłami ścisłymi oraz ma postawionych wiele wymogów, przez co tylko wyróżnione jednostki będą miały możliwość współpracy ze specjalistami z różnych dziedzin, poznania wielu ciekawych person oraz skrupulatnej perspektywy nauki wśród najlepszych.

Rola służb specjalnych w działaniach dezinformacyjnych

Obowiązek zwalczania dezinformacji oraz wykonywania działań dezinformacyjnych przypisuje się służbom specjalnym (wywiadowi oraz kontrwywiadowi). Bezdyskusyjny jest fakt, że większość operacji oraz działań służb specjalnych jest tajna. Są to operacje propagandowe, polityczne, militarne, logistyczne, techniczne oraz finansowe wspieranie ugrupowań (często opozycyjnych)[45]. Do zadań wywiadu i kontrwywiadu należy również zwalczanie nielegalnych motywów, które zagrażają bezpieczeństwu swojego państwa w tym zagranicznych grup przestępczych, terrorystów. Ich celem nie jest gromadzenie informacji, lecz realizacja celów polityki zagranicznej i obronności państwa[46].

Doktryna o operacjach informacyjnych ministerstwa obrony narodowej

Rola informacji (dezinformacji) jest również dostrzegana przez Ministerstwo Obrony Narodowej. W Centrum Doktryn i Szkolenia Sił Zbrojnych

[43] https://www.gov.pl/web/obrona-narodowa/rusza-cybermil-z-klasa, dostęp: 13.01.2021 r.
[44] https://www.cyber.mil.pl/misja-i-wizja/, dostęp: 13.01.2021 r.
[45] M. Minkina, B. Gałek, *Gry wywiadów. Kłamstwo i podstęp we współczesnym świecie*, Oficyna Wydawnicza RYTM, Warszawa 2015, s. 36.
[46] Tamże.

opracowano instrukcję pt. Operacje Informacyjne DD-3.10(A), na podstawie, której sekcje (wydziały) InfOps (ang. *information operations*) planują skoordynowane działania[47].

W doktrynie podkreślono, że operacje informacyjne prowadzone są samoczynnie, ale także równolegle z militarnymi. W trakcie konfliktów ogromną rolę odrywają media, kształtują one postawy obywateli oraz motywują ich do określonych działań. Głównym zagrożeniem w walce informacyjnej jest silne oddziaływanie na czołowe podmioty państwa, szczególnie w momentach podejmowania decyzji.

Proces działań informacyjnych został przedstawiony jako złożony proces. Polega on na tym, że na początku należy je dokładnie przeanalizować, zaplanować, zintegrować a następnie ocenić. Po stworzeniu planu działania należy go wdrożyć wzmacniając lub osłabiając dane rodzaje zachowań przeciwnika. Pożądanymi efektami będą: dokonanie rozłamu społeczeństwa popierającego od ich panujących przywódców oraz wpływanie na sojuszników przeciwnika. Podczas działań należy pamiętać o stałej ochronie swoich zdolności. W całym procesie decyzyjnym istotne jest poprawne postrzeganie i interpretowanie sytuacji ze względu na możliwości przewidywania zdarzeń oraz manipulacja tym czynnikiem u przeciwnika. Przy prowadzeniu takich działań trzeba uwzględnić swoje zdolności, a zdolności przeciwnika osłabić lub zniszczyć. Takimi zdolnościami jest to, co pozwala przeciwnikowi na efektowne zrozumienie sytuacji oraz zgodne z zamiarem dowodzenie wojskami[48].

Opisana doktryna jest najważniejszym dokumentem, którym przedstawione są działania informacyjne Sił Zbrojnych Rzeczypospolitej Polskiej. Opisuje ona oraz ustala zakres operacji i działań informacyjnych.

Metodologia

Praca została napisana na podstawie dokładnej analizy materiałów zwartych, artykułów naukowych oraz rzetelnych stron internetowych. Analizując źródła dokonano sprawdzenia wiarygodności stron internetowych oraz autorów publikacji naukowych. Praca powstała etapami - zgodnie z rozpisanym harmonogramem działania. Początkowo określono cel, czyli umiejscowienie dezinformacji wśród działań będących składową wojny hybrydowej, uporządkowanie aparatu pojęciowego oraz przedstawienie działań podejmowanych przez organy państwowe w celu minimalizacji zagrożeń. Następnie postawiono problem badawczy: *czy dezinformacja stanowi jeden z najbardziej niebezpiecznych działań wojny hybrydowej?* oraz hipotezę zakładającą, że zjawisko dezinformacji jest coraz bardziej powszechne i ma za sobą ogromne znaczenie w wojnie hybrydowej.

Przegląd literatury

Pracę napisano głównie w oparciu o materiały krajowe, a mianowicie książki, artykuły naukowe, strony internetowe oraz dokument normatywny. Zakres

[47] Operacje informacyjne, DD-3.10(A), Ministerstwo Obrony Narodowej, Centrum Doktryn i Szkolenia Sił Zbrojnych, Bydgoszcz 2017.
[48] Tamże, s. 16-17.

informacji zawiera zarówno starsze dane jak i dotychczasowe osiągnięcia. Na podstawie zebranych danych dokładnie opisano umiejscowienie dezinformacji w wojnie hybrydowej, podano rodzaje, przykłady dezinformacji oraz ocenę zagrożenia przez polskie podmioty.

Wnioski

Zjawisko dezinformacji jest coraz powszechniejsze. Bezustannie rozwijające się portale społecznościowe oraz media sprzyjają działaniom dezinformacyjnym, które są wykorzystywane w znacznej większości współczesnych konfliktów. Działania te, stają się coraz częstszym problemem badawczym wielu artykułów naukowych oraz są stale regulowane przez prawo. Wiele instytucji oraz organów państwowych regularnie wprowadza nowe kodeksy, doktryny, regulacje. Sam proces rozpowszechniania dezinformacji jest bardzo złożony, składa się z wielu czynników, w tym działań psychologicznych. Jej użycie może wpłynąć na pojedynczą jednostkę, grupę, państwo oraz na całą arenę międzynarodową. Celem pracy było przeanalizowanie działań dezinformacyjnych w wojnie hybrydowej. Na podstawie współczesnych konfliktów zbrojnych oraz działań dezinformacyjnych można bezsprzecznie stwierdzić, że jest ona jej częścią.

Bibliografia

Opracowania zwarte

1. Aleksandrowicz T.R., *Podstawy walki informacyjnej*, Editions Spotkania, Warszawa 2016.
2. Banasik M., *Wojna hybrydowa i jej konsekwencje dla bezpieczeństwa euro atlantydzkiego*, Wydawnictwo Difin, Warszawa 2018.
3. Dela P., *Teoria walki w cyberprzestrzeni*, Akademia Sztuki Wojennej, Warszawa 2020.
4. Denysiuk I., Osypowicz M., *Współczesne oblicze konfliktów zbrojnych – nowe zjawisko a kontynuacja nurtu działań partyzanckich*, Oficyna Wydawnicza ASPRA-JR, Siedlce 2018.
5. Minkina M., Gałek B., *Gry wywiadów. Kłamstwo i podstęp we* współczesnym *świecie*, Oficyna Wydawnicza RYTM, Warszawa 2015.
6. Żebrowski A., *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2016.

Artykuły

1. Mazur P., Targ M., *Geopolityczne i ekonomiczne korzyści zaangażowania się Rosji w konflikt syryjski*, „Przegląd Geopolityczny", nr 25/2018.
2. Niedzielski, *Zagrożenia hybrydowe. Podstawowe informacje i zdolności Sił Zbrojnych RP*, „Kwartalnik Bellona", nr 2/2016.

Źródła internetowe

1. https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbnpropozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html, dostęp: 20.12.2020 r.
2. https://repozytorium.ukw.edu.pl/bitstream/handle/item/4197/Proba%20wyjasnienia%20pojecia%20i%2 0istoty%20wojen%20hybrydowych.pdf?sequence=1&isAllowed=y, dostęp: 11.12.2020 r.
3. https://www.defence24.pl/wojska-specjalne-a-zagrozenia-hybrydowe-cz-1-czym-tak-naprawde-jest-wojna-hybrydowa-raport, dostęp: 02.01.2021 r.
4. https://www.ce.uw.edu.pl/pliki/pw/4-2015_hajduk.pdf, dostęp: 11.12.2020 r.
5. hhtps://www.bbn.gov.pl/pl/wydarzenia/6671,Juz-jutro-konferencja-BBN-i-AON-nt-zagrozenhybrydowych.html, dostęp: 01.01.2021 r.
6. https://encyklopedia.pwn.pl/haslo/terroryzm;3986796.html, dostęp: 20.12.2020 r.
7. https://sjp.pwn.pl/sjp/dezinformacja;2554971.html, dostęp: 07.12.2020 r.
8. https://www.app.college.police.uk/app-content/information-management/management-of-police-information/collection-and-recording/, dostęp: 11.12.2020 r.
9. https://www.cyberdefence24.pl/dyrektor-ncbc-wojska-obrony-cyberprzestrzeni-z-pelna-zdolnosciaoperacyjna-do-2025, dostęp: 17.01.2021 r.
10. https://www.gov.pl/web/obrona-narodowa/rusza-cybermil-z-klasa, dostęp: 13.01.2021 r.
11. https://studiadesecuritate.up.krakow.pl/wp-content/uploads/sites/43/2018/10/DanutaKa%C5%BAmierczak-Walka-informacyjna-we-wsp%C3%B3%C5%82czesnych-konfliktach-i-jejspo%C5%82eczne-konsekwencje.pdf, dostęp: 13.01.2021 r.
12. http://www.autonom.edu.pl/publikacje/kossecki_jozef/elementy_wojny_informacyjnej-ocr.pdf, dostęp: 11.12.2020 r.
13. https://www.znak.com.pl/ksiazka/wspolczesne-konflikty-zbrojne-los-robert-reginia-zacharski-jacek44116, dostęp: 30.12.2020 r.
14. https://www.abw.gov.pl/download/1/1925/skoneczny.pdf, dostęp: 20.12.2020 r.
15. https://graduacja.lazarski.pl/fileadmin/user_upload/dokumenty/student/Sun_Tzu_sztuka_wojny.pdf, dostęp: 30.12.2020 r.
16. https://rsawl.awl.edu.pl/images/Archiwum/2011/nr_2/10justyna_szkola.pdf, dostęp: 13.01.2021 r.
17. http://wiedzaobronna.edu.pl/index.php/wo/article/view/39/39, dostęp: 12.12.2020 r.
18. https://socjocybernetyka.files.wordpress.com/2010/08/totalna-wojna-informacyjna.pdf, dostęp: 11.12.2020 r.
19. https://www.cyber.mil.pl/misja-i-wizja/, dostęp: 13.01.2021 r.
20. http://www.abw.gov.pl/download/1/2170/TomaszRAleksandrowicz.pdf, dostęp: 20.12.2020 r.

21. https://rsawl.awl.edu.pl/images/Archiwum/2011/nr_2/10justyna_szkola.pdf, dostęp: 13.01.2021 r.

Dokumenty normatywne

1. DD 3.10(A) Operacje informacyjne, Ministerstwo Obrony Narodowej, Centrum Doktryn i Szkolenia Sił Zbrojnych, Bydgoszcz 2017.

bsmt pchor. Manuela CHAMERA

SOCJOTECHNIKA A CYBERPRZESTĘPCZOŚĆ NA WYBRANYCH PRZYKŁADACH

Streszczenie

Socjotechnika w głównej mierze opiera się na manipulacji przy pomocy takich elementów jak atrakcyjność, wywieranie sympatii w rozmówcy czy umiejętności komunikacyjne. Pozornie przeciętny człowiek nie dostrzegłby powiązania socjotechnika, czyli osoby korzystającej z tych metod z cyberprzestępczością. Spowodowane jest to stereotypowym obrazem hakera jako antyspołecznej otyłej osoby w okularach siedzącej głównie w swoim pokoju. Cyberprzestępcy nie rzadko korzystają z inżynierii społecznej by zwieść ofiarę, nie musi jednak to być kontakt „face to face", a przykładowo rozmowa telefoniczna, czy tak skonstruowany e-mail aby odbiorca go otworzył jednocześnie nieświadomie infekując swoje urządzenie. Istnieją jednak sposoby, by zwiększyć swoje bezpieczeństwo i uchronić się przed takimi atakami. W tym celu jednak należy poznać podstawy tego zagadnienia i zrozumieć, w jaki sposób działają takie osoby. Rezultatem niniejszej pracy jest przedstawienie korelacji pomiędzy zjawiskami takimi jak socjotechnika i cyberprzestępczość.

Słowa kluczowe:
cyberprzestępczość, socjotechnika, przestępstwo, cyberprzestrzeń, cyberbezpieczeństwo, inżynieria społeczna, phishing, vishing, smishing, test penetracyjny.

Abstract

Social engineering and cybercrime on selected examples

Social engineering mainly depends on manipulation using attraction, making sympathy or even social skills. A seemingly average person would not see any relations between social engineer and cyber security. Due to stereotypical hacker image as antisocial obese person in glasses which is only sitting in front of PC in his room. Cyber criminals are often using social engineering to lure their victims. It does not have to be a face-to-face contact, but it can be done by simple cellphone call, or even a mail which will infect his device when it opened. There are ways to improve our safety and protect ourselves from such attacks. To do this however, you need to know the basics of this issue and understand how such people work. The main goal of this article was to present the objective, which was presenting the correlation between phenomena such as social engineering and cybercrime.

Keywords:
cybercrime, social engineering, crime, cyberspace, cybersecurity, phishing, vishing, smishing, penetration testing.

Wstęp

W dobie XXI wieku zaawansowana technologia spotykana jest na każdym kroku. Obecna jest ona w telefonach, telewizorach, w inteligentnych lodówkach, samochodach mówiąc w skrócie wszędzie. Technologia wiąże się z urządzeniami, a więc pociąga za sobą konsekwencję w postaci możliwości włamania do każdego z nich.

Naukowe odkrycia związane z technologią bezustannie się rozwijają znacznie powiększając swój zakres. Nieustanne śledzenie nowych rozwiązań nie jest prostym zadaniem dla osób niezajmujących się tym tematem zawodowo bądź nawet hobbystycznie. Starsze społeczeństwo nie jest tak obeznane w technologii jak młodsze jego wydanie, które w większości i tak nie jest w stanie posiadać tak rozległej wiedzy na temat ataków hakerskich. Obecnie przestępcy zdobywają coraz większe pole do popisu, które wykorzystują.

Dawniej przestępstwo ograniczało się między innymi do zwykłej fizycznej kradzieży czy oszustwa. W następstwie wejścia w życie komputerów, Internetu zaczęło się hakerstwo. Początkowo było ono drobne jednak w miarę upływu czasu zaczęło być coraz to poważniejsze jak i sprytniejsze. Obecnie jesteśmy jednak na etapie wysoko zaawansowanych kodów, podstępów we włamywaniu się do firm bądź zmyślnego nakłonienia do kliknięcia w zainfekowany dokument lub hiperłącze.

Podstawowe pojęcia z zakresu cyberprzestępczości

Przestępstwo jest czynem człowieka, czynem zabronionym przez Polski Kodeks Karny. W ustawie tej nie została ujęta konkretna definicja pojęcia przestępstwo, czyli sensu stricto „Przestępstwo jest to …”[1]. Można ją jednak skonstruować z art. 1, 2, 3, 7 i 9, a mianowicie jest to czyn zabroniony pod groźbą kary przez prawomocny dokument programowy, którego szkodliwość społeczna musi być w wyższym stopniu niż znikoma, jest bezprawny i zawiniony. Istotnym jest również fakt, że aby ponieść karę, wina musi być przypisana w chwili popełnienia czynu. Art. 7 określa przestępstwo jako zbrodnię lub występek, określając w następnej kolejności różnice pomiędzy tymi dwoma terminami[2].

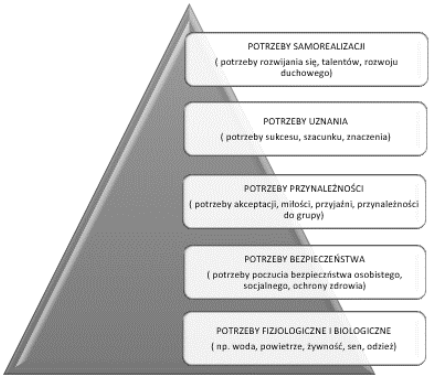
Cyberprzestrzeń jest to przestrzeń przetwarzania i wymiany informacji, która tworzona jest przez systemy teleinformatyczne wraz z powiązaniami między nimi oraz relacjami z użytkownikami[3]. Definicja ta przejdzie jednak zapewne wiele zmian na przestrzeni następnych lat.

[1] L. Gardocki, *Pojęcie przestępstwa i podziały przestępstw w polskim prawie karnym*, Lublin 2013, s. 29.
[2] Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny.
[3] Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. z 2011 nr 222, poz. 1323).

Przekładając, cyberprzestrzeń jest to przestrzeń wirtualna. Termin ten używany jest by określić połączenie o charakterze wirtualnym, utworzonym i funkcjonującym na podstawie jej fizycznej formy, czyli komputerów i infrastruktury telekomunikacyjnej. Jej podstawowym elementem jest sieć Internet, jednak równie ważne są urządzenia teleinformatyczne i połączenia między nimi.

W cyberprzestrzeni odbywa się bezustanna wymiana danych i komunikacja, a wszystkie te dane są gromadzone i przechowywane. To, co w teorii zostało usunięte w rzeczywistości wciąż można je tam znaleźć, jeśli tylko posiada się odpowiednią wiedzę i umiejętności. Za jej pośrednictwem możliwe jest również w prosty sposób wprowadzenia paniki wśród społeczności internetowej, a dokładnie za pomocą dezinformacji. Część informacji znajdujących się w Internecie jest weryfikowana, jednak kontrolowanie tego na bieżąco jest niemożliwa stąd też większa część danych nie jest sprawdzana i może zawierać fałszywe informacje.

Punkt odniesienia w pojęciu cyberbezpieczeństwo stanowi słowo bezpieczeństwo. Amerykański psycholog, Abraham Maslow, w 1943 r. opracował tzw. piramidę potrzeb, której nazwa wzięła się od hierarchicznego uporządkowania potrzeb człowieka[4]. Graficznie piramidę potrzeb wg Masłowa przedstawiono na rysunku 2.1. Człowiek potrzebuje wszystkich wymienionych przez niego elementów do prawidłowego funkcjonowania. Ich brak ma ogromny wpływ na postrzeganie świata jak i podejście do niego, a także elementy te oddziałują na podejście do siebie samego.



Źródło: opracowanie własne na podstawie książki A. Maslow, *Motywacja i osobowość*, IW PAX, Warszawa 1990.

Rysunek 2.1. Piramida potrzeb wg Maslowa

Według Maslowa bezpieczeństwo jest drugą najważniejszą potrzebą człowieka, gdyż pierwszą są potrzeby fizjologiczne i biologiczne. Potrzeba ta

[4] A. Maslow, *Motywacja i osobowość*, IW PAX, Warszawa 1990, s. 76.

polega na poczuciu spokoju, pewności i opieki. Mowa tu również o posiadaniu pracy, stabilności finansowej, ochronie zdrowia i o ogólnym poczuciu braku zagrożenia.

Człowiek potrzebuje poczucia bezpieczeństwa, nie tylko w rzeczywistym życiu, ale i w obszarach niematerialnych, po których się porusza. W cyberprzestrzeni ludzie spędzają ogromne ilości czasu, logują się na rozmaite strony i podają różne dane, pozostawiając przy tym ślad swojej obecności. Z natury ludzie są ufnymi istotami[5], dopiero z czasem stają się bardziej świadomi niebezpieczeństw czyhających na „naiwne owieczki". Wiele jednak zależy od ich doświadczeń. Jednak bez odpowiedniej wiedzy nie są w stanie poruszać się bezpiecznie po Internecie.

Pojawienie się przestępców internetowych jest oczywistą koleją rzeczy, początkowo jednak posiadali poczucie bezpieczeństwa w cyberświecie. Uważali, że nikt ich nie wytropi i będą mogli przykładowo dokonywać coraz większych oszustw, kradzieży, jak i poszukiwań sposobu na dokonanie zemsty.

Dość naturalnie najpierw w nieformalnym znaczeniu i następnie w formalnym pojawiły się takie terminy jak cyberprzestępca czy cyberbezpieczeństwo. Według ustawy cyberbezpieczeństwo jest to odporność systemów informacyjnych na działania naruszające 4 podstawowe cechy: poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[6].

Cyberprzestępczość można określić jako nielegalne działania, które popełniane są za pomocą technik komputerowych lub dotyczące systemów lub sieci komputerowych, czyli mowa tu o elementach specyficznych dla cyberprzestrzeni. Przestępcy stosują różne techniki, metody i narzędzia, takie jak wyłudzanie danych, wirusy, oprogramowanie typu spyware lub ransomware oraz metody socjotechniczne. Ich celem często jest kradzież danych osobowych lub oszustwo.

Klasyfikacja ataków w cyberprzestrzeni

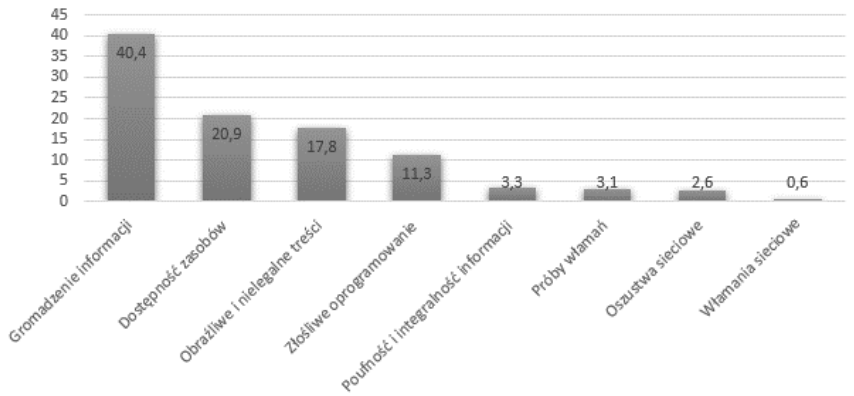
CERT Orange Polska jest to specjalistyczna jednostka, której celem jest zapewnienie bezpieczeństwa użytkownikom Internetu. Jednostka ta pomaga i stara się uświadomić społeczeństwu o czyhającym zagrożeniu w cyberprzestrzeni. Od 2014 r. publikuje raporty, w których opisywane są zestawienia różnego rodzaju ataków, sposoby obrony i nie tylko.

W 2015 r. CERT Orange Polska zaproponował następującą klasyfikację incydentów:

[5] E. Lucas, *Oswoić cyberświat Tożsamość, zaufanie i bezpieczeństwo w Internecie*, Kurhaus Publishing, Warszawa 2017, s. 23.
[6] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).

- obraźliwe i nielegalne treści (np. SPAM, piractwo i plagiat, pornografia dziecięca, groźby);
- złośliwe oprogramowanie (np. hostowanie C&C, wiadomość ze złośliwym oprogramowaniem);
- gromadzenie informacji (np. podsłuch, phishing, skanowanie portów);
- próby włamań (np. nieuprawnione logowanie, wykorzystanie podatności w celu zakłócenia funkcjonowania usług);
- włamania sieciowe (np. nieautoryzowany dostęp do systemu, poprzez wykorzystanie podatności);
- dostępność zasobów (np. ataki typu DDoS);
- poufność i integralność informacji (np. przechwycenie, udostępnienie zbioru informacji, zniszczenie lub zmodyfikowanie danych);
- oszustwa sieciowe (np. użycie zasobów sieciowych niezgodne z ich przeznaczeniem, nieuprawnione użycie nazwy organizacji bądź jej zasobów);
- inne (takie, które nie zaliczają się do żądnej z powyższych kategorii)[7].

Procentowe występowanie incydentów w CERT Orange Polska w 2019 roku przedstawia rysunek 2.2.



Źródło: Opracowanie własne na podstawie https://www.cert.orange.pl/raporty-cert, dostęp: 10.12.2020 r.

Rysunek 2.2. Procentowe występowanie incydentów w CERT Orange Polska w 2019 roku

[7] https://www.cert.orange.pl/raporty-cert, dostęp: 10.12.2020 r.

W cyberprzestrzeni jest wiele zagrożeń, a jeden z częściej spotykanych to malware. Pojęcie to oznacza w szerokim tego słowa znaczeniu oprogramowanie, którego celem jest szkodliwe działanie na urządzeniu ofiary bez jej zgody i wiedzy[8].

Malware jest w stanie uzyskać zdalną władzę nad systemem informatycznym, może wyłączyć system bezpieczeństwa, rejestrować i wysyłać dane do osób nieuprawnionych. Zagraża on integralności, poufności jak i dostępności informacji[9].

Znaleźć go można w mailach, zainfekowanych stronach internetowych m.in. przez zaakceptowanie regulaminu strony, w ściąganych plikach, grach, pirackich programach. Czasem wystarczy tylko jedno nieprzemyślane kliknięcie myszką, aby malware znalazł się natychmiast na urządzeniu.

Wśród rodzajów malware wyróżnić można:

- Wirus, jest to złośliwy kod lub fragment kodu, którego główną cechą jest konieczność posiadania nosiciela w odróżnieniu do robaka komputerowego, który rozprzestrzenia się samoistnie poprzez wyszukanie luk systemowych bądź wykorzystanie naiwności ofiary. Wirus może przykładowo wyświetlać coś na monitorze, usuwać pliki, dokonywać zmian jak i formatować dysk. Robak natomiast jest w stanie przykładowo przesyłać spam, usuwać pliku jak i pełnić rolę konia trojańskiego lub backdoor[10].
- Trojan, zwany jest również koniem trojańskim, jest to szkodliwy program, który udaje potrzebną aplikację lub oprogramowanie jednak nie posiada funkcji samoistnego rozmnażania się. Jest jednak w stanie przykładowo uszkodzić sprzęt i dane, wgrać wirusy jak i doprowadzić do przejęcia kontroli nad systemem przez osoby nieuprawnione[11].
- Rootkit, jest to złośliwe oprogramowanie/zbiór narzędzi, które są w stanie ukryć swoją jak i obecność innego malware, może również wyłączyć antywirusa. Dodatkowo zapewnia hakerowi uprawnienia administracyjne[12].
- Keylogger, jest to niebezpieczne oprogramowanie, które sczytuje zapis naciśnięć z klawiatury i ruchów myszki. Wszystkie te dane są gromadzone w dzienniku. Mogą one być również selekcjonowane przykładowo poprzez monitorowanie konkretnych aplikacji i stron internetowych[13].

[8] https://www.cert.orange.pl/raporty-cert, dostęp: 10.12.2020 r.
[9] J. Kosiński, *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015, s. 93.
[10] https://trybawaryjny.pl/rodzaje-wirusow/, dostęp: 14.12.2020 r.
[11] https://www.netia.pl/pl/blog/malware-co-to-jest-jakie-zagrozenie-sprawia, dostęp: 14.12.2020 r.
[12] https://bitdefender.pl/co-to-jest-rootkit-oraz-jak-go-trwale-usunac-z-komputera/, dostęp: 15.12.2020 r.
[13] https://bitdefender.pl/abc-cyberbezpieczenstwa-k-jak-keylogger/, dostęp: 15.12.2020 r.

- Spyware, jest to szpiegujące oprogramowanie, które sczytuje dane na temat aktywności ofiary w Internecie, historii przeglądarki, zwyczajów użytkownika, poufne dane i in.[14].
- Ransomware, zwany jest oprogramowaniem szantażującym, gdyż zazwyczaj wykorzystywany jest do wymuszenia zapłaty okupu. Dochodzi do tego poprzez zablokowanie dostępu do urządzenia i zaszyfrowanie części bądź wszystkich danych jednocześnie wyświetlając komunikat o żądaniu zapłaty[15].

Kolejnym na liście popularnych zagrożeń jest atak typu **Denial-of-Service**, tłumacząc na język polski oznacza odmowę dostępu. Atak ten przeprowadzony jest z jednej maszyny i jego celem jest zaburzenie pracy atakowanego serwera, doprowadzając do sytuacji, w której dany serwer przestanie udzielać odpowiedzi na zapytania jak i możliwość łączenia się z nim będzie niemożliwa. Wyróżnia się kilka technik wykorzystywanych w celu wyłączenia serwera:

- ograniczenie wydajności;
- zużywanie zasobów;
- zawieszenie systemu;
- atakowanie poszczególnych warstw.

Przykładowo technika ograniczenia wydajności polega na wysyłaniu ogromnej ilości wiadomości, im wyższe zaawansowanie wysyłanych zapytań, tym serwer będzie potrzebował więcej czasu na poradzenie sobie z nimi. Serwer musi każdą z nich przetworzyć, dlatego też nie jest w stanie na bieżąco odpowiadać na prawdziwe wiadomości[16].

Jako równie popularne zagrożenie, a będące pochodną ataku typu DoS jest atak typu **Distributed Denial-of-Service**, czyli w tłumaczeniu dosłownym rozproszona odmowa usługi. Podobnie jak atak typu DoS polega na przesłaniu bardzo dużej liczby wiadomości do atakowanego systemu, jednak w DoS atak następował z jednego urządzenia natomiast w DDoS atak jest wykonywany z różnorakich maszyn, które nie znajdują się na jednej przestrzeni, a na wielu.

W celu przeprowadzenia ataku tego typu najpierw infekuje się maszynę ofiary wirusem, który daje przestępcy kontrolę nad tą maszyną, co oczywiście odbywa się bez wiedzy użytkownika. W stosunku do takich komputerów używa się określenia zombie, który za pomocą programu działającego w tle i na komendę hakera może stać się jednym z wielu elementów biorących udział przy ataku DDoS.

Tego typu atak jest o wiele trudniejszy do wykrycia z powodu wielu źródeł, których ilość można liczyć nawet w tysiącach, a lokalizacje mogą

[14] https://www.avast.com/pl-pl/c-spyware, dostęp: 18.12.2020 r.
[15] https://mks-vir.pl/virus/ransomware/, dostęp: 18.12.2020 r.
[16] http://www.crypto-it.net/pl/ataki/dos.html, dostęp: 18.12.2020 r.

wskazywać na różne państwa czy strony świata. Koszty takiego ataku są minimalne, gdyż przestępca musi tylko skonstruować odpowiedniego wirusa i następnie go rozprzestrzenić po środowisku wirtualnym[17].

Socjotechnika jako element ataków w cyberprzestrzeni

Termin socjotechnika posiada dwie składowe: technika i socjo, który pochodzi od łacińskiego słowa societas oznaczający społeczeństwo. W 1966 r. uważano ją, jako zbiór zaleceń, które nawiązują do umiejętności realizowania świadomego przeobrażenia społecznego po to, aby uzyskać zaplanowane cele[18]. Od tego czasu znaczenie to nie uległo wielkim zmianom, rozwinął się jednak zakres jego stosowania.

Kevin Mitnick termin ten określa jako zbiór metod, które służą do oddziaływania na ludzi, do czego wykorzystywana jest również perswazja. Stosowana jest w celu zwiedzenia potencjalnej ofiary, często kryjąc się za fałszywą tożsamością. To dzięki takim zabiegom socjotechnik jest w stanie umiejętnie manipulować ofiarą w taki sposób, aby nieświadomie podała wszystkie potrzebne mu informacje[19].

W celu skutecznej manipulacji wykorzystuje się pewne zabiegi, aby odpowiednio wpłynąć na osobę, która jest jej poddawana, a także w celu osiągnięcia założonych wcześniej efektów. Robert Cialdini po wielu badaniach wyodrębnił najczęściej stosowane zasady, którymi kierują się przestępcy i nie tylko oni, gdyż działania te można również dostrzec w reklamach, marketingu jak i w życiu codziennym[20].

Sześć reguł według Cialdiniego

Regułę wzajemności uważać można za nieodłączny element każdej społeczności. Opiera się ona na kurtuazji i poczuciu zobowiązania. Jeżeli ktoś mi pomógł to innym razem ja również powinienem pomóc tej osobie. Przestępca może ją wykorzystać poprzez oddanie przysługi „koledze z pracy" np. pomoże mu poprzez przepchnięcie jakiegoś dokumentu, a następnym razem już ten przestępca poprosi być może o dostęp do dokumentów, do których nie posiada uprawnień, bądź podłączenie pendrive w celu skopiowania czegoś. W teorii nawet, jeżeli ofiara zdaje sobie sprawę, że nie powinna tego robić to jednak w praktyce kieruje się myślą, że skoro on jej wcześniej pomógł to nie wypada mu teraz odmówić.

Reguła zaangażowania i konsekwencji opiera się na podświadomym dążeniu ludzi do bycia osobami konsekwentnymi w swych dążeniach, aby tak

[17] https://dataspace.pl/blog/dos-rodzaje-atakow-cz-1/, dostęp: 19.12.2020 r.
[18] A. Podgórecki, *Zasady socjotechniki*, Wiedza Powszechna, Warszawa 1966, s. 33.
[19] K. Mitnick, W. Simon, *Sztuka podstępu. Łamałem ludzi, nie hasła*, Helion, Gliwice 2002, s. 6.
[20] R. Cialdini, *Wywieranie wpływu na ludzi. Teoria i praktyka*, GWP Gdańskie Wydawnictwo Psychologiczne, Gdańsk 1984 r.

inni ich postrzegali. Hakerzy mogą tą zasadę wykorzystać przykładowo najpierw poprzez małe prośby, następnie przechodząc do następnych. Przykładowo, jeżeli poprosili daną osobę o wprowadzenie do firmy pod pretekstem, że są tu nowi i zapomnieli przepustki z biura, a ta osoba się zgodzi wtedy o wiele łatwiej przestępcy prosić o kolejną drobną przysługę. Ofierze natomiast z każdą kolejną prośbą jest coraz ciężej się wycofać, skoro zaangażował się już w pomoc.

Reguła społecznego dowodu słuszności jest powszechnie stosowana, szczególnie często spotkać ją można w reklamach jak i na wielu stronach internetowych. Opiera się ona na konformizmie, czyli tak zwanym podążaniu za tłumem. Firmy wykorzystują tą regułę poprzez stosowanie takich sloganów jak 98% konsumentów zarekomendowały ten produkt swojemu przyjacielowi lub odniosą się do konkretnej liczby. Przestępcy mogą wykorzystać tą regułę przykładowo poprzez dodanie do zamówienia w formie gratisu zainfekowane urządzenia typu USB pracownikom korporacji. Duże prawdopodobieństwo wskazuje na to, że jeżeli choć jedna osoba podłączy go do komputera to i reszta to zrobi.

Reguła lubienia i sympatii polega na tym, że zdecydowanie chętniej ludzie pomagają czy wyświadczają przysługę osobie, którą darzą sympatią. W przypadku osób, które rozmawiają ze sobą pierwszy raz wykorzystuje się manipulację atrakcyjnością i podobieństwem, a także komplementowanie i chwalenie[21]. Ta reguła doskonale współgra z regułą zaangażowania i konsekwencji. Opierając się na tamtym przykładzie ofiara chętniej pomoże temu tak zwanemu nowemu pracownikowi, który zapomniał przepustki, a który wzbudza ich sympatię, na podstawie wyglądu czy zachowania niż komuś, do kogo tej sympatii nie odczuwają.

Z regułą autorytetu każda osoba ma styczność od najmłodszych lat. Początkowo są to rodzice, których z reguły uważa się za osoby mądre, doświadczone, których decyzje na pewno są słuszne i prawidłowe. Następni są nauczyciele, profesorzy, przełożeni jak i lekarze czy prawnicy. Na każdym etapie życia można spotkać taki autorytet. Powszechnie uważa się, że lekarz w dziedzinie medycyny będzie miał rację, niż osoba, która nigdy medycyny nie studiowała. Przestępcy wykorzystują tą regułą przykładowo poprzez podawanie się za osobę na wysokim stanowisku w firmie pisząc maila bądź w trakcie rozmowy telefonicznej. W mailu ofiara proszona jest o szybką odpowiedź, sprawdzenie załącznika, a podczas rozmowy o podanie konkretnych danych potrzebnych przestępcy. Innymi osobami, za które mogą podać się przestępcy jest policjant, strażak jak i oficer.

Reguła niedostępności opiera się na powszechnej opinii, że to, co jest trudno dostępne bądź rzadkie to znaczy, że jest lepsze. Jeśli jest rzadkie to znaczy, że nie każdy może to mieć i przez to staje się bardziej wartościowe, a jeśli jest trudno dostępne to zapewne jest dobre, skoro ludzie to wykupują.

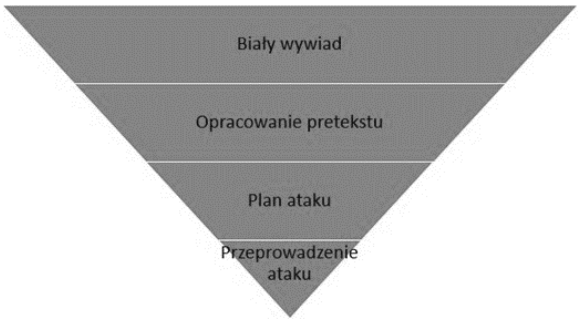
[21] http://perswazja.biz/szesc-regul-roberta-cialdiniego/, dostęp: 30.12.2020 r.

Przykładem marketingowym mogą być oferty „last minute", edycja limitowana jak i wyświetlający się komunikat: pospiesz się pozostał ostatni pokój do wynajęcia w naszym hotelu. Przestępcy wykorzystują ją często poprzez wysyłanie fałszywych maili informujących ofiarę, że wygrała jakąś nagrodę, a do jej odebrania wystarczy tylko wysłać sms z tym, że czas jest ograniczony.

Piramida Inżynierii Społecznej

Podobnie jak do wygłaszania prezentacji czy prowadzenia wykładów, do ataku z użyciem technik socjotechnicznych również należy się odpowiednio przygotować. Na podstawie obserwacji i dogłębnych analiz takich ataków Christopher Hadnagy opracował piramidę inżynierii społecznej zwaną również piramidą socjotechniki. Służy ona do zobrazowania działań socjotechnika, w jaki sposób przygotowuje się do ataku, a nawet przybliża jego sposób myślenia. Są to jednak ataki nienakierowane na masową skalę, a na konkretną organizację, firmę czy osobę prywatną. Piramidę inżynierii społecznej zobrazowuje rysunek 3.1.

U podstaw takich ataków leży biały wywiad. Jest on bardzo istotny, gdyż dzięki niemu atakujący zdobywa informacje na temat celu jak i jego otoczenia. To informacja przez cały proces przygotowań jak i realizacji ataku odgrywa najważniejszą rolę stąd też zajmuje najwięcej miejsca w piramidzie. Nie polega ten etap jednak na zdobywaniu przypadkowych danych, a na określeniu, jakie dokładnie informacje są potrzebne. Następnie dąży się do ich uzyskania za pomocą różnych dostępnych metod i je odpowiednio dokumentuje.



Źródło: opracowanie własne na podstawie C. Hadnagy, *Socjotechnika. Sztuka zdobywania władzy nad umysłami*, Helion, Gliwice 2020, s. 29.

Rysunek 3.1. Piramida Inżynierii społecznej

W socjotechnice pojęcie pretekst oznacza przykrywkę, czyli wcielanie się w kogoś innego. Niejednokrotnie polega na stworzeniu nowej tożsamości, aby osiągnąć zamierzony cel. Opracowanie pretekstu opiera się na właściwym przemyśleniu, jaka przykrywka najlepiej się sprawdzi w celu osiągnięcia celu. Nie musi to być jednak tylko jeden pretekst, a może być ich kilka. Przykładowo

w inny sposób przestępca może dostać się do firmy, a w jeszcze inny do konkretnego gabinetu. Socjotechnik może wcielić się w role deratyzatora, policjanta, osoby, która przyszła na rozmowę o pracę i wiele innych, możliwości ma nieskończenie wiele.

Następnym krokiem po opracowaniu pretekstu jest sporządzenie planu ataku. Istotne jest tutaj udzielenie odpowiedzi na trzy pytania:

- „co?", czyli co jest celem ataku, co chce za jego pomocą osiągnąć;
- „kiedy?", czyli kiedy powinien zostać przeprowadzony atak, jaki jest najlepszy czas na jego realizację;
- „kto?", czyli kto może być jeszcze potrzebny w czasie ataku, w razie, gdyby potrzebne było wsparcie[22].

Istotne jest, aby plan nie był skonstruowany zbyt szczegółowo, gdyż to zawęża pole do improwizacji, a także może sprawić, że przykładowa rozmowa nie jest naturalna. Powinien być zapisywany ogólnikowo bez konkretnych słów i działań. Po tym etapie występuje już tylko przeprowadzenie ataku.

Podstawowe typy ataków wykorzystujących inżynierię społeczną

Phishing jest najczęściej stosowanym atakiem socjotechnicznym i opiera się na wysyłaniu wiadomości email. W tych wiadomościach przestępca podszywa się pod jedną z zaufanych organizacji bądź osobę w celu zdobycia poufnych informacji. Mogą być to takie dane jak hasła i loginy do kont bankowych, jak i dane kart kredytowych.

W dużej mierze ich podstawą jest przekonanie ofiary, iż pilnie muszą wejść w podany link przykładowo z powodu zablokowania konta bądź potrzeby zmiany hasła, gdyż wykryto nieznaną próbę logowania. Oczywiście występują również wiadomości typu informujące o wygraniu konkursu, a w celu jej odebrania wystarczy wejść w podanego linka i podać swoje dane. Większość osób logicznie pomyśli, że nie brało udziału w żadnych konkursie czy losowaniu, jednak znajdzie się zawsze osoba, która z ciekawości wejdzie nie przypuszczając, że przez samo wejście w podany link zainfekuje swoje urządzenie

Podczas gdy człowiek zostaje poddany presji czasu o wiele łatwiej popełnia błędy. W przypadku fałszywego emaila błędy te polegają często na niesprawdzeniu źródła wiadomości jak i niedokładnym sprawdzeniu czy w adresie email nie znajdują się znaki tylko przypominające jakąś daną literkę lub liczbę, lub niezwróceniu uwagi na brak polskich znaków, co zasadniczo dość rzadko już się zdarza. Po przekierowaniu na określoną stronę internetową również ludzie często nie zwracają uwagi na drobne szczegóły, które sugerują, iż jest ona podrobiona. Jednym z tych szczegółów może być brak certyfikatu bezpieczeństwa bądź drobna zmiana w adresie URL.

[22] C. Hadnagy, *Socjotechnika. Sztuka zdobywania władzy nad umysłami*, Helion, Gliwice 2020, s. 35.

SMiShing opiera się na wiadomościach wysyłanych na telefon bądź komunikator typu WhatsApp. Ten rodzaj ataku jest znacznie rzadziej spotykany, jednak wciąż praktykowany przez socjotechników[23].

W tego typu wiadomości przestępcy najczęściej zachęcają, a raczej wymuszają zadzwonienie na podany numer telefonu lub na wejście w wyszczególniony link. Głównie ataki te nakierowane są na zdobycie danych do konta bankowego, czyli dokładnie jak w przypadku phishingu celem są poufne dane. W tego typu ataku problem stanowi niemożność sprawdzenia faktycznego wyglądu linku bez biegłej wiedzy na temat poruszania się po urządzeniu mobilnym w odróżnieniu od komputera, na którym wystarczy tylko najechać kursorem na podany link.

Treść takiej wiadomości zazwyczaj jest krótka, zwięzła i na temat. Nie ma tam miejsca na nawiązywanie relacji, czy nadmierne rozpisywanie się. Naturalnie jednak musi zawierać taką treść, aby nakłonić odbiorcę do natychmiastowego działania[24].

W przypadku wykonania połączenia na podany numer z reguły uruchamia się automatyczna sekretarka, która przykładowo prosi o takie dane jak login, hasło, kod PIN lub nawet numer karty płatniczej. Zdarzają się również ataki z wykorzystaniem prośby o przesłanie SMS- a, z którego kosztem klient nie zostaje zapoznany[25].

Vishing wykorzystywany znacznie częściej niż jeszcze kilka lat temu, co więcej, jest on bardzo skuteczną metodą. Pod względem celu nie różni się od phishingu czy smishingu, w dalszym ciągu jego przeznaczeniem jest uzyskanie poufnych danych[26].

Sposób wykorzystania vishingu można podzielić na dwa przypadki. Pierwszym jest wykorzystanie automatycznego systemu głosowego. Może do niego dojść poprzez wcześniejszy atak smishingowy, który nakłonił ofiarę do wykonania połączenia. Po dokonaniu połączenia załącza się automat, który prosi o podanie wszystkich potrzebnych danych w zależności, na czym opierała się wcześniejsza wiadomość tekstowa. Drugim sposobem jest niekorzystanie z automatów, a wykorzystanie faktycznej rozmowy. Często atak ten jest wykorzystywany w białym wywiadzie w celu weryfikacji posiadanych danych, jak i próby zdobycia innych istotnych z punktu widzenia ataku informacji. Innym jego zastosowanie jest oczywiście zdobycie przykładowo konkretnie danych uwierzytelniających.

W celu dokonania skutecznego ataku socjotechnik musi opracować pretekst. Zazwyczaj przeprowadzany jest on na podstawie zdobytych wcześniej informacji, aby zwiększyć szanse na oczekiwany wynik. Niejednokrotnie

[23] https://www.skef.pl/smishing-rodzaj-przestepczosci-internetowej/, dostęp: 03.01.2021 r.
[24] C. Hadnagy, *Socjotechnika. Sztuka …*, dz. cyt., s. 262.
[25] https://zgasryzyko.pl/baza-wiedzy/co-to-jest-phishing-vishing-smishing/#toggle-id-3, dostęp: 03.01.2021 r.
[26] C. Hadnagy, *Socjotechnika. Sztuka …*, dz. cyt., s. 255, 261.

jednak w przypadku większych organizacji lub firm sytuacja wymaga przeprowadzenia kilku ataków vishingowych z wykorzystaniem różnych pretekstów.

Sposoby obrony przed atakami

W przypadku ataków opierających się na inżynierii społecznej obrona jest niezwykle trudnym zadaniem. Czynnik ludzki stanowi największą lukę w bezpieczeństwie, której załatanie jest niezmiernie trudne, a dokładniej nie da się tego dokonać w 100%. Na pomoc jednak przychodzą sposoby, które bezsprzecznie należy stosować, gdyż mogą one zmniejszyć prawdopodobieństwo powodzenia takiego ataku.

Podstawowym i zarazem najważniejszym elementem w dążeniu do zapewnienia bezpieczeństwa jest świadomość i wiedza. Ignacy Baliński powiedział kiedyś „nauka to potęgi klucz", stwierdzenie to nie straciło na wartości po dziś dzień i bez wątpienia jest wciąż aktualne. Bez odpowiedniej bądź, chociaż minimalnej wiedzy nie jest się w stanie zapewnić sobie lub firmie bezpieczeństwa. W związku z tym samokształcenie będzie się odnosiło w wyższym stopniu do osób prywatnych, natomiast szkolenia do firm. Wynika to z różnicy położenia nadmienionych grup.

W dążeniu do zapewnienia bezpieczeństwa istotnym elementem jest poznanie technik i reguł wykorzystywanych przez socjotechników, w jaki sposób działają. Dodatkowo ważne jest również zrozumienie wartości informacji, nawet tych z pozoru nieistotnych. Dla osoby, która nigdy wcześniej nie miała do czynienia z inżynierią społeczną poznanie podstawowych faktów wywoła wystarczające zdumienie i niedowierzanie. Nawet z pozoru nieistotna informacja o wyjeździe czy nieobecności w pracy może przyczynić się do powodzenia ataku.

Szkolenia powinny odbywać się regularnie co rok jako stała część procesu budowania świadomości w pracownikach[27]. Takie szkolenia poza dostarczeniem wiedzy podstawowej powinny pomóc rozwinąć w pracownikach umiejętność rozpoznawania stosowanych metod w prawdziwym życiu. W przypadku firm nie rzadko piętą Achillesa stają się tacy pracownicy jak przykładowo sprzątaczka. Na osoby o podobnym stanowisku często nie zwraca się uwagi, są to osoby pomijane. Niejednokrotnie jednak bywa, że właśnie taka osoba nie wiedząc nic o inżynierii społecznej w prosty sposób da się oszukać i wpuści napastnika. Dołączenie takiej grupy osób finansowo może wymagać większego wkładu pieniężnego, jednak przy tym może uchronić firmę. Szkolenia chodź nie tanie są niezbędne do zwiększenia bezpieczeństwa firmy. Jak powiedział sam Benjamin Franklin „inwestycja w wiedzę opłaca się najlepiej". Jeżeli pracownicy poza firmą wprowadzą również zmiany w życiu prywatnym będzie to najlepszym wyznacznikiem określającym udane i pomyślnie przeprowadzenie szkolenia.

[27] Tamże, s. 394.

Następnym istotnym elementem są programy wymagające zaangażowania uczestników. W pojęciu program kryje się dążenie do ciągłej poprawy bezpieczeństwa, bezustannemu zmierzaniu do rozwoju świadomości pracowników w firmie, czy też w kontekście osoby prywatnej. Nawiązuje to do efektywnego planowania i prowadzenia szkoleń, których celem nie jest tylko przeczytanie teorii, przeklikanie prezentacji czy obejrzenie filmiku.

Zaangażowanie uczestnika w dyskusję lub w przeprowadzeniu testu jest najbardziej efektownym sposobem na zdobycie jego zainteresowania. Co więcej dzięki zaangażowaniu odbiorców nie wyłączą się oni po 5 minutach jak niejednokrotnie dochodzi w czasie wykładu i nie uznają ich za nudne. Dodatkowo wnioski płynące z tego typu szkoleń prędzej uznają za praktyczne i przydatne, a nie jako obowiązkową pozycję do odhaczenia.

U podstaw obrony przed wszelakimi atakami nakierowanymi na systemy teleinformatyczne można między innymi wymienić:

- aktualizowanie systemu operacyjnego,
- posiadanie jak i aktualizowanie oprogramowania antywirusowego,
- zaktualizowane narzędzia takie jak Adobe Reader czy MS Word i inne,
- tworzenie kopii zapasowych.

Jako ostatni element w dążeniu do poprawy bezpieczeństwa jest przeprowadzanie testów penetracyjnych. Polegają one na zatrudnieniu specjalisty, który za pomocą wybranych metod sprawdzi bezpieczeństwo firmy. Takie testy wpisały się już w wiele norm bezpieczeństwa, które wymagają od firmy przeprowadzania ich, co najmniej raz w roku. Jest to jednak minimum, gdyż w celu poprawy i utrzymania wysokiego poziomu bezpieczeństwa powinny być przeprowadzane częściej.

Tego typu test opiera się na sprawdzeniu zarówno ludzi jak i fizycznych zabezpieczeń. Stanowi swego rodzaju symulację faktycznego ataku, ale z poszanowaniem zasad moralnych i poufnych danych. Taki audytor nie ma na celu skompromitowania firmy ani wyrządzenia jej szkód czy strat. Wszystkie wyznaczone przez klienta zasady są przestrzegane i respektowane, to samo tyczy się nagrywania bądź opisywania ataku w przyszłości podając go za przykład. Jeżeli firma wyraziłaby zgodę na wykorzystanie filmu bądź opisu testu, dane te zostałyby pozbawione wszelkich nazwisk, nazw firmy i innych charakterystycznych elementów, które pozwoliłyby na jakąkolwiek identyfikację.

Metodologia

Opracowanie *Socjotechnika a cyberprzestępczość na wybranych przykładach* przedstawia analizę i krytykę materiałów źródłowych pochodzących z opracowań zwartych, których liczba nie była zbyt duża w badanej tematyce, ale mimo to przydatna. Zostały one wybrane w wyniku rzetelnej selekcji, szczególnie w przypadku stron internetowych. Spowodowane to było dużą ilością nieprawdziwych informacji zamieszczanych w Internecie. Źródła internetowe, które poddano odpowiedniej selekcji i weryfikacji, stanowią większą

część materiałów podjętych badaniom. Wynika to z nowoczesności tematyki. Badania oparto również opracowania zwarte oraz dokumenty normatywne.

Przegląd literatury

W celu jak najdokładniejszego pogłębienia tematów analizie poddane zostały liczne źródła internetowe jak i parę pozycji z literatury zwartej. Jako pierwsza w tematyce cyberprzestępczości przydatna okazała się książka Jerzego Kosińskiego *Paradygmaty cyberprzestępczości* z 2015 r. W swej treści ukazywała wiele kluczowych informacji w tym zakresie przybliżając tą tematykę i wskazując interesujące jej aspekty.
Kolejną pozycją z tematyki socjotechniki było *Wywieranie wpływu na ludzi. Teoria i praktyka* Roberta Cialdiniego z 1984 r., która w bardzo dokładany sposób opisywała wszystkie sześć reguł ukazując dodatkowo szeroką gamę przykładów.

Dwie pozycje pod tymi samymi tytułami *Socjotechnika. Sztuka zdobywania władzy nad umysłami* zarówno z 2020 r. autorstwa Christophera Hadnagy, a w przypadku pozycji z 2012 r. dodatkowo autorstwa Paula Wilsona stanowiły największą bazę informacji na temat socjotechniki. Porównując nawet do źródeł internetowych te książki stanowiły znacznie lepsze źródło informacji. Christopher Hadnagy jest osobą, która pracuje przy testach penetracyjnych, to właśnie dzięki jego ogromnemu doświadczeniu i zdobytej wiedzy te książki stanowią tak doskonałe pozycje w niniejszej tematyce.

Wnioski

Rodzajów zagrożeń w cyberprzestrzeni jest wiele i wciąż ich przybywa. Tym, na co warto jednak zwrócić uwagę jest fakt, że część z nich przestaje traktować użytkowników bezosobowo. Mowa tu o atakowaniu osób, ludzi, którzy mają imię, stanowisko, empatię, którzy są zapracowani i w natłoku zadań łatwiej im jest popełnić błąd w szczególności wywierając na nim presję czasu.

W przypadku takich ataków najpowszechniejszą jego formą jest phishing wraz z jego pochodnymi, takimi jak SPAM, ataki telefoniczne czy wiadomości tekstowe. Skuteczność takich ataków spowodowana jest zazwyczaj nieświadomością ludzką w tym obszarze, zwyczajnym codziennym pośpiechem bądź też strachem. Łączenie zasady autorytetu z pilnym nakazem wykonania jakiegoś zadania sprawia, że ich skuteczność wzrasta.

Mówiąc o dążeniu do poprawy bezpieczeństwa zarówno osób indywidualnych jak i organizacji podstawową pomoc stanowi wiedza i samokształcenie. W przypadku organizacji może to być tworzenie specjalnych programów szkoleń, czy przeprowadzanie testów bezpieczeństwa, które mogą zwiększyć świadomość pracowników, ich niedostatków jak i możliwości napastników. Ostatecznie jednak to, jaką wiedzę posiądą pracownicy zależy głównie od nich

samych. Pracodawca natomiast może jedynie dołożyć wszelkich starań, aby dać im taką możliwość.

Bibliografia

Opracowania zwarte

1. Gardocki L., *Pojęcie przestępstwa i podziały przestępstw w polskim prawie karnym*, Uniwersytet Marii Curie-Skłodowskiej, Lublin 2013.
2. Maslow A., *Motywacja i osobowość*, IW PAX, Warszawa 1990.
3. Kosiński J., *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015.
4. Lucas E., *Oswoić cyberświat Tożsamość, zaufanie i bezpieczeństwo w Internecie*, Kurhaus Publishing, Warszawa 2017.
5. Podgórecki A., *Zasady socjotechniki*, Wiedza Powszechna, Warszawaw 1966.
6. Mitnick K., Simon W., *Sztuka podstępu*. *Łamałem ludzi, nie hasła*, Helion, Gliwice 2002.
7. Cialdini R., *Wywieranie wpływu na ludzi. Teoria i praktyka*, GWP Gdańskie Wydawnictwo Psychologiczne, Gdańsk 1984.
8. Hadnagy C., *Socjotechnika. Sztuka zdobywania władzy nad umysłami*, Helion, Gliwice 2020.
9. Hadnagy C., Wilson P., *Socjotechnika. Sztuka zdobywania władzy nad umysłami*, Helion, Gliwice 2012.

Dokumenty normatywne

1. Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. z 2011 nr 222, poz. 1323).
2. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).
3. Ustawa z dnia 6 czerwca 1997 r. Kodeks Karny.

Źródła internetowe

1. https://www.netia.pl/pl/blog/malware-co-to-jest-jakie-zagrozenie-sprawia, dostęp: 14.12.2020 r.
2. https://bitdefender.pl/co-to-jest-rootkit-oraz-jak-go-trwale-usunac-z-komputera/, dostęp: 15.12.2020 r.
3. https://bitdefender.pl/abc-cyberbezpieczenstwa-k-jak-keylogger/, dostęp: 15.12.2020 r.
4. http://perswazja.biz/szesc-regul-roberta-cialdiniego/, dostęp: 30.12.2020 r.
5. https://www.skef.pl/smishing-rodzaj-przestepczosci-internetowej/, dostęp: 03.01.2021 r.

6. https://zgasryzyko.pl/baza-wiedzy/co-to-jest-phishing-vishing-smishing/#toggle-id-3, dostęp: 03.01.2021 r.
7. https://www.cert.orange.pl/raporty-cert, dostęp: 10.12.2020 r.
8. https://trybawaryjny.pl/rodzaje-wirusow/, dostęp: 14.12.2020 r.
9. https://www.avast.com/pl-pl/c-spyware, dostęp: 18.12.2020 r.
10. https://mks-vir.pl/virus/ransomware/, dostęp: 18.12.2020 r.
11. http://www.crypto-it.net/pl/ataki/dos.html, dostęp: 18.12.2020 r.
12. https://dataspace.pl/blog/dos-rodzaje-atakow-cz-1/, dostęp: 19.12.2020 r.

bsm. pchor Szymon CYDEJKO

AUDYT I CERTYFIKACJA WOJSKOWYCH SYSTEMÓW TELEINFORMATYCZNYCH

Streszczenie

Podejmowana praca ma na celu zbadanie istoty audytu i certyfikacji wojskowych systemów teleinformatycznych. Jego realizacja nastąpiła głównie poprzez analizę literatury z zakresu bezpieczeństwa systemów teleinformatycznych oraz sposobów ich audytowania i certyfikowania. Dochodzi do tego zwrócenie uwagi na akty prawne oraz standardy z zakresu bezpieczeństwa teleinformatycznego. W niniejszej pracy prezentuje się wybrane zagadnienia dotyczące polityki bezpieczeństwa informacji. W ten zakres wpisuje się wyjaśnienie istoty informacji oraz opisanie elektronicznych metod ich przetwarzania. Uzupełnienie stanowią regulacje prawne podnoszące poziom bezpieczeństwa przetwarzanych informacji, a także aktualnie obowiązujące standardy w zakresie systemów teleinformatycznych. Ponadto przedstawiony został proces akredytacji bezpieczeństwa teleinformatycznego. Rozważania w tym zakresie rozpoczyna się od wyjaśnienia czym jest akredytacja oraz jak klasyfikuje się zasoby zaliczane do systemu teleinformatycznego. Dochodzi do tego złożony z kilku punktów proces audytu, a także dokumentacja opisująca bezpieczeństwo systemu teleinformatycznego. Spajane jest to przez krótkie rozważania poruszające tematykę certyfikowania takich systemów. Poprzez dogłębną analizę literatury przedmiotu z systemów teleinformatycznych oraz przetwarzania danych udało się zrealizować główny cel pracy, którym było: zbadanie istoty audytu i certyfikacji wojskowych systemów teleinformatycznych. Wykazano, że zarówno audyt, jak i certyfikacja są działaniami o charakterze procesowym, gdzie poszczególne czynności są wyraźnie rozłożone w czasie. Okazało się, że audyt musi być tak złożony i rygorystyczny, gdyż takie systemy przetwarzają szczególnie wrażliwe dane. Jak to zostało wykazane błędy na etapie audytu oraz dalej certyfikacji mogłyby doprowadzić do sytuacji, w której nieodpowiednio zabezpieczony system odpowiadałby za przetwarzanie wrażliwych danych, które mogłyby być ważne z punktu widzenia bezpieczeństwa państwa.

Słowa kluczowe:
audyt, certyfikacja, system teleinformatyczny, bezpieczeństwo, ryzyko, szacowanie ryzyka, dokumentacja bezpieczeństwa teleinformatycznego.

Abstract

Audit and certification of military ICT systems

The undertaken article is aimed at examining the essence of the audit and certification of military ICT systems. Its implementation was carried out mainly through the analysis of the literature on the security of ICT systems and the methods of their auditing and certification. There is also the emphasis on legal acts and standards in the field of ICT security. This paper presents selected issues related to information security policy. This scope includes explaining the essence of information and describing electronic methods of its processing. It is supplemented by legal regulations increasing the level of security of the processed information, as well as the current standards in the field of ICT systems. In addition, the ICT security accreditation process was presented. Considerations in this area begin with explaining what accreditation is and how to classify resources included in the ICT system. In addition, there is an audit process consisting of several points, as well as documentation surrounding the security of the ICT system. It is connected by short considerations about certification of such systems. Through an in-depth analysis of the literature about ICT systems and data processing, the main goal of the work was achieved, which was: to examine the essence of auditing and certification of military ICT systems. It has been shown that both audit and certification are process activities, where individual activities are clearly spread over time. It turned out that auditing must be so complex and rigorous as such systems process particularly sensitive data. As it has been shown, errors at the audit stage and further certification could lead to a situation in which an inadequately secured system would be responsible for the processing of sensitive data that could be important from the point of view of state security.

Keywords:
audit, certification, ICT system, security, risk, risk assessment, ICT security documentation.

Wstęp

W XXI wieku jeden z cenniejszych zasobów stanowi informacja. Widać to nawet po ludzkich zachowaniach, gdzie bardziej niż wojny ludzie obawiają się utraty dostępu do informacji. Jest to tematyka zyskująca na znaczeniu, jeśli uwzględni się dane przetwarzane przez systemy teleinformatyczne. Ze względu na potrzebę przetworzenia znacznej ilości danych w XXI wieku kwestie takie podejmowane są tylko pośrednio przez człowieka. Bezpośredni nadzór nad ich bezpieczeństwem sprawują specjalnie stworzone na tę okoliczność systemy teleinformatyczne. To właśnie przy ich pomocy można przetworzyć znaczne zasoby danych i to w możliwie krótkim czasie, co jest niemożliwe dla ludzkiego umysłu. Z uwagi na wrażliwość przetwarzanych danych systemy teleinformatyczne zajmujące się ich przetwarzaniem muszą bezwarunkowo spełniać wysokie wymagania. W podejmowanej pracy szczególną wagę przykłada się do procesu audytu oraz certyfikacji systemów teleinformatycznych. Obydwa pojęcia w dużym stopniu odnoszą się do sprawdzania poprawności działania systemu obsługującego wrażliwe dane. Problem audytu danych wydaje się zasadny do pojęcia, gdyż pośrednio chodzi o ludzkie bezpieczeństwo. Jak to zostanie wykazane audyt musi być procedurą skrajnie wymagającą, aby nie dopuścić do sytuacji, w której funkcjonalność systemu zostanie zagrożona.

Celem niniejszej pracy jest zbadanie istoty audytu i certyfikacji wojskowych systemów teleinformatycznych. Jego realizacja nastąpi głównie poprzez analizę literatury z zakresu bezpieczeństwa systemów teleinformatycznych oraz sposobów ich audytowania i certyfikowania. W niniejszej pracy prezentuje się wybrane zagadnienia dotyczące polityki bezpieczeństwa informacji. W ten zakres wpisuje się wyjaśnienie istoty informacji oraz opisanie elektronicznych metod ich przetwarzania. Ponadto przedstawiony został proces akredytacji bezpieczeństwa teleinformatycznego. Rozważania w tym zakresie rozpoczyna się od wyjaśnienia czym jest akredytacja oraz jak klasyfikuje się zasoby zaliczane do systemu teleinformatycznego. Dochodzi do tego złożony z kilku punktów proces audytu, a także dokumentacja opisująca bezpieczeństwo systemu teleinformatycznego. Spajane jest to przez krótkie rozważania poruszające tematykę certyfikowania takich systemów.

Praca w obszarze audytu oraz certyfikacji systemów teleinformatycznych bazuje wyłącznie na źródłach wtórnych, którymi są pozycje książkowe z rozpatrywanego zagadnienia. Całość zakończona jest wnioskami.

Podstawowe założenia polityki bezpieczeństwa informacji

Definicja informacji

Człowiek, aby mógł się prawidłowo rozwijać potrzebuje do tego sprzyjającego otoczenia. Chodzi przede wszystkim o to, aby z otoczenia wykluczyć wszystkie potencjalne zagrożenia. W poszczególnych dziesięcioleciach wyraźnie zmieniały się kwestie, które dla człowieka były fundamentalne.

Obecnie na początku XXI wieku taką zmienną jest informacja. To właśnie dzięki niej jednostka wie czego może się spodziewać w najbliższej przyszłości oraz jak może się przygotować do konkretnych sytuacji. Już na wstępie podejmowanych rozważań zauważa się, że ludzi żyjących w XXI wieku określa się mianem społeczeństwa informacyjnego. Pośrednio wynika to z rozwoju technologii internetowych oraz w znacznym stopniu bazowaniu na informacji przekazywanej drogą elektroniczną. W ogólnym ujęciu informację można przyrównać do dość specyficznego dobra, które warunkuje społeczeństwu swobodę egzystencjonalną oraz względne bezpieczeństwo. Dodając do tego wymiar ekonomiczny informację przyrównuje się do towaru niematerialnego, który może być zasobem o znaczeniu strategicznym. W swojej uniwersalności informacja może odnosić się do pojedynczej osoby, większej zbiorowości, podmiotów gospodarczych, a nawet państwa. Już ten prosty przykład potwierdza, że informacje wykorzystywane są przez wszystkich. Informacja jest kluczowa dla bezpieczeństwa, gdyż to właśnie dzięki niej można uzyskać przewagę nad każdym przeciwnikiem, niezależnie od tego jak bardzo jest silny. Dzięki niej można podjąć pewne działania z wyprzedzeniem i w pewnym stopniu zaskoczyć przeciwnika. Jednak, aby to było możliwe to informacja musi charakteryzować się określoną jakością i być przede wszystkim prawdziwa. Ze względu na takie wymierne korzyści informacja staje się dobrem, które za określoną kwotę można kupić. Sprawdza się to na każdej płaszczyźnie, nie tylko militarnej, ale również biznesowej i prywatnej. Osoba, która odpowiednio wcześnie pozyskała informację, której nie ma jeszcze otoczenie może to wykorzystać na swoją korzyść[1].

Do informacji można podchodzić także jako do szczególnego dobra, które pozwala skutecznie rywalizować. W wielu przypadkach odpowiednia informacja stanowi czynnik pozwalający osiągnąć przewagę. Przy czym zależnie od charakteru samej informacji taka przewaga może wystąpić na płaszczyźnie: gospodarczej, militarnej, politycznej lub dowolnie innej. Jest to aspekt coraz bardziej zyskujący na znaczeniu w zglobalizowanym i ściśle konkurencyjnym świecie, gdzie dany ruch powinien odbywać się w oparciu o sprawdzone informacje[2].

Wprowadzenie do bezpieczeństwa informacji

Informacja jako szczególne dobro może być postrzegane także jako zmienna ukierunkowana na bezpieczeństwo. Jeśli następuje połączenie typowej informacji z bezpieczeństwem to uzyskuje się czynnik bezpieczeństwa informacyjnego. Tłumaczyć to można jako podstawę zaufania podmiotu, co do faktu, że przekazywana informacja jest rzetelna w przekazie i ma służyć jego

[1] K. Liderman, *Bezpieczeństwo informacyjne - nowe wyzwania*, PWN, Warszawa 2014, s. 17-18.

[2] A. Bógdał-Brzezińska, M. F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2003, s. 323.

dobru. Tym samym jednostka nie powinna mieć obaw, że wykorzystana informacja przełoży się na jej szkodę. Inaczej można przyrównać je do uzasadnionego zaufania w zakresie prawdziwości przekazywanej lub pozyskiwanej informacji. Jest ono jedną z podstaw bezpieczeństwa informacyjnego, na którym bazują nie tylko przedsiębiorstwa, ale również rządy państw. Przy czym jest to kwestia dużo bardziej złożona, gdyż działania nie kończą się na przekazaniu rzetelnej informacji. Równie ważne jest to, aby taka informacja cały czas podlegała ochronie, w wyniku czego nie może być dostępna dla osób trzecich. W zakresie bezpieczeństwa informacyjnego same informacje dzielone są na kilka rodzajów. W jednym z dostępnych kryteriów informacje dzieli się na wrażliwe oraz niewrażliwe. Naturalnie dużo większa uwaga w zakresie ochrony musi być zwracana na informacje zaliczane do tej pierwszej grupy. Jeśli informacja wrażliwa zostanie przejęta przez podmiot zewnętrzny to może być wykorzystana na rzecz spowodowania jakiejś szkody. Nie można wykluczyć przypadku, że niedopatrzenia w dziedzinie bezpieczeństwa przyczynią się do zniekształcenia samej informacji. Bardzo często wymóg ochrony informacji wrażliwych jest regulowany zapisami aktów prawnych lub innymi wewnętrznymi regulaminami podmiotu. Po drugiej stronie uwzględnia się informacje niewrażliwe, które z założenia są mało istotne przez co nie muszą być chronione, gdyż pozyskanie ich przez podmioty trzecie nie będzie stanowić czynnika zagrożenia. W szczególnych przypadkach informacja niewrażliwa może stać się informacją wrażliwą. Dzieje się tak często, gdy przekazywany jest większy pakiet informacji, łącząc tym samym kilka uzupełniających się wątków.

Stawiając w centrum państwo zauważa się, że bezpieczeństwo informacyjne to po prostu podejmowanie się ściśle określonych działań ochronnych w dziedzinie informacji. Głównie chodzi o zapobieganie pozyskania przez osoby nieuprawnione dostępu do informacji niejawnych. Wszelkimi dostępnymi sposobami powinno się zapobiegać ujawnianiu informacji, które posiadają rangę niejawnych. Zależnie od potrzeb może zachodzić wymóg zagwarantowania bezpieczeństwa, fizycznego lub technicznego. Ze względu na posiadane technologie informatyczne dużo częściej nacisk zostanie położony na ten drugi przypadek. Jednak nie oznacza to, że w bezpieczeństwie informacyjnym ochrona fizyczna może zostać pominięta. Bardzo ważne jest to, aby fizycznie zabezpieczyć całe pomieszczenia, serwery lub konkretne nośniki służące do przechowywania informacji niejawnych. Z punktu widzenia państwa takie inicjatywy przełożą się na bezpieczeństwo wymiany informacji z innymi państwami. Działania w zakresie bezpieczeństwa informatycznego uznawane są za dość kosztowne ze względu na fakt, że znaczne zasoby informatyczne przechowywane są w formie wirtualnej, co wymaga nie tylko zaawansowanego technologicznie sprzętu, ale również oprogramowania. Przy czym zasoby

takie dość szybko tracą na skuteczności, przez co konieczne jest ich modernizowanie lub wymiana na zupełnie nowe technologie[3].

Proces akredytacji bezpieczeństwa teleinformatycznego

Czym jest akredytacja bezpieczeństwa teleinformatycznego?

Stworzenie sytemu teleinformatycznego nie oznacza tego, że jest on zdatny do użycia, oraz że dane przez niego przetwarzane są bezpieczne. Ukierunkowując się na względy bezpieczeństwa przeprowadzany jest proces akredytacji, który jest po prostu procedurą dopuszczenia systemu teleinformatycznego do użycia. Przez użycie rozumie się możliwość bezpiecznego przetwarzania przez system informacji niejawnych. Już na wstępie warto odnotować, że wszystkie zasoby wchodzące w skład systemu teleinformatycznego muszą pozytywnie przejść proces akredytacji. Za proces akredytacji zależnie od potrzeb odpowiadać będzie ABW lub SKW. Takie zatwierdzenie będzie przeprowadzane na bazie dostarczonej dokumentacji opisującej działanie systemu. Wspomniane dwa podmioty będą zawsze odpowiadać za akredytację, jeśli system będzie stworzony do przetwarzania informacji z klauzulą poufne. Jeśli dane będą posiadać jedynie klauzule zastrzeżone to wystarczy, że akredytację przeprowadzi kierownik organizacji tworzącej system. Aby proces akredytacji mógł się zakończyć pozytywnie to zawsze podstawą jest sporządzenie możliwie szczegółowej dokumentacji opisującej system, a także sposób jego działania. Dochodzi do tego wymóg wyznaczenia przynajmniej jednej osoby, a najlepiej kilku, które będą czuwać nad bezpieczeństwem systemu. Zdarza się, że w bardzo rozbudowanych systemach teleinformatycznych cała komórka organizacyjna odpowiedzialna jest za utrzymanie należytego poziomu bezpieczeństwa systemu. Jeśli systemem ma posługiwać się tylko jedna organizacja to wystarczy, że akredytacja zostanie przeprowadzona przez kierownika organizacji. Jednak nawet takie przypadki nie wyłączają obowiązku komunikowania się z ABW lub SKW. Chodzi o to, że maksymalnie do 30 dni od dnia przeprowadzenia akredytacji kierownik organizacji powinien wysłać stosowny raport z podjętych działań wspomnianym podmiotom. ABW oraz SKW pełnią w takim przypadku jedynie funkcję nadzorującą, gdyż otrzymują już zatwierdzony raport, który sprawdzają pod kątem potencjalnych uchybień. Odpowiedź musi nastąpić najpóźniej do 30 dni od otrzymania raportu, a tym samym może być on zaakceptowany lub zostaną wydane dyspozycje, co do działań naprawczych. Naturalnie szczególny nacisk będzie kładziony na ochronę informacji niejawnych, gdzie podmiot może być poproszony o wprowadzenie dodatkowych zabezpieczeń. Zdarzyć się może również, że trzeba będzie przemodelować ustawienia konfiguracyjne, gdyż zdaniem ABW lub SKW mogą być one mało skuteczne w dziedzinie bezpieczeństwa. Od otrzymania takich wytycznych kierownik ma jedynie 30 dni na wprowadzenie żądanych ulepszeń. Jeśli termin zostanie przekroczony to akredytacja uzyskuje wynik negatywny. Co

[3] K. Liderman, *Bezpieczeństwo informacyjne…,* dz. cyt., s. 180.

wartym odnotowania okresowo proces akredytacji przeprowadzany jest w stosunku do systemów teleinformatycznych będących już w użyciu. Jeśli odnotuje się jakieś nieprawidłowości to sprawa jest poważna, gdyż akredytacja nie jest przedłużana, a system czasowo musi zostać wyłączony z użycia. W wyniku zauważonych nieprawidłowości akredytacja przeprowadzona przez kierownika organizacji może być niewystarczająca i cała procedura przejmowana jest zależnie od stopnia podległości przez ABW lub SKW. Co do wymiaru czasowego zgodnie z obwiązującym prawem dokumentem akredytacji jest ważny tylko 5 lat, po czym proces musi być przeprowadzony ponownie[4].

Przyjmuje się, że im bardziej wrażliwe dane przetwarzane są przez system to tym proces akredytacji będzie bardziej złożony. Naturalnie najbardziej dokładna akredytacja musi być przeprowadzona względem systemów, które dysponują danymi o statusie tajnych lub ściśle tajnych. Takie warianty wymuszają bezpośrednie przesyłanie dokumentacji systemowej do ABW lub SKW. Do tego kierowany jest do tych instytucji specjalny wniosek z prośbą o przeprowadzenie akredytacji. W kolejnym etapie następuje ustalenie terminu oraz zakresu przeprowadzanych działań akredytacyjnych. Po faktycznym przeprowadzonym audytu do instytucji przesyłany jest raport, w którym ujmowane są ewentualne różnice pomiędzy dokumentacją, a faktycznym stanem działania systemu. Wymóg wprowadzenia zmian naprawczych w systemie automatycznie wymusza ponowne przeprowadzenie audytu po usunięciu usterek. Jeśli nieprawidłowości w systemie już nie ma to wystawiane jest świadectwo akredytacyjne, które ważne jest do 5 lat. Co wartym odnotowania to fakt, że audyt nie jest darmowy. Osoby odpowiedzialne za audyt zgodnie z prawem otrzymują 0,1 stawki przeciętnego miesięcznego wynagrodzenia za każdą przepracowaną godzinę. Z takich opłat zwolnione są jedynie podmioty administrujące systemami, które posiadają status jednostek budżetowych[5].

Klasyfikacja zasobów teleinformatycznych

Zasoby teleinformatyczne celem zapewnienia im jak najlepszego bezpieczeństwa poddawane są złożonej klasyfikacji. Najczęściej w wyniku podjętej klasyfikacji poszczególnym zasobom przypisywane są po prostu prawa dostępu. Już na wstępie należy powiedzieć, że zasoby teleinformatyczne znacząco różnią się od siebie i nie każdy może otrzymać status publicznego. Takie podejście byłoby po prostu skrajnie niebezpieczne dla poszczególnych systemów. W tym miejscu szczególna uwaga zostanie poświęcona klasyfikacji bezpieczeństwa. Wyznacza się ją poprzez zwrócenie uwagi na poziom tajności danego zasobu. W uproszczeniu każdy zasób otrzymuje etykietę ochrony, która może traktować dany element jako: zastrzeżony, poufny, tajny lub ściśle tajny. Przy klasyfikacji stosuje się zasadę wiedzy niezbędnej. Oznacza to, że dany zasób powinien być upubliczniony tylko w takim stopniu, w jakim jest to absolutnie konieczne. Pełne sklasyfikowanie danego zasobu skupia się na

[4] B. Iwaszko, *Ochrona informacji*…, dz. cyt., s. 148-149.
[5] Tamże, s. 150.

przypisaniu mu kategorii tajności oraz poziomu tajności. Wartym odnotowania jest fakt, że wprowadzenie w przedsiębiorstwie klasyfikacji bezpieczeństwa zasobów teleinformatycznych automatycznie będzie musiało się wiązać z klasyfikacją pracowników. W uproszczeniu chodzi o to, aby dostęp do najbardziej poufnych informacji mieli najbardziej odpowiedzialni pracownicy. Jest to zadanie dość trudne, gdyż wymaga zestawienia ze sobą wszystkich zasobów i pracowników działających w danym podmiocie. W praktyce bardzo często będzie dochodzić do późniejszych zmian w uprawnieniach, gdyż cały czas podejmować się będzie inicjatywy na rzecz poprawy bezpieczeństwa. W pewnym stopniu stanowi to wyraz zaufania do poszczególnych pracowników, gdyż na szali stawia się bezpieczeństwo nie rzadko bardzo rozbudowanego systemu. Sama klasyfikacja stanowi formę miary ważności poszczególnych zasobów systemowych. Przechodząc do kolejnego kryterium klasyfikacyjnego uwzględnia się parametr ochrony prawnej. W tym zakresie zasoby dzielone są na prawnie chronione oraz niepodlegające prawnej ochronie. W pierwszej grupie znajdą się wszystkie informacje niejawne ze szczególnym naciskiem na dane osobowe oraz tajemnice prawnie chronione. Za takie tajemnice uznaje się te będące w posiadaniu: banków, dziennikarzy, lekarzy, przedsiębiorców, a nawet księży. Z kolei informacje niepodlegające ochronie prawnej uwzględniają wszystkie zasoby, które nie muszą być chronione. Naturalnie nie oznacza to, ze takie zasoby są mało ważne dla instytucji, jednak nie uznaje się ich za kluczowe[6].

Klasyfikacja zasobów teleinformatycznych jest o tyle ważna, że pomaga w dogłębnym zaplanowaniu ochrony konkretnego systemu. Jeśli taki system tworzony jest w obrębie państwa to jego poszczególne komponenty muszą być poddane procedurze ochronnej przez Służby Bezpieczeństwa Państwa. Dokonuje się tego na postawie Szczegółowych Wymagań oraz Procedur i Bezpieczeństwa Eksploatacji. Na szczeblu państwowym do użytku zostaną dopuszczone jedynie zasoby, które posiadają odpowiednie certyfikaty bezpieczeństwa. Jeszcze jednym kryterium różnicującym zasoby teleinformatyczne jest to odnoszące się do rodzaju przetwarzanych danych oraz mogących dotyczyć ich zagrożeń. Jednym z nich są zasoby z poziomem podstawowym, gdzie w systemie nie są przetwarzane dane wrażliwe. Za przykład takich danych mogą służyć poglądy religijne oraz przynależność partyjna. Ponadto konieczne jest, aby żaden element systemu posiadający taki status nie był połączony z siecią publiczną. Drugą grupą są zasoby posiadające status podwyższony. Tutaj dane wrażliwe mogą już być przetwarzane, jednak odbywa się to tylko dla celów konkretnego przedsiębiorstwa, a system nie posiada połączenia do sieci publicznej. Najbardziej rozbudowany zakres ochrony przewidziany jest dla zasobów systemowych posiadających poziom podwyższony. System tworzony w ramach tego poziomu może dysponować dostępem do ściśle tajnych

[6] K. Liderman, *Analiza ryzyka*…, dz. cyt., s. 33-34.

informacji, a do tego przynajmniej jeden komponent posiada bezpośrednie połączenie z siecią publiczną. To właśnie zasoby z tej ostatniej grupy muszą być zabezpieczane przy wykorzystaniu rozwiązań kryptograficznych. Przy czym takie szyfrowanie będzie odnosić się nie tylko do samych danych wrażliwych, ale również do tych danych, które służą jedynie do uwierzytelniania systemowego. Niezależnie od tego, do jakiej grupy ochronnej zasoby systemowe zostały sklasyfikowane zawsze konieczne jest prowadzenie instrukcji zarządzania systemem informatycznym. Wpisywać się to będzie w prowadzoną przez przedsiębiorstwo politykę bezpieczeństwa[7].

Dokumentacja bezpieczeństwa teleinformatycznego

Szczególne wymagania bezpieczeństwa

System teleinformatyczny to nie tylko zasoby sprzętowe oraz programowe. Równie ważna dołączona jest do niego dokumentacja, która stanowi pisemne potwierdzenie spełnionych wymogów bezpieczeństwa. Naturalnie taka dokumentacja będzie składać się z kilku części tematycznych, a jedną z nich jest grupa dokumentów nazywana szczególnymi wymaganiami bezpieczeństwa (SWB). Jak sama nazwa wskazuje w takim dokumencie znajdują się dość specyficzne dane, które w istocie skupiają się na przetwarzaniu informacji niejawnych. Ważnym odnotowania jest fakt, że taki dokument zawsze tworzony jest w momencie samego projektowania systemu teleinformatycznego. Uwzględnia on kilka elementów, jednak każdy z nich musi odnosić się do konkretnego systemu teleinformatycznego. Wynika to z faktu, że każdy system nieznacznie inaczej jest tworzony, a do tego specyfika działania przedsiębiorstwa wymuszać może pewne ograniczenia. Pomimo tego, że dokument ten tworzony jest na etapie projektowania to jak najbardziej powinna następować jego aktualizacja już w momencie faktycznego wdrażania systemu do działania. Kolejne uaktualnienia dokumentu podejmowane są w fazie eksploatacji systemu. W ujęciu technicznym dokument taki uwzględnia zapisy dotyczące rodzajów oraz klauz tajności informacji niejawnych. Jednak dotyczy to wyłącznie pakietów danych, które faktycznie mają być przetwarzane przez konkretny system. Ze względu na przyjęte ustawienia konfiguracyjne dokumentacja powinna skupić się na ujęciu funkcji oraz przeznaczenia systemu. Wśród licznych zapisów uwzględnionych dokumentów uwzględnia się także kwestie dotyczące szacowania ryzyka. Przy czym musi być to kompletny raport z takiego procesu, aby dało się wyciągnąć bardziej rozbudowane wnioski na rzecz poprawy bezpieczeństwa[8].

Dochodzi do tego informacja o ryzkach szczątkowych. Co do zasady są to niewielkie zagrożenia dla sytemu teleinformatycznego, jednak kierownictwo powinno zaakceptować taki stan rzeczy składając pod tym stosowny podpis. To właśnie w tym dokumencie uwzględnia się grupy pracowników

[7] Tamże, s. 35.
[8] B. Iwaszko, *Ochrona informacji*…, dz. cyt., s. 145.

z podziałem na uprawnienia w zakresie przetwarzania informacji. Dochodzą do tego zapisy ukierunkowane na bezpieczeństwo pracy samego systemu. Co do samych pracowników mających mieć dostęp do systemu to w dokumencie szczegółowo zostają wymienione zaliczone przez nich szkolenia oraz specjalne uprawnienia, które zostały im wcześniej przypisane. Nie mniej istotne są zapisy dotyczące poświadczeń bezpieczeństwa użytkowników oraz ich sposoby uwierzytelniania. Chodzi o to, aby na papierze zostało przedstawione na jakiej podstawie system ma zezwolić konkretnemu pracownikowi na dostęp do zasobów systemowych. W SWB uwzględnia się dokładną lokalizacje systemu teleinformatycznego. Przy czym nie chodzi jedynie o wskazanie firmy, która jest operatorem konkretnego sytemu, ale najlepiej sale, w których zlokalizowane są zasoby sprzętowe. Równie ważne są kwestie odnoszące się do wymogów sprzętowych oraz w oprogramowaniu, które muszą zostać spełnione, aby wymienić dane pomiędzy przynajmniej dwoma niezależnymi systemami. Co do kwestii ochrony fizycznej dokument również uwzględnia pewne informacje z tego zakresu. Szczególnie ważne są strefy ochronne, które mogą być przekraczane wyłącznie przez uprawnionych pracowników. Wpisują się w to także informacje o zastosowanych zabezpieczeniach. Jeśli system jest chroniony rozwiązaniami o charakterze typowo elektromagnetycznym lub kryptograficznym to dokument bezwzględnie musi to opisywać[9].

Cały czas ukierunkowując się na bezpieczeństwo to SWB podejmuje dość istotną kwestię, jaką jest potrzeba zachowania ciągłości działania systemu. W tym zakresie opisany musi być sposób tworzenia kopii zapasowej oraz przywracania danych z takich zasobów. Równie ważne uwzględnienie jest zapisów odnoszących się do przewidzianego zasilania awaryjnego, które ma zapewnić ciągłość działania systemu w przypadku przerw w dostawie energii elektrycznej. Dochodzą do tego informacje dotyczące sposobu przeprowadzania przeglądów diagnostycznych, ewentualnych napraw oraz działań, które cały czas powinny podnosić poziom bezpieczeństwa systemu. Pomimo wyraźnego postępu cyfryzacji pewne dane systemowe mogą być przechowywane na oddzielnych nośnikach. Omawiany dokument powinien i je również uwzględniać, szczególnie w zakresie przechowywania takich zasobów oraz niszczenia tych niepotrzebnych. Jest to dokument, który na bieżąco powinien podejmować kwestie podejmowanych uaktualnień systemowych oraz wszystkich innych zmian, ze szczególnym naciskiem na te o charakterze bezpieczeństwa. Ostatnia część dokumentu zawiera dokładne ustalenia co do tego, w jaki sposób system ponownie powinien przejść proces akredytacji lub zostać wycofany z użycia[10].

Procedury bezpieczeństwa eksploatacji

Wśród licznych dokumentów w jakimś stopniu regulujących kwestie bezpieczeństwa systemu teleinformatycznego są procedury bezpieczeństwa

[9] Tamże, s. 146.
[10] Tamże, s. 146.

eksploatacji (PBE). Jak sama nazwa wskazuje jest to dokument opisujący sposób jego wykorzystania tak, aby dane przez niego obsługiwane nie były zagrożone. Jest to dokument bezpośrednio odwołujący się do art. 2 Ustawy o ochronie informacji niejawnych z dnia 5 sierpnia 2010 roku. Wynika z tego, że systemy teleinformatyczne służą do przetwarzania tego typu danych, co wymaga specjalnych regulacji. Jest to dokument, który szczegółowo uwzględnia zakres obowiązków dla pracowników mających styczność z systemem teleinformatycznym. Co do zasady dokument jest sporządzany dopiero na etapie wdrażania systemu i zawsze po zakończonym szacowaniu ryzyka. Natomiast w czasie eksploatacji następuje jego uaktualnienie. Znaczna część dokumentu poświęcona jest procedurom, które muszą zostać przeprowadzone na rzecz poprawy bezpieczeństwa systemu. Przy czym muszą być uwzględnione szczegółowe rozwiązania pozwalające zaadaptować w praktyce wspomniane procedury. Zgodnie z zapisami w dokumencie najczęściej za wprowadzanie procedur będą odpowiadać tylko dwie osoby, czyli administrator sytemu oraz inspektor bezpieczeństwa teleinformatycznego. Rzadziej dokument uwzględnia, że inicjatorem wprowadzania poszczególnych zmian może być pełnomocnik ochrony lub kierownik kancelarii tajnej. Jest to kolejny dokument, w którym podejmowana jest kwestia zabezpieczeń systemowych po stronie oprogramowania i sprzętu. Celem poprawy bezpieczeństwa dokument szczegółowo uwzględnia sposoby modyfikowania systemu oraz postępowanie na wypadek ponownej konfiguracji. Nie mniej istotne są zapisy dające wytyczne do serwisowania systemu. W dalszej części znajdują się wytyczne w zakresie przeprowadzania audytu bezpieczeństwa. Dochodzą do tego procedury, które bezwzględnie trzeba zainicjować w momencie wystąpienia zagrożeń lub sytuacji nieprzewidzianych. Tym samym na podstawie rozwiązań awaryjnych możliwe jest utrzymanie ciągłości działania systemu. Dokument w tym punkcie będzie wskazywać na potrzebę uaktywnienia się administratora systemu, który ma za zadanie wprowadzić takie rozwiązania w praktykę[11].

Dokument w aspekcie bezpieczeństwa podejmuje również kwestie zachowań pracowników mających styczność z systemem. Szczególny nacisk kładziony jest na zachowania pracowników zatrudnionych w komórce ochronnej. Duży nacisk kładziony jest na zapewnienie fizycznej ochrony systemu, co ma bezpośrednie przełożenie na przeprowadzoną analizę bezpieczeństwa. Niektóre sugestie w dokumencie będą odnosić się do postępowania pracowników z elektronicznymi urządzeniami magazynującymi. Jeżeli system ma dostęp do materiałów szyfrowanych kryptograficznie, to dokument powinien jasno wskazać, co pracownicy powinni zrobić z takimi danymi. Dochodzą do tego dokładne wytyczne, co do zachowań pracowników, którzy powinni podjąć konkretne działania, jeśli zauważą, że bezpieczeństwo systemu jest zagrożone. Dokument wskazuje, że każdy incydent zagrażający bezpieczeństwu powinien być zgłaszany[12].

[11] Tamże, s. 147.
[12] Tamże, s. 148.

Ostania część dokumentu to wytyczne dla samych użytkowników systemu oraz personelu pomocniczego, który prowadzi swoje czynności bezpośrednio w pomieszczeniach, gdzie fizycznie znajduje się system. Wpisują się w to instrukcje dotyczące pobierania danych z systemu, aby wszystko zachodziło bezpiecznie oraz kwestie ukierunkowane na uruchamianie ora zamykanie systemu. Często zdarza się, że dokument uwzględniać będzie okresowe szkolenia użytkowników systemu, aby tym samym wiedzieli oni jak się nim posługiwać. Przy czym częstotliwość szkoleń może się znacząco różnić i być zależna od grupy, do której przypisany jest dany użytkownik systemu. Co do pracy personelu pomocniczego to przede wszystkim uwzględniane są kwestie wpuszczania innych osób do pomieszczeń, w których znajdują się urządzenia połączone z systemem. Tym samym dokument może sugerować, że nie w każdym przypadku zgoda na wejście do pomieszczenia będzie udzielana przez personel pomocniczy, a spoczywać to będzie na administratorze systemu. Dochodzą do tego wytyczne nadzoru użytkowników systemu, w pomieszczeniach, gdzie znajduje się system. Dokument wskazuje, że osoby trzecie nie powinny nawet przebywać w takich pomieszczeniach bez nadzoru personelu pomocniczego[13].

Resumując widać wyraźnie, że jest to bardzo ważny dokument, który od strony technicznej kładzie bardzo duży nacisk na względy bezpieczeństwa. Jeśli pracownicy administrujący systemem oraz sami użytkownicy postępują według zapisów wspomnianego dokumentu to nie powinny zdarzyć się sytuacja zagrażające bezpieczeństwu danych.

Analiza ryzyka

Dostęp do zasobów informatycznych zawsze rozpatrywany jest w kategoriach, które można wykorzystać na rzez poprawy sytuacji ekonomicznej podmiotu. Jednak zawsze należy pamiętać, że zasoby teleinformatyczne mogą ulegać pewnym awariom lub być atakowane przez osoby trzecie. Każde z tych zdarzeń wpisuje się w zakres zagrożeń, co w jakimś stopniu stanowi ryzyko dla całego podmiotu. Chcąc uniknąć wymienionych sytuacji stawia się na kompleksową analizę ryzyka, która co do zasady jest rozpatrywana w kategoriach procesu. Sama analiza ryzyka wpisuje się w szersze pojęcie jakim jest zarządzanie ryzykiem. Co do samej analizy składa się ona z trzech uzupełniających się komponentów. Przede wszystkim chodzi o proces identyfikacji: zagrożeń oraz potencjalnych strat. Na podstawie tego możliwe jest oszacowanie ryzyka oraz jego fundamentalna ocena. Tym samym można powiedzieć, że analiza ryzyka to grupa działań zmierzających do identyfikacji środowiska, w którym się działa oraz zagrożeń mogących w nim wystąpić. Przy czym co do samej identyfikacji samych zagrożeń to powinno być to przeprowadzone w taki sposób, aby dało się je porównać. Jest to czynność konieczna, jeśli oczekuje się zapewnienia systemowi teleinformatycznemu pożądanego stopnia

[13] Tamże, s. 148.

bezpieczeństwa. W każdym przypadku system będzie uzależniony od otoczenia oraz od przygotowania się na zagrożenia mogące wystąpić. Tym samym analiza jest konieczna, aby zapewnić odpowiedni poziom bezpieczeństwa. Analiza ryzyka nie powinna ograniczać się wyłącznie do zagrożeń występujących w otoczeniu. Równie ważne jest skupienie się na charakterze działania danego podmiotu. Tym samym uwzględnić się powinno zmiany organizacyjne oraz sprzętowo-programowe dotyczące konkretnego systemu teleinformatycznego. W dodatku takie działania powinny przyjmować charakter cykliczności. Im częściej analiza ryzyka będzie przeprowadzana to tym większa szansa na to, że przedsiębiorstwo będzie mogło lepiej przygotować się na aktualne potencjalne zagrożenia. Naturalnie szereg zagrożeń będzie ewoluować, przez co taka cykliczność pozwala zrozumieć działania potencjalnych agresorów. To właśnie taka analiza stanowić będzie również bazę do wszelkich modyfikacji w zakresie zabezpieczeń systemu. Najczęściej dodawane będą kolejne zabezpieczenia po otrzymaniu wyników z analizy. Raczej nie stosuje się strategii, gdzie usuwane są pewne zabezpieczenia mimo, iż analiza ryzyka wykazała, że dane zagrożenie nie jest już istotne dla poprawności działania systemu. Poza samymi zagrożeniami w takiej analizie zwraca się uwagę na podatność systemu na możliwość ulegnięcia konkretnemu zagrożeniu. Oznacza to, że w otoczeniu może występować zagrożenie, jednak system został tak stworzony, że nie jest zupełnie na niepodatny[14].

Podejmowana analiza ryzyka wpływać będzie na wszystkie obszary funkcjonowania przedsiębiorstwa, a nie tylko na konkretne zasoby teleinformatyczne. Szczególnie duży wpływ odnotowuje się na wybrane strategie działania, którymi może się kierować przedsiębiorstwo. Analiza ryzyka szczególnie może dotyczyć działań o charakterze strategicznym. W tym zakresie uwzględnia się wpływ o charakterze długoterminowym, gdzie zagrożone mogą być cele o znaczeniu fundamentalnym. Nie mniej niebezpieczne są zagrożenia wpływające na działania operacyjne. Takie zagrożenia mogą zagrażać prawidłowości podejmowania codziennych działań. Jest to bardzo ważne z punktu widzenia klientów, którzy poprzez zmaterializowanie się zagrożenia mogą mieć utrudniony dostęp do wcześniej poprawnie funkcjonującego systemu teleinformatycznego. Następne są zagrożenia o charakterze finansowym, w których chodzi o zagrażanie kapitałowi przedsiębiorstwa oraz prawidłowym działaniem, co wymuszać może wypłacanie odszkodowań dla odbiorców. W pewnym stopniu taka analiza wpływać będzie na strategię informacyjną, gdzie chodzić będzie o bezpieczeństwo pakietów informacji nie rzadko poufnych, które przynajmniej czasowo są w posiadaniu przedsiębiorstwa. Uzupełniane jest to przez strategię zgodności, w której chodzi o to, aby działać w sposób zgodny z obowiązującym prawem[15].

[14] K. Liderman, *Analiza ryzyka*…, dz. cyt., s. 79.
[15] Tamże, s. 78-79.

W analizie ryzyka ukierunkowując się na identyfikację zagrożeń można podzielić je na te, które wymagają posiadania wiedzy, co do funkcjonowania konkretnego systemu teleinformatycznego oraz takie, które takiej wiedzy nie wymagają. Dla przykładu w tej drugiej grupie chodzić może o zagrożenia determinowane katastrofami naturalnymi, czego reprezentantem będzie pożar lub powódź. Co prawda takie zagrożenie nie ma nic wspólnego z zasobami informatycznymi, jednak analitycy muszą je uwzględnić, gdyż realnie mogą zagrażać posiadanym zasobom. W wyniku takiej analizy może zostać podjęta decyzja o potrzebie automatycznego tworzenia kopii zapasowych lub utrzymywania newralgicznych części systemu w pomieszczeniach, które wyłączone są spod takich zagrożeń. Drugą grupę stanowią zagrożenia, które wykazują związek z wiedzą odnoszącą się do konkretnego systemu. Przykładowymi zagrożeniami w tej grupie będą: awarie systemów IT, utrata kluczowych pracowników lub grupy klientów. Przy analizie ryzyka pomocne mogą być raporty z przeszłości, a szczególnie takie, które dotyczyły zmaterializowania się jakichś zagrożeń. Zależnie od przypadków takie raporty mogą znajdować się w zasobach przedsiębiorstwa lub być w posiadaniu podmiotów ubezpieczeniowych[16].

W zakres analizy ryzyka wpisuje się także jego szacowanie. Chodzi w tym o możliwie dokładne przedstawienie szansy na zmaterializowanie się konkretnego zagrożenia. Etap takich działań nie zostanie dobrze przeprowadzony, jeśli osoby odpowiedzialne za przeprowadzanie tytułowej analizy nie będą dysponować należytą wiedzą z zakresu podatności. W takim kontekście analiza ryzyka może być przeprowadzona przy wykorzystaniu metod ilościowych oraz jakościowych. Jeśli chodzi o te pierwsze to bazą zawsze są miary zdarzeń losowych. Wszystkim zagrożeniom przypisuje się ich prawdopodobieństwo wystąpienia z przedziału 0-1. Z kolei przy metodach jakościowych korzysta się z rozwiązań opisowych, próbując określić to, jak bardzo dany zasób systemowy jest podatny na konkretne zagrożenie. Zdarza się, że wynik takiej analizy będzie prezentowany na podstawie tabeli lub wykresu. Jest to podejście bardzo czytelne dla odbiorców, gdyż pozwala granicznie przedstawić wzajemne oddziaływanie zagrożeń. Na podstawie takiego wyniku dużo łatwiej jest opracować zbiór działań, które należy podjąć, aby dane zagrożenie, nie miało większego znaczenia dla poprawności działania systemu. W bardziej zaawansowanym podejściu spotkać się można z przypadkami, że poszczególne zagrożenia są opisywane według konkretnych parametrów. Jednym z takich parametrów jest uwzględnienie potencjalnych skutków finansowych, które mogą wystąpić, jeśli zagrożenie się zmaterializuje. Dokładnie chodzi o to, jakie koszty podmiot będzie musiał ponieść, aby przywrócić działanie systemu sprzed wystąpienia zagrożenia. Równie ważne jest liczbowe przedstawienie prawdopodobieństwa wystąpienia zagrożenia oraz opisanie okoliczności,

[16] Tamże, s. 80.

w których dane zagrożenie może mieć większe szanse na powstanie. Tym samym podmiot może decydować się na opisanie trzech różnych scenariuszy. Najbardziej niekorzystnego, optymalnego oraz mało znaczącego. Naturalnie najpoważniejsze konsekwencje, szczególnie te finansowe wystąpią w tym pierwszym scenariuszu[17].

Bardzo pomocne w analizie ryzyka jest bazowanie na przeszłości oraz obserwacji konkretnych zasobów, aby dało się następnie liczbowo przedstawić prawdopodobieństwo wystąpienia zagrożenia. Tutaj dobrym przykładem będzie odniesienie się do liczby prób kradzieży danego zasobu teleinformatycznego, przykładowo serwera w zadanym przedziale czasowym. Równie dobrze dokładnie w takim sam sposób analizie poddaje się ataki z przestrzeni publicznej realizowane przy wykorzystaniu Internetu. To właśnie te zagrożenia muszą być szczególnie dogłębnie przeanalizowane, gdyż zasoby teleinformatyczne w znacznym stopniu bazują na potencjale przestrzeni wirtualnej. W każdym z tych przypadków na bazie przeszłości precyzyjnie można określić koszty, jakie zostały poniesione, celem przywrócenia działania systemu. Mogło się zdarzyć, że pewna część systemu została zainfekowana, przez co należało jedynie odtworzyć go z kopii zapasowej. Dużo bardziej kosztowne są kradzieże lub uszkodzenia fizycznych zasobów, które trzeba kupić. W analizie ryzyka występują produkty wejściowe oraz wyjściowe. Produktem wejściowym jest przede wszystkim poziom bezpieczeństwa jakiego się oczekuje. W profesjonalnym podejściu nie można bazować jedynie na stwierdzeniu, że oczekuje się wysokiego bezpieczeństwa. Powinno zostać dokładnie wykazane to czego się oczekuje oraz na jakiego rodzaju zagrożenia zasoby teleinformatyczne nie powinny być podatne. Jeśli chodzi o parametry wejściowe to kluczowe są produkty wejściowe. W ich zakresie dość ważna jest lista zagrożeń oraz podatność systemu na wymienione zagrożenia. Za punkty wejściowe w analizie ryzyka uznaje się także listę zalecanych zabezpieczeń oraz określenie ryzyka szczątkowego. Po stronie wyjściowej uwzględnia się natomiast określenie standardów, według których będzie się postępować oraz określenie miary gwarancyjności odporności. Tym samym, jeśli dany zasób otrzyma określony status to powinien być odporny na zagrożenia z przyjętej listy[18].

Zbliżając się do końca podejmowanych rozważań w dziedzinie analizy ryzyka należy odnotować, że może być ona przeprowadzana na cztery różne sposoby. Jednym z wariantów jest analiza standardowa, w której to pozyskuje się, a następnie grupuje informacje o zagrożeniach. Dochodzi do tego uwzględnienie wymagań ochronnych dotyczących konkretnego systemu teleinformatycznego. Jeśli sytuacja tego wymaga to przeprowadza się modyfikacji i sprawdzania, jak zareaguje na konkretne zagrożenia. Sumarycznie można powiedzieć, że analiza standardowa opiera się na takich komponentach, jak: środki ochronne, podatność, obiekt oraz zagrożenie. Drugim wariantem jest

[17] Tamże, s. 85-86.
[18] Tamże, s. 86.

skorzystanie z analizy nieformalnej, w której to przeprowadza się na bazie posiadanej wiedzy, która aktualnie jest w posiadaniu pracowników. Najczęściej nie odnosi się ona do żadnych fundamentalnych standardów działania, przez co jej efekty mogą być nie zawsze takich, jakich się oczekuje. Dużo bardziej praktyczna jest szczegółowa analiza ryzyka. Jak sama nazwa wskazuje uwzględnia ona wymóg podjęcia szeregu działań, aby zbadać dosłownie każdy zasób informatyczny. W takim podejściu operuje się parametrami prawdopodobieństwa oraz podatności. Chodzi w niej o to, aby przeanalizować zagrożenia pod kątem potencjalnych strat, jakie mogą wystąpić. Ostatnim wariantem jest podejście mieszane, które charakteryzuje się największą praktycznością. To właśnie taką analizę da się dostosować do wymogów przedsiębiorstwa oraz specyfikacji samego systemu teleinformatycznego[19].

Zasady audytu

Proces audytowy

Audyt jest w istocie grupą czynności, które ze względu na swój charakter muszą być rozłożone w czasie. Już sam czynnik czasu powoduje, że do audytu można podchodzić, jak do procesu. Proces audytowy to po prostu uwzględnienie kilku kluczowych czynności, które co do zasady powinny być przeprowadzane w ściśle określonej kolejności. Jedną z ważniejszych czynności w procesie audytowym jest sporządzenie listy audytowej. Naturalnie taka lista musi być zawsze tworzona według uprzednio wybranego standardu. Jeśli przykładowo zostanie wybrany standard o oznaczeniu BS 7799 to lista audytowa składać się będzie aż ze 127 punktów. Jednak wcale nie jest to najbardziej wymagający standard, gdyż jeśli zostanie podjęta decyzja, aby działać w oparciu o standard COBIT 4.0 to taka lista będzie składać się aż z 214 punktów. Warto tutaj odnotować, że niezależnie od wybranego standardu każdy z podpunktów będzie opisany specjalnym komentarzem. Najczęściej spotka się podział na cztery opisy, wśród których uwzględnia się status: spełniony, niespełniony, częściowo spełniony lub nie dotyczy. Takie wypełnianie listy audytowej będzie odbywać się na podstawie wywiadów, wizji lokalnej lub po prostu analizy dokumentów będących w dyspozycji instytucji. Równie dobrze, celem poprawy wiarygodności przypisywanych statusów można posłużyć się testami kontrolnymi. Na proces składają się również czynności podejmowane w ramach badania systemu ochrony fizycznej i technicznej. Przy czym takie testy muszą być przeprowadzone w oparciu o specjalistyczne narzędzia, również takie o potencjale penetracyjnym. Co do zasady testy penetracyjnie nie wpisują się w zakres przeprowadzanego audytu, a stanowią jedynie pomocniczą bazę do wyprowadzenia bardziej miarodajnych wniosków. Po przeprowadzeniu takich testów zawsze proces audytowy powinien kończyć się sporządzeniem raportu. Tym samym przy jego pomocy dokumentuje się czynności, które zostały podjęte oraz prezentuje wyniki i wnioski, które powinny dać sugestie

[19] Tamże, s. 124.

przedsiębiorstwu, co do dalszych działań. Taki raport uzna się za rzetelny tylko wówczas, gdy znajdą się pod nim podpisy wszystkich osób biorących udział w audycie[20].

Fazy audytu

Wiedząc, że audyt jest procesem naturalnie na myśl przychodzą jego fazy, w których podejmowane są konkretne działania. Zależenie od podejścia liczba faz w audycie może być różna, jednak najczęściej będzie to tylko kilka etapów. Chociaż zdarzają się i takie standardy, które wyliczają aż kilkanaście faz. Dla przykłady standard COBIT wskazuje na występowanie tylko pięciu faz, które zawsze muszą zachodzić w tej samej kolejności. Pierwszą fazą jest zapoznanie się z procesem audytowym. Przede wszystkim w tej fazie analitycy mają za zadanie zapoznać się z zaprojektowanymi mechanizmami kontrolnymi w ramach istniejącego systemu. Przy czym wiedza z tego zakresu powinna być możliwie rozbudowana, co przełoży się na sprawność podejmowania kolejnych czynności. Drugą fazą jest ocena mechanizmów kontrolnych. Na tym etapie ocenie poddawana jest rzetelność oraz efektywność systemu kontrolnego. Etap trzeci to ocena zgodności. Jak sama nazwa wskazuje w tej fazie chodzi o sprawdzenie stopnia wdrożenia mechanizmów kontrolnych. Jest to etap bazujący głównie na dostarczonej wraz z systemem dokumentacji, przez co sprawdza się, czy wszystkie podpunkty będące założeniami faktycznie zostały zaimplementowane na rzecz systemu. Czwartą fazą jest ocena ryzyka. W tym zakresie wyszukiwane są dowody mające świadczyć o tym, że w systemie występują pewne braki, a tym samym może stanowić to ryzyko dla zasobów przetwarzanych przez system. Szczególny nacisk kładziony jest na błędy strukturalne oraz te zachodzące podczas tworzenia systemu. Jest to bardzo ważna część audytu, gdyż pominięcie potencjalnych błędów mogłoby wpłynąć niekorzystnie na zakładane cele biznesowe. Ostatnią fazą jest określenie osiągania celów. Jest to po prostu faza zmierzająca do stworzenia raportu końcowego. W takim raporcie kluczowe jest to, aby ocenić poziom osiągnięcia badanych celów, a tym samym aspekty bezpieczeństwa[21].

Nieznacznie inaczej fazy audytu przedstawią się, jeśli będzie się postępować według zaleceń metodyki LP-A. W takim przypadku wszystko rozpoczyna się od spotkania wstępnego, które ma posłużyć do skompletowania zespołu odpowiedzialnego za przeprowadzenie audytu. Bardzo często będą to osoby niepowiązane z przedsiębiorstwem, przez co wymagane jest sporządzenie specjalnej umowy pomiędzy stronami. Chodzi o to, że w czasie takiego audytu uzyskiwany jest dostęp do danych wrażliwych. Samo spotkanie wstępne jest odpowiedzią na zapytanie ofertowe oraz dostarczone dokumenty uwierzytelniające zespół audytowy. Efektem zakończonego spotkania wstępnego powinien być stworzony zakres upoważnień oraz zarządzenie o audycie, a także zarządzenie o seminarium. W trzecim kroku podejmowanych działań

[20] Tamże, s. 135.
[21] Tamże, s. 135.

przechodzi się do badania na zgodność ze standardem. Chodzi w tym o to, aby sprawdzić, czy analizowany system został stworzony tak, jak to pierwotnie zakładano. Sprawdzenia dokonuje się na podstawie kwestionariuszy audytowych oraz dokumentacji porządku prawnego. Czynność ta finalizowana jest raportem końcowym z audytu od zgodności z normą. W kolejnym kroku przechodzi się do bania ochrony systemu oraz podłączonej do niej sieci, co jest przeprowadzane na bazie dokumentacji technicznej. Podobnie, jak w poprzednim etapie również tutaj tworzony jest raport końcowy z badań technicznych. Na bazie dwóch poprzednich raportów opracowywany jest dokument końcowy z audytu. Wszystko finalizowane jest odbiorem wyników audytu, co zostało uwzględnione w dokumencie odbioru[22].

Wykorzystanie oprogramowania narzędziowego w audycie

Audyt ukierunkowany na systemy teleinformatyczne wykorzystuje kilka narzędzi o charakterze sprawdzającym. Jest tym po prostu specjalistyczne oprogramowanie narzędziowe. Dodatkowo osoba wykonująca zadania audytorskie powinna posiadać należytą wiedzę z zakresu systemów informatycznych. Szczególny nacisk powinien być położony na wiedzę o systemach z rodziny Unix, Windows oraz MVS. Ta wiedza powinna dotyczyć głównie umiejętności wyszukiwania słabych punktów systemów, działających w oparciu o taką architekturę. Co prawda audyt może być przeprowadzony bez korzystania ze specjalistycznego oprogramowania, ale wówczas będzie on niepełny. Oprogramowanie będzie stanowić narzędzie wspomagające oraz dające pewność, że testowany system jest faktycznie bezpieczny. Co warte odnotowania takich narzędzi jest kilkadziesiąt różnych rodzajów, co jeszcze bardziej może utrudniać zadanie audytorowi, który musi zdecydować się na wybór najbardziej adekwatnych do zadanego systemu. Przy ich wyborze zawsze należy bazować na osobistej wiedzy oraz czasie, który został przeznaczony na potrzeby audytu. Pobocznym czynnikiem może być dostępność konkretnego oprogramowania audytowego. Niezależenie od wybieranego narzędzia zawsze należy posługiwać się pewnym algorytmem działania. Wszystko rozpoczyna się od oceny własnych wymagań w stosunku do takich narzędzi. Następnie sprawdzana jest funkcjonalność oprogramowania, na które się zdecydowało oraz jego testowanie zgodności z oczekiwaniami. Dopiero po tych działaniach konkretne narzędzie może być włączone do audytu[23].

Jedną z grupą narzędzi są komputerowe techniki wspomagania audytu, w skrócie nazywane CAATs. W ramach tego narzędzia uwzględnia się: procedury analityczne, próbkowanie oraz testowanie szczegółów transakcji. Pomocne może być również oprogramowanie służące do testowania włamań, co symulować będzie potencjalne ataki na system. Takie narzędzie bardzo dobrze sprawdzi się przy sprawdzaniu aplikacyjnych mechanizmów kontrolnych oraz

[22] Tamże, s. 142.
[23] M. Molski, M. Łacheta, *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2014, s. 340.

ponownym przeliczaniu operacji realizowanych przez systemy księgowe. Takie narzędzie wymaga poświęcenia bardzo małych zasobów czasowych, co przekłada się na ograniczenie kosztów. Dodatkowo nie ma potrzeby bazowania na próbkach, gdyż takie narzędzie bada system kompleksowo. Wystarczy jedynie ustalić wymagania początkowe oraz sformułować procedury przetwarzania, aby otrzymać wynik audytu[24].

W niektórych przypadkach sprawdzą się uniwersalne programy audytowe (GASP). Przy pomocy takiego oprogramowania w systemie możliwe jest wyszukanie niewyjaśnionych różnic oraz porównanie danych w systemach o podobnych profilach. Ma to na celu ułatwienie znalezienia ewentualnych defektów. Co do samej architektury systemowej również i w tym aspekcie narzędzie może się sprawdzić wykazując poprawność powiązań pomiędzy zaimplementowanymi obiektami. Dochodzi do tego możliwość zlokalizowania anomalii lub operacji, które nie powinny mieć miejsca. Tym samym lokalizowane są przyczyny powstawania nieoczekiwanych transakcji. Wartym odnotowania jest fakt, że takie narzędzie sprawdzi się do audytowania systemów, które działają już pewien czas, gdyż pozwalają wykazać trendy w szerszych przedziałach czasowych. Potencjał takiego narzędzia odnosi się również do możliwości wyszukiwania istotnych danych przy pomocy: sortowania, próbkowania lub filtrowania. W praktycznym ujęciu w tej grupie audytorzy najchętniej korzystają z takich programów, jak: IDEA oraz ACL. Co ciekawe takie oprogramowanie dostępne jest w wariancie licencjonowanym lub w wersji demo, co również pozwala audytować systemy. W przypadku oprogramowania ACL możliwe jest kontrolowanie integralności oraz zgodności z przyjętymi standardami. W przypadku tej pierwszej kontroli sprawdzana jest kompletność systemu, jego unikatowość, prawidłowość zaimplementowanych relacji oraz czy nie występują jakieś uszkodzenia. Z kolei podczas kontroli zgodności sprawdza się, jak system reaguje na komendy, zmienne oraz wyrażenia. System poprzez podjętą analizę dostarcza raport, który później może być przetworzony przez audytora[25].

Jeśli zachodzi potrzeba przebadania funkcji systemów informatycznych to bardzo dobrze sprawdzą się narzędzia określane mianem testów mechanizmów kontrolnych. Są to narzędzia, z których korzysta się, jeśli zachodzi potrzeba przeprowadzenia testów zgodności lub testów dowodowych. W tym pierwszym przypadku oprogramowanie pozwala odpowiedzieć na pytanie, czy wszystkie funkcje zaimplementowane w systemie działają dokładnie w taki sposób, jak sugeruje o tym dokumentacja. Z kolei przy testach dowodowych chodzi o wykazanie poprawności przeprowadzanych przez system transakcji. Takie oprogramowanie ma potwierdzić, czy system operuje danymi w sposób wiarygodny i czy nie dostarcza użytkownikom zafałszowanych wyników. Przy

[24] Tamże, s. 341.
[25] Tamże, s. 342.

pomocy takich testów sprawdza się także to, jak system reaguje na skróty klawiszowe, czy nie powoduje to jakichś błędów[26].

Certyfikowanie

Certyfikacja urządzeń i narzędzi oraz środków przeznaczonych do ochrony informacji niejawnych

Urządzenia mające przetwarzać informacje niejawne muszą posiadać odpowiednie certyfikaty, co będzie potwierdzeniem tego, że przy ich pomocy można bezpiecznie operować danymi wrażliwymi oraz tajnymi. Co do samej certyfikacji to jest to proces, który kończy się przyznaniem określonej klasy certyfikatu dla konkretnego urządzenia. Jeśli dane narzędzia wykazują jakiekolwiek powiązania z zasobami kryptograficznymi to istnieje możliwość przydzielenia im jednego z trzech rodzajów certyfikatów. Wśród nich uwzględnia się certyfikat typu „T". Urządzenie z takim oznaczeniem będzie posiadać potwierdzenie, że może chronić informacje niejawne. Jeśli dane urządzenie wcześniej miało przyznany już jakiś certyfikat i dalej wykazuje ono funkcje ochronne to przypisuje się mu certyfikat zgodności oznaczany literą „Z". Uzupełnienie w tej grupie stanowią certyfikaty przyznawane urządzeniom, które operują informacjami niejawnymi posiadającymi status zastrzeżonych. Zgodnie z rozporządzeniem nr 45 szefa ABW z dnia 17 sierpnia 2012 roku w sprawie certyfikacji urządzeń, narzędzi oraz środków przeznaczonych do ochrony informacji niejawnych możliwe jest również przyznawanie certyfikatów dla środków ochrony elektromagnetycznej oraz dla urządzeń, które pełnią funkcje typowo zabezpieczające. Co do samej procedury certyfikacyjnej może być ona wyraźnie rozłożona w czasie, gdyż sam proces certyfikacji może się rozpocząć nawet do 3 miesięcy od dnia złożenia wniosku. Takiej certyfikacji dokonuje jednostka certyfikująca wraz z zespołem badawczym. Jeśli komisja uzna taką potrzebę to do podmiotu, który dysponuje danym urządzeniem może się zgłosić z prośbą o jego zaprezentowanie. Tym samym podczas faktycznej pracy sprawdzane jest to, czy dane urządzenie działa prawidłowo i mechanizmy zabezpieczające w nim zastosowane są wystarczające. Może także zaistnieć potrzeba dostarczenia dokumentacji uzupełniającej, aby mieć pewność, że przyznany certyfikat jest zasadny. Naturalnie, aby proces certyfikacji mógł się zakończyć pozytywnie to niezbędne jest zatwierdzenie przez podmiot certyfikujący wszystkich dostarczonych materiałów. Nawet jeśli jeden dokument opisujący działanie urządzenia nie zostanie zatwierdzony to certyfikat nie zostanie przyznany. Jest to na tyle istotna kwestia, że wszystkie etapy podejmowanych działań muszą być udokumentowane. Do tego cały zespół w terminie do 30 dni od faktycznie przeprowadzonego badania urządzenia musi dostarczyć przedsiębiorstwu szczegółowy raport. Z technicznego punktu widzenia za wydawanie certyfikatów ochrony kryptograficznej odpowiada szef ABW. Jednak, jeśli ma zostać wydany certyfikat zgodności, to za takie czynności będzie

[26] Tamże, s. 345.

odpowiadać Dyrektor ABW. W każdym z tych przypadków wydanie certyfikatu będzie mogło nastąpić dopiero po uregulowaniu stosownej opłaty. W szczególnych przypadkach Szef ABW może zlecić badanie narzędzia lub urządzenia podmiotowi zewnętrznemu. Jednak takie badanie musi być przeprowadzone według dokładnych wytycznych Szefa ABW. Jeśli jakieś urządzenie operujące na danych zastrzeżonych otrzymało już certyfikat od krajowej władzy bezpieczeństwa państwa to ABW oraz SKW nie przeprowadzają dodatkowych badań[27].

Reasumując certyfikacja stanowi ostatni element procesu akredytacji bezpieczeństwa teleinformatycznego. W ramach certyfikacji wyrobów SKW oraz ABW prowadzi procesy zarówno certyfikacji typu oraz certyfikacji zgodności. Następnie wydawane są zależnie od typu, rodzaje odpowiednich certyfikatów. W rodzaje certyfikatów wydawanych przez SKW wpisują się: Certyfikat Ochrony Kryptograficznej, Certyfikat Bezpieczeństwa Teleinformatycznego oraz Certyfikat Ochrony Elektromagnetycznej. Reasumując certyfikacja jest procedurą potwierdzającą bezpieczeństwo funkcjonowania systemów, a dokładniej komponentów sprzętowych działających w jego zakresie.

Metodologia

Praca została napisana w oparciu o dogłębną analizę literatury z przedmiotu bezpieczeństwa przetwarzania danych, systemów teleinformatycznych oraz sposobów ich audytowania i certyfikowania. Ponadto w pracy zwrócono uwagę na obowiązujące akty prawne oraz standardy z zakresu bezpieczeństwa teleinformatycznego. Dzięki temu udało się zrealizować główny cel pracy, którym było: zbadanie istoty audytu i certyfikacji wojskowych systemów teleinformatycznych. Problem audytu wydaje się byś zasadny do pojęcia, gdyż pośrednio chodzi o ludzkie bezpieczeństwo. Praca w obszarze audytu oraz certyfikacji systemów teleinformatycznych bazuje wyłącznie na źródłach wtórnych, którymi są pozycje książkowe z rozpatrywanego zagadnienia.

Przegląd literatury

Praca opiera się głównie na literaturze z zakresu bezpieczeństwa przetwarzania informacji oraz sposobach audytowania i certyfikacji systemów teleinformatycznych. Zaprezentowane zostały zagadnienia dotyczące polityki bezpieczeństwa informacji, w co wpisuje się wyjaśnienie istoty informacji oraz opisanie elektronicznych metod ich przetwarzania. Uzupełnienie w tym zakresie stanowią regulacje prawne takie jak: Ustawa z dnia 5 sierpnia 2010 r. *o ochronie informacji niejawnych* (Dz.U. 2010 nr 182 poz. 1228) oraz Zarządzenie nr 45 szefa ABW z dnia 17 sierpnia 2012 roku *w sprawie certyfikacji urządzeń, narzędzi oraz środków przeznaczonych do ochrony informacji nie-*

[27] Zarządzenie nr 45 szefa ABW z dnia 17 sierpnia 2012 roku *w sprawie certyfikacji urządzeń, narzędzi oraz środków przeznaczonych do ochrony informacji niejawnych*.

jawnych. Ponadto zawarte zostały źródła odwołujące się do procesu akredytacji bezpieczeństwa teleinformatycznego. Rozważania w tym zakresie rozpoczyna się od wyjaśnienia, czym jest akredytacja oraz jak klasyfikuje się zasoby zaliczanie do systemu teleinformatycznego. Dochodzi do tego złożony proces audytu, a także dokumentacja opisująca bezpieczeństwo systemu teleinformatycznego. W niniejszą sferę wpisują się następujące pozycje: Iwaszko B., *Ochrona informacji niejawnych w praktyce*, PWN, Warszawa 2014 oraz Liderman K., *Bezpieczeństwo informacyjne - nowe wyz*wania, PWN, Warszawa 2014. Dopełnienie pracy stanowi zaprezentowanie procesu zarządzania ryzykiem wraz z metodami jego szacowania. Szczególny nacisk został położony na metodę jakościową oraz ilościową. Przestawienie tematyki z tego zakresu bazuje na książce: Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008.

Wnioski

Przeprowadzona analiza oraz badanie literatury pozwoliła na dokonanie następujących wniosków:

1. Audyt i certyfikacja są działaniami o charakterze procesowym, gdzie poszczególne czynności są wyraźnie rozłożone w czasie. Audyt musi być tak złożony i rygorystyczny, gdyż wojskowe systemy teleinformatyczne przetwarzają nierzadko szczególnie wrażliwe dane. Proces ten powinien opierać się jedynie na ściśle określonych i rygorystycznych normach z zakresu bezpieczeństwa przetwarzania danych. Jak to zostało wykazane, niewykryte błędy na etapie audytu oraz dalej certyfikacji mogłyby doprowadzić do sytuacji, w której nieodpowiednio zabezpieczony system odpowiadałby za przetwarzanie wrażliwych danych, które mogłyby być ważne nawet z punktu widzenia państwa.
2. Niniejsza praca pozwoliła zrozumieć to, jak cennym zasobem w XXI wieku jest informacja. O takie zasoby należy odpowiednio dbać oraz starać się je chronić wszelkimi dostępnymi sposobami. Pomimo tego, że na rynku dostępnych jest wiele zabezpieczeń z zakresu bezpieczeństwa teleinformatycznego to cały czas prowadzone są prace nad nowymi. Wynika to głównie ze względów bezpieczeństwa, gdzie oczekuje się jeszcze doskonalszego zabezpieczenia danych przetwarzanych przez takie systemy.
3. Pozytywnym aspektem certyfikacji jest to, że pozwala wykorzystywać wyłącznie te rozwiązania systemowe, które faktycznie się sprawdzają i zapewniają pożądany poziom bezpieczeństwa. Certyfikacja zapewnia również większe poczucie bezpieczeństwa dla użytkowników wiedząc, że wykorzystywane systemy teleinformatyczne przeszły pozytywnie audyt oraz okresową procedurę certyfikacji.
4. Zagrożenia bezpośrednio oddziałujące na bezpieczeństwo przetwarzania danych oraz systemy teleinformatyczne pozwalają poszukiwać nowych rozwiązań w dziedzinie bezpieczeństwa.

Bibliografia

Opracowania zwarte

1. Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2003.
2. Iwaszko B., *Ochrona informacji niejawnych w praktyce*, PWN, Warszawa 2014.
3. Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Warszawa 2008.
4. Liderman K., *Bezpieczeństwo informacyjne - nowe wyz*wania, PWN, Warszawa 2014.
5. Molski M., Łacheta M., *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2014.

Akty prawne

1. Zarządzenie nr 45 szefa ABW z dnia 17 sierpnia 2012 roku w sprawie certyfikacji urządzeń, narzędzi oraz środków przeznaczonych do ochrony informacji niejawnych.

bsmt pchor. Marlena DYMOWSKA

INŻYNIERIA SPOŁECZNA W ATAKACH HAKERSKICH

Streszczenie

Niniejsze opracowanie dotyczy technik inżynierii społecznej, jakimi posługują się współcześni cyberprzestępcy oraz jak wykorzystują je w swoich atakach. W pracy wyjaśniono definicje, które odnoszą się do tematu. Przedstawiono podstawowe pojęcia z zakresu socjotechniki i reguł wywierania wpływu, które stosowane są w życiu codziennym oraz przez socjotechników. Zwrócono uwagę na podział zagrożeń występujących w Internecie oraz jakie skutki mogą nieść za sobą zbyt szybkie decyzje w sieci. Omówiono jak negatywny wpływ mają zagrożenia na ludzkie zachowanie i psychikę. W pracy ustalano możliwe sposoby obrony przez atakami. Praca koncentruje się na zagadnieniu stosowania technik socjotechnicznych w atakach hakerskich. Wskazuje w jaki sposób atakujący dzięki wykorzystaniu inżynierii społecznej dokonują czynów zabronionych i atakują użytkowników Internetu.

Słowa kluczowe:
inżynieria społeczna, socjotechnika, atak hackerski, socjotechnik, reguła socjotechniczna, atak socjotechniczny, cyberprzestępca, cyberprzestrzeń.

Abstract

Social engineering in hacker attacks

The aim of the work was to present the social engineering techniques used by modern cybercriminals and how they use them in their attacks. The work explains the definitions, I'll break out the topic. The basic principles of social engineering and the standards of exerting influence, which are used in everyday life and by social engineers, were presented. Attention was paid to the use of results occurring on the Internet and what they can bring too fast on the web. The negative influence of threats on human behavior and psyche is discussed. Possible methods of defense against attacks were determined in the work. The work focuses on the use of social engineering techniques in hacking attacks. Work on how social engineering attackers commit bans and attack Internet users.

Keywords:
social engineering, social engineering, hacking attack, social engineering, social engineering rule, social engineering attack, cybercriminal, cyberspace.

Wstęp

W obecnych czasach świat szybko rozwija się. Z dnia na dzień pojawiają się nowe odkrycia i wynalazki, które mają za zadanie polepszyć i ułatwić życie społeczeństwa. Jednak coraz to większą część życia ludzi stanowią media społecznościowe, cyfrowe oraz mobilne. Już ponad 4,5 miliarda ludzi na świecie korzysta z Internetu, a liczba użytkowników mediów społecznościowych przekroczyła już 3,8 miliarda. Prawie 60% światowej populacji jest już online[1].

Internet powstał na koniec 1969 roku. Na początku miał funkcjonować tylko na potrzeby wojska. Udoskonalanie sieci trwało wiele lat, aż w 1990 r. ARPANET[2] został zlikwidowany, a jego miejsce zastąpił Internet, który istnieje do dziś. Wraz z biegiem lat, Internet przynosił coraz to nowe korzyści oraz możliwości. To sprawiło, że cieszył się coraz to większą sławą. Ludzie zaczęli korzystać z mediów społecznościowych, słuchać muzyki, oglądać filmy, a także szukać ciekawych informacji w wyszukiwarce.

Wraz z rozwojem technologii, rozwinęły się również zagrożenia, które czekają na użytkowników Internetu. Coraz częściej przestępstwa przenoszą się z prawdziwego życia do sieci. Co najgorsze liczba przestępstw rośnie i rozwija się z niesamowitą prędkością, wraz z umiejętnościami cyberprzestępców. Z powodu pojawiania się nowych niebezpieczeństw, które stanowią wielki problem, pojawiły się nowe techniki, jaki i dziedziny nauki, które mają zdefiniować, reagować oraz zapobiegać negatywnym zdarzeniom, które mają miejsce w Internecie.

Jak stosowana jest inżynieria społeczna w atakach hakerskich? Ataki z użyciem technik inżynierii społecznej, są podstępne, często przygotowywane przez długi czas. Osoby, które stają się ofiarami takich ataków, zwykle nie mają o tym pojęcia, ponieważ są manipulowane i nawet nie zdają sobie sprawy, że gdyby nie wpływ, odpowiednie użycie słów głosu, bądź po prostu podszycie się pod odpowiednią osobę, nie spełniłyby oczekiwanego żądania, nakazu. Zwykle ataki z użyciem socjotechniki prowadzą do utraty dostępu do konta społecznościowego bądź przejęcia całego komputera, w najgorszym przypadku do utraty całych funduszy z konta lub permanentnego dostępu do niego.

Jak brzmią główne pojęcia odnoszące się do inżynierii społecznej? Pojęcia przedstawione w rozdziale pierwszym, są terminami, które najlepiej obrazują, czym jest właściwie inżynieria społeczna oraz jak działa. Reguły socjotechniczne pokazują, że nie musi się ona odnosić tylko do złego, może być stosowana także w dobrych intencjach, na co dzień, przez bliskie osoby, albo przez sklepy, by nakłonić do kupna produktu. Jednak socjotechnika ma drugie dno i może doprowadzić wielu nieprzyjemnych sytuacji.

---

[1] https://mobirank.pl/2020/01/31/raport-digital-i-mobile-na-swiecie-w-2020-roku/, dostęp: 12.01.2021 r.

[2] Pierwsza sieć rozległa oparta o rozproszoną architekturę i protokół TCP/IP. Jest bezpośrednim przodkiem Internetu, *https://pl.wikipedia.org/wiki/ARPANET,* dostęp: 12.01.2021 r.

Jak dzielimy ataki hakerskie? Zagrożeń w sieci jest mnóstwo i niestety będzie coraz więcej. Każdy atak jest groźny. Niektóre z nich mogą doprowadzić do bankructwa, śledzenia naszych ruchów w sieci, są to np.: keyloggery, robaki, trojany itp. Istnieją też takie niebezpieczeństwa, które powodują problemy psychiczne i powodują problem, które w stanie będzie rozwiązać tylko psycholog. Przykładem takiego zagrożenia jest cyberstalking.

Jakie ataki socjotechniczne stosowane są w cyberprzestrzeni? Dzięki metodom inżynierii społecznej, ataki są o wiele bardziej skuteczne. Wskazanymi atakami, w których używane są techniki manipulacji oraz wpływu są: phishing, zjawisko deepfake, pretexting oraz dezinformacja. W niniejszym opracowaniu zwrócono uwagę na to jak te ataki wpływają na emocje, zachowania i odczucia odbiorców.

Głównym celem pracy jest przedstawienie metod inżynierii społecznej wykorzystywanych przez hakerów do przeprowadzenia skutecznych ataków. W pracy zostały wyjaśnione definicje, które odnoszą się do wybranego tematu.

Temat pracy *Inżynieria społeczna w atakach hakerskich* został wybrany, ze względu na coraz większą popularność Internetu na świecie, z powodu korzyści, jakie przynosi użytkownikom. Przynosi jednak również wiele nieprzyjemnych sytuacji, czego niestety duża część społeczeństwa nie jest świadoma. Jeden nieodpowiedni krok, utrata pieniędzy i dostępu do wszystkich kont i problem przedostaje się do prawdziwego życia.

Podstawowe pojęcia w inżynierii społecznej

Inżynieria społeczna, zwana również socjotechniką, jest to zbiór wielu różnych technik, za pomocą, których można wywierać wpływ, manipulować lub skłonić społeczeństwo do podjęcia decyzji, których świadomie sam nikt by nie podjął. Socjotechnika opiera się na ludzkich emocjach tj.: smutek, współczucie i stara się uśpić ludzki rozum. Dąży również do wykorzystania małej wiedzy najsłabszego ogniwa bezpieczeństwa, jakim są ludzie i nakłonić ich do wyjawienia potrzebnych informacji. Należy zauważyć, że socjotechnika nie musi być używana tylko w złych celach, może posłużyć do zmotywowania kogoś do czegoś, np.; do porzucenia uzależnień. Socjotechnika jest integralnym elementem codziennego życia. Korzysta z niej każdy, rozpoczynając od małych dzieci, które próbują nakłonić dziadków, aby kupili im lizaka, kończąc na lekarzach bądź politykach.

Inżynieria społeczna opiera się przede wszystkim na wywieraniu wpływu, czyli sztuce perswazji. Polega ona na oddziaływaniu na osobę, aby zechciała wykonać i uwierzyć w to, czego oczekuje osoba wywierająca wpływ. Perswazja jest procesem niezauważalnym, dla ofiary, nie jest ona świadoma tego, że gdyby nie odpowiednie metody wywierania wpływu, nigdy nie byłoby to w jej interesie i nie zgodziłaby się podjąć narzucanych jej działań i poglądów. „Wywieranie wpływu i perswazję można podzielić na pięć istotnych aspektów. Pięć podstawowych czynników perswazji ma kluczowe znaczenie w każdym przypadku wywierania wpływu na ofiarę:

- wyznaczanie jasnych celów,
- wypracowanie porozumienia,
- uważne obserwowanie otoczenia,
- elastyczność,
- samoświadomość”[3].

Wymienione czynniki mają ogromne znaczenie, aby zrozumieć sztukę perswazji, pomagają na osiągnięcie celu i wykonanie przez ofiarę to, czego się od niej oczekuje.

Inżynier społeczny może posługiwać się również manipulacją, która polega na wywieraniu wpływu, polegającym na celowym oszukaniu osoby lub społeczeństwa. Te działania służą do tego, aby skłonić ludzi do zachowania, które nie wpłynie pozytywnie na ich dobro i interes.

Skuteczność manipulacji społeczeństwem zależy od bezwzględności osoby manipulującej oraz od tego jak osoba lub grupa osób są podatni na atak. Manipulująca osoba, dąży za wszelką cenę ku osiągnięciu wyznaczonego celu. Im większy cel, tym większa skłonność do wykorzystania słabości ofiary np.: trudnej sytuacji finansowej bądź rodzinnej. W większości ataków socjotechnicznych ofiara zostaje wprowadzana w błąd przez manipulację emocjonalną, która daje socjotechnikowi przewagę w każdej interakcji. W podwyższonym stanie emocjonalnym jest bardziej prawdopodobne to, że ofiara podejmie nieracjonalne i nierozsądne działania. Aby przekonać ofiarę napastnik, wykorzystuje takie emocje jak: strach, podniecenie, wina, smutek oraz gniew. Socjotechnikiem nazywamy osobę, która za pomocą manipulacji, wydobywa od innych informacje. Posiada ona wiedzę o psychice ludzkiej oraz technikach inżynierii społecznej.

Techniki, które pomagają socjotechnikowi w jego działalności to m.in. manipulacja, sztuka perswazji oraz neurolingwistyczne programowanie. Wszystkie trzy wymienione techniki pomagają inżynierowi społecznemu sterować swoimi ofiarami i uzyskiwać od nich wiele informacji, a także nakłaniać do wykonania pewnych nieświadomych czynności. Może to być ujawnianie loginów i haseł, wyjawienie poufnych informacji na temat firmy lub przekazanie ważnych dokumentów, w zależności, jakie informacje w danej chwili są potrzebne oszustowi.

Dobry socjotechnik jest elastyczny, płynnie dostosowuje się do prowadzonej rozmowy, dokładnie słucha swoją ofiarę i każde słowo wykorzystuje do spełnienia swoich celów. Dobre aktorstwo jest kolejną potrzebną cechą dla socjotechnika, musi on wcielać się w różne role i za pomocą reguły autorytetu, która została wspomniana już we wcześniejszych podrozdziałach może zdziałać cuda. Warto wspomnieć, że oszust nie musi wykorzystywać komputerów do uzyskania ważnych informacji. Wystarczy zwykła rozmowa przez telefon,

[3] Ch. Hadnagy, *Socjotechnika. Sztuka zdobywania władzy nad umysłami,* Helion, Gliwice 2012, s. 222.

podczas której socjotechnik może wyciągnąć od ofiary hasło do np. komputera. Udać może mu się to, gdy użyje reguły autorytetu i zadzwoni do ofiary, jako dyrektor firmy i natychmiast zażąda hasła do komputera. Udawanie gniewu i podniesienie głosu, potęguje wagę sytuacji i w tym momencie ofiara niema wyjścia i podaje oczekiwane od niej informacje. Połączenie dobrej gry aktorskiej, wykorzystanie strachu ofiary oraz zasugerowanie, co może wiązać się z niespełnieniem żądania socjotechnika zwykle prowadzi do pomyślnego zrealizowania celu oszusta.

Podział i charakterystyka wybranych ataków hakerskich

Codziennie dostęp do sieci mają miliony ludzi na świecie. Z Internetu korzystają małe dzieci, nastolatkowie, dorośli oraz osoby starsze. Internet służy do komunikacji, pracy, nauki, robienia zakupów, wykonywania opłat za prąd, wodę itp. oraz do innych codziennych czynności.

Poza dobrami, z których korzysta każdy człowiek w sieci występują też niebezpieczeństwa, na które zawsze warto być przygotowanym. Do grupy niebezpieczeństw można zaliczyć ataki przeprowadzone z pomocą złośliwego oprogramowania, wirusów komputerowych, programów, które mają na celu kradzież danych lub wyłudzanie pieniędzy. Jednak poza niebezpieczeństwami typowo technicznymi istnieje również te na poziomie psychologicznym. Przykładami zagrożeń, które mogą wyrządzić krzywdę na poziomie psychologicznym są:

- **Cyberstalking -** forma nękania drugiego użytkownika za pomocą nowoczesnych technologii. „Stalking rozumiany jest, jako złośliwe i powtarzające się nagabywanie, naprzykrzanie się, które wywołać może u ofiary poczucie zagrożenia. Obejmuje ono zachowania polegające na obsesyjnym śledzeniu, obserwowaniu albo kontaktowaniu się z inną osobą wbrew jej woli”[4]. W taki sposób osoba stalkująca chce zmusić swoją ofiarę do zachowania się w konkretny sposób. Przemoc werbalna, zamieszczanie negatywnych postów na portalach społecznościowych, krzywdzących zdjęć i filmów potrafi wywołać nieusuwalne i negatywne skutki dla psychiki ofiary, a nawet doprowadzić do targnięcia na swoje życie.
- **Flaming** (ang. *flame war*) czyli wojna na obelgi jest to kolejny rodzaj cyberprzemocy. Pod tym terminem kryje się celowe „zaognianie” wymiany zdań między użytkownikami w serwisach dyskusyjnych i społecznościowych[5]. Atak ten polega na wybuchu agresji i wycofaniu się z rzeczywistego tematu rozmowy w kierunku wyzwisk, przekleństw i gróźb.

[4] http://nawokandzie.ms.gov.pl/numer-3/wokanda-3/paragraf-na-stalkera.html, dostęp: 10.12.2020 r.

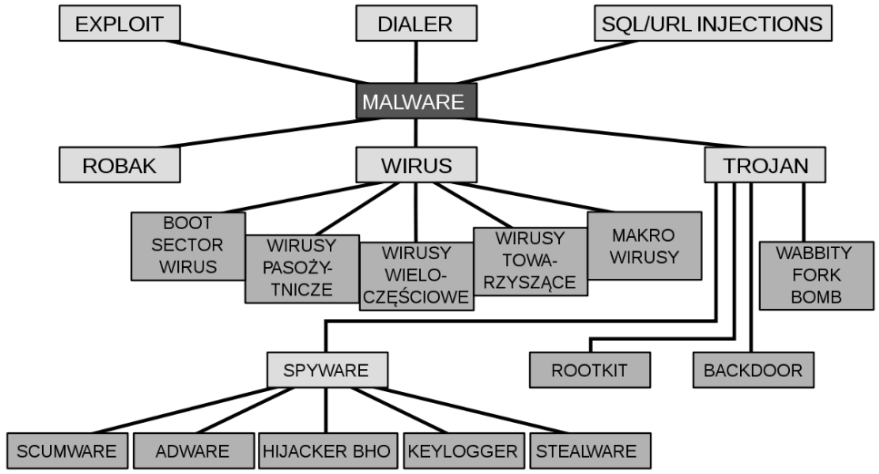
[5] http://uzaleznienie.com.pl/siecioholizm/poradnik-dla-rodzicow-d4/sexting-stalking-flaming-niebezpieczenstwa-czyhaja-w-sieci/, dostęp 10.12.2020 r.

- **Child grooming.** Tak nazywany jest cały proces, podczas którego osoba dorosła „przygotowuje" dziecko do wykorzystania seksualnego[6]. Początkowy etap polega na nawiązaniu znajomości i zaprzyjaźnieniu się z dzieckiem, a następnie nawiązaniu silnej relacji, aby ofiara stała się uzależniona od swego oprawcy. To wszystko ma na celu doprowadzenie do wykorzystania seksualnego dziecka i produkcji pornografii z jego udziałem.
- **Ruch - Pro-ana.** Jest to świadome promowanie anoreksji, jako pożądanego stylu życia oraz negowanie faktu, że anoreksja jest chorobą. Wyznawczynie tego stylu życia nazywają się „motylkami". Nazwa Pro-ana wywodzi się od wyrazu anoreksja, czyli zaburzenia odżywiania, które polega na chorobliwym głodzeniu się. Znakiem rozpoznawczym „motylków" jest dekalog pro-ana, który zaczyna się hasłem: „Jeśli nie jesteś szczupła, to znaczy, że nie jesteś atrakcyjna"[7]. Na blogach można zobaczyć zdjęcia wychudzonych kobiet jako wzorów do naśladowania. Niestety w późniejszym etapie prowadzenia takiego trybu życia kobiety popadają w kompleksy i w później czasie nie potrafią poradzić sobie bez wsparcia specjalisty.

Zagrożeniem, które może spowodować utratę pieniędzy, bądź utratę dostępu do własnego konta może być **malware** (skrót od ang. *malicious software*). Jest uważany za uciążliwy lub szkodliwy typ oprogramowania, który ma na celu potajemnie uzyskać dostęp do urządzenia bez wiedzy użytkownika[8]. Malware ma na celu dezaktywację lub uszkodzenie komputerów, systemów komputerowych, sieci, tabletów, urządzeń przenośnych, najczęściej poprzez przejecie kontroli nad działaniem urządzenia[9].

Rysunek 4.1 przedstawia malware, jego rodzaje oraz powiązania między nimi. Do rodzajów wirusa należą min.: makro wirusy, boot sector wirus i wirusy towarzyszące. Rodzajami spyware jest: adware, keylogger czy też stealware. Natomiast trojan to np.: backdoor lub rootkit. Każdy z nich jest złośliwym oprogramowaniem, które ukrywa się w komputerze ofiary i niszczy go od środka lub szpieguje użytkownika i jego każdy ruch w sieci.

[6] http://uzaleznienie.com.pl/siecioholizm/poradnik-dla-rodzicow-d4/sexting-stalking-flaming-niebezpieczenstwa-czyhaja-w-sieci/, dostęp: 09.12.2020 r.
[7] http://uzaleznienie.com.pl/siecioholizm/poradnik-dla-rodzicow-d4/sexting-stalking-flaming-niebezpieczenstwa-czyhaja-w-sieci/, dostęp: 09.12.2020 r.
[8] https://www.avast.com/pl-pl/c-malware, dostęp: 08.12.2020 r.
[9] https://pl.malwarebytes.com/malware/, dostęp: 09.12.2020 r.



Źródło: https://pl.wikipedia.org/wiki/Złośliwe_oprogramowanie, dostęp: 10.01.2021 r.

Rysunek 4.1. Podstawowe grupy szkodliwego oprogramowania i ich wzajemne powiązania

Rodzajami malware są:

- **Wirus** to najstarsza wersja zagrożenia komputerowego, znana jeszcze w erze przed Internetowej[10]. Jest to program albo urywek kodu, który przedostaje się do komputera bez wiedzy i pozwolenia użytkownika.
- **Robak**, podobny w działaniu do wirusa, bardzo szybko się szerzy i powiela, jednak robak nie potrzebuje podczepiać się do innych plików i potrafi rozpowszechniać się samoistnie.
- **Koń trojański** to typ wirusa, który udaje, że jest użyteczny lub pomocny, podczas gdy w rzeczywistości uszkadza komputer i kradnie dane[11]. Rozprzestrzenia się, jako dodatek podczas pobierania narzędzi lub programów komputerowych.
- **Adware** jest rodzajem oprogramowania wyświetlającego reklamy, które pojawiają się w przeglądarce, w wyskakujących oknach lub na paskach narzędzi.

Zapobieganie atakom

Sposobów, aby chronić się przed cyberprzestępstwami jest wiele, najważniejsze jest jednak to, aby być przede wszystkim ostrożnym i nie podejmować decyzji pochopnie. W sieci nie można podawać lekkomyślnie własnych danych. Nie należy wysyłać ważnych danych tj., hasła, dane do logowania do

[10] T. Trejderowski, *Kradzież tożsamości. Terroryzm informatyczny,* Eneteia, Warszawa 2013, s. 218.
[11] https://www.avast.com/pl-pl/c-trojan, dostęp: 10.12.2020 r.

kont bankowych, szczegółów, które dotyczą kart bankowych przez e-maile lub portale społecznościowe.

Należy pamiętać przy tym, aby hasła miały odpowiednią długość oraz poziom trudności. Najlepiej, więc nie ustawiać w haśle własnego imienia lub nazwiska i nie ułatwiać zadania cyberprzestępcy. Tym silniejsze ono będzie, jeśli nie będzie związane z danymi osobistymi i nie będzie składało się tylko z liter, ale także z cyfr i znaków małych i dużych.

Kolejna kwestia to ostrożność podczas korzystania z sieci publicznych np.: w centrach handlowych. Złodzieje są bardzo czujni w miejscach z ogólnodostępnym Wi-Fi, tak więc najlepiej nie korzystać z takich sieci i nie logować się na swoje konta.

Następny krok to ciągła aktualizacja systemu operacyjnego i oprogramowania. Często okazuje się, że zawierają one pewne luki, o czym szybko mogą dowiedzieć się cyberprzestępcy. Luki są na bieżąco korygowane przez producentów, ale aby zostały wprowadzone, muszą być aktualizowane przez użytkowników komputerów.

Następna sprawa to pobieranie muzyki, filmów, aplikacji, oprogramowania z nieznanych stron, jest to kolejny błąd, który może wgrać na komputer szkodliwe oprogramowanie. Należy pobierać pliki tylko ze znanych i zaufanych stron, ponieważ pobranie ulubionej muzyki może kosztować użytkownika wgranie oprogramowania szpiegującego każdy jego krok w sieci.

Kolejną rzeczą, której nie wolno robić to otwieranie nieznanych załączników i linków, które przychodzą z podejrzanych adresów e-mail. Nie można zapomnieć też o programie antywirusowym. Warto zainwestować w dobre, licencjonowane oprogramowanie antywirusowe, które będzie chroniło użytkownika w Internecie oraz komputer przed atakami.

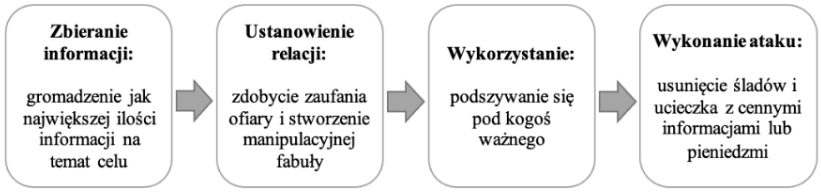
Osoby, które stają się ofiarami w Internecie, często nie wiedzą, co zrobić i gdzie zgłosić incydent. Powinny wiedzieć, że istnieje wiele miejsc, do których można zgłosić niebezpieczne zajście. Można to zrobić np.: na stronie https://incydent.cert.pl, na której udostępniono formularz, w którym można przedstawić niebezpieczne zajście. Ponadto, jeżeli osoba podejrzewa, że ktoś ma np.: dostęp do konta bankowego, należy zadzwonić do banku i powiadomić o tym pracownika. W Polsce funkcjonują również kancelarie prawne, które wskażą, jakie kroki należy podjąć. Jeżeli chodzi o groźby z udostępnieniem zdjęć prywatnych osoby, jeżeli nie wpłaci odpowiedniej ilości pieniędzy, to takie zajścia należy zgłaszać na policję bądź do prokuraturze. Nie należy bagatelizować żadnych incydentów w Internecie i natychmiast zgłaszać je w odpowiednie miejsca, może to uchronić nas oraz inne osoby przed skutkami ataków cyberprzestępców.

Wiele ataków nie doszłoby do skutku, gdyby nie osoby, które korzystają z różnych usług w cyberprzestrzeni. Lekceważenie podstawowych zasad bezpieczeństwa, przez pracowników firm, przedsiębiorców lub instytucje pań-

stwowe bądź publiczne prowadzi do tego, że pierwszym celem ataków cyberprzestępców jest człowiek. Dopiero później zaplecze informatyczne danej instytucji czy firmy.

Ataki socjotechniczne w cyberprzestrzeni

Ataki opierające się na technikach inżynierii społecznej towarzyszą użytkownikom Internetu każdego dnia. Nie są oni najczęściej nawet tego świadomi. Ponieważ są manipulowani przez socjotechników, których techniki rozwijają się coraz bardziej. Przykładowy schemat przebiegu ataku socjotechnicznego, który prawie zawsze wygląda tak samo przedstawia rysunek 4.2. Socjotechnicy mogą zaatakować swoją ofiarę przez maila, podczas rozmowy telefonicznej, ale także, gdy przyjdzie sam osobiście do swojej ofiary. Wykorzystując znajomość psychologii oraz socjologii pozyskują wiele informacji na tematy, które ich najbardziej interesują. Poufne dane, hasła są to jedne z nielicznych informacji, które cyberprzestępca wykorzysta przeciwko ofiarom. Kreatywność cyberprzestępców nie ma granic, istnieje wiele ataków, które w szczególności opierają się na manipulacji i wywieraniu wpływu. Bardzo często spotykane w obecnych czasach są między innymi: phishing, deepfake, pretexting oraz rozprzestrzenianie błędnych informacji w celach dezinformacji społeczeństwa.



Źródło: opracowanie własne na podstawie schematu https://www.social-engineer.org/framework/attack-vectors/attack-cycle/ dostęp: 17.12.2020 r.

Rysunek 4.2. Schemat przebiegu ataku socjotechnicznego

Pierwszym przykładem ataku socjotechnicznego jest:

– **Phishing** to jeden z najpopularniejszych typów ataków opartych o wiadomości e-mail lub SMS.[12] Posługuje się technikami socjotechnicznymi, za pomocą których przestępcy próbują oszukać osobę otwierającą wiadomość mailową bądź SMS. Nazwa budzi dźwiękowe skojarzenia z fishingiem – czyli łowieniem ryb. Przestępcy, podobnie jak wędkarze, stosują bowiem odpowiednio

[12] https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y, dostęp: 16.12.2020 r.

przygotowaną „przynętę”[13]. Atak phishingowy rozpoczyna się od odebrania wiadomości, która została przygotowana przez cyberprzestępców. Wiadomości te zwykle wyglądają bardzo autentycznie, ale tak naprawdę są fałszywe. Odbiorcy wydaje się, że otrzymał wiadomość od banku, sklepu internetowego, zaufanej osoby bądź legalnej organizacji tj.: firmy kurierskiej lub telekomunikacyjnej albo agencji rządowej. W takich wiadomościach zawarte są grzeczne prośby o aktualizację bądź zatwierdzenie informacji, często sugerowane jest, że pojawiły się jakieś problemy, wraz z wiadomością zawarty jest link lub załącznik, który należy kliknąć, aby potwierdzić, o co prosi cyberprzestępca. Niestety po kliknięciu w link ofiara zostaje przekierowana na nieautentyczną stronę, aby podać informacje dotyczące konta, bądź link to strony, która rozpowszechnia szkodliwe oprogramowanie albo jest po prostu zainfekowana.

- **Fake news** jest to fałszywa wiadomość, często o charakterze sensacyjnym, publikowana w mediach z intencją wprowadzenia odbiorcy w błąd w celu osiągnięcia korzyści finansowych, politycznych lub prestiżowych.[14] Najczęściej spotykanym modelem Fake news jest clickbait. Jest to przyciąganie odbiorców nieuczciwymi sposobami. Zazwyczaj są to odnośniki w formie tekstu lub grafiki, które swoim zakresem zachęcają odbiorców do wejścia na daną stronę. Najczęściej są to nagłówki artykułów, które nie mają nic wspólnego z autentyczną treścią strony. Misją clickbaitu jest przekonanie odbiorcy do wejścia w link i na docelową stronę. Dzięki temu wzrasta liczba odsłon strony, a tym samym przychodu z reklam.
- **Dezinformacja** pojęcie to przybrało niebywale wszechstronnego znaczenia. Pod pojęciem dezinformacja kryje się zarówno propaganda jak i wcześniej wspomniane fake news. Istnieje wiele definicji dezinformacji. Powszechnie kojarzona dezinformacja odnosi się do informacji, która jest jej przeciwieństwem, informacją kłamliwą i fałszywą, która wprowadza w błąd czytelnika. Głównym założeniem dezinformacji jest podanie odbiorcy pozornie prawdziwą wiadomość, która w rzeczywistości jest bezużyteczna, a nawet można powiedzieć, że szkodliwa, która ma posłużyć do podjęcia przez odbiorcę mylnych decyzji, które korzystne są z punktu widzenia osoby dezinformującej.
- **Pretexting** jest formą ataku socjotechnicznego, w której napastnik, za pomocą wymyślonego scenariusza, próbuje przekonać

[13] https://www.orange.pl/poradnik/twoj-internet/co-to-jest-phishing-i-jak-sie-przed-nim-bronic/, dostęp: 16.12.2020 r.
[14] https://wid.org.pl/wp-content/uploads/E_wydanie-Mały-Leksykon-Postprawdy.pdf, dostęp: 17.12.2020 r.

ofiarę do przekazania, ujawnienia cennych informacji lub dostępu do usługi lub systemu, których nie powinna ujawniać. Cechą charakterystyczną tego rodzaju ataku jest to, że oszuści wymyślają historię, pretekst, która ma na celu oszukanie ofiary. Wymyślony scenariusz ma na ogół postawić napastnika w roli kogoś z autorytetem. W pretextingu często przyjmujemy on postać klienta, kierownika, reportera, albo nawet członka rodziny współpracownika. Pretexting często używany jest przeciwko korporacjom, które przechowują dane klientów, takim jak banki, firmy obsługujące karty kredytowe.

Metodologia

Praca pt: *Inżynieria społeczna w atakach hakerskich* została napisana na podstawie analizy materiałów źródłowych. Materiały źródłowe, które zostały wybrane do przeanalizowania to: artykuły Internetowe oraz literatura w tematyce pracy. Ilość artykułów Internetowych była zdecydowanie większa niż literatury ze względu na dość małą dostępność książek w tematyce pracy. Materiały dostępne w Internecie zostały przeanalizowane z rozwagą, ponieważ nie wszystkie informacje zamieszczone na stronach internetowych są zgodne z prawdą. Dlatego materiały źródłowe zostały porównane z innymi.

Przegląd literatury

Do analizy wykorzystano wiele artykułów dostępnych w Internecie, ze względu na dość małą dostępność literatury w tematyce pracy. Pierwszą pozycją wybraną do analizy było: *Wywieranie wpływu na ludzi. Teoria i praktyka* Roberta Caldiniego. To książka z dziedziny psychologii społecznej, która przedstawia sześć reguł wywierania wpływu. Autor nazywa je „zasadami", każda z nich jest szczegółowo opisana. Są to: zasada wzajemności, zobowiązanie i konsekwencja, dowód społeczny, lubienie kogoś, autorytet, niedostępność. Opisuje, jak wpływać na innych ludzi, a także jak bronić się przed takim wpływem bądź manipulacją. Można dowiedzieć się także, jak zachęcić innych ludzi do zmiany decyzji i jak przekonać ich do tego, by tej zmiany sami zapragnęli.

Kolejna pozycja, która została przeanalizowana to książka Christophera Hadnagy *Socjotechnika. Sztuka zdobywania władzy nad umysłami*. Autor książki definiuje i rozkłada na cząstki elementarne definicję socjotechniki, przytaczając analizy i prawdziwe historie. Przedstawione zostały także powszechne, codzienne sytuacje, pod kątem scenariuszy socjotechnicznych. Ostatnia część dotyczy porad i wskazówek profesjonalnych socjotechników.

Innym źródłem była książka Tomasza Trejderowskiego, *Kradzież tożsamości. Terroryzm informatyczny*. Książka ta podejmuje zagadnienia socjotechniki oraz wykorzystania ułomności ludzkiej psychiki do przełamywania zabezpieczeń systemów informatycznych. Pokazuje, jak człowiek, wykonując

kilka rozmów telefonicznych lub wysyłając kilka e-maili, może narazić firmę lub osobę prywatną na nawet bankructwo Autor pokazuje, że nie ma danych i informacji bezwartościowych. We współczesnych czasach ofiarą może stać się każdy i w każdej chwili.

Wnioski

W obecnych czasach Internet odgrywa bardzo ważną rolę w życiu społeczeństwa. Wraz z rozwijaniem się sieci, rozwinęły się również zagrożenia. Niestety nie wszystko, co zostaje zamieszczane na stronach internetowych jest prawdą, ponieważ każdy człowiek jest w stanie zamieszczać swoje teksty, które nie zawsze są prawdziwe. Mogą mieć one na celu wprowadzenie w błąd społeczności. Jednak błędne informacje w Internecie nie są jedynym problemem, z jakim muszą zderzać się użytkownicy sieci. Coraz częściej można zauważyć, że przestępstwa zaczynają przenosić się z życia codziennego do Internetu i zamiast kradzieży pieniędzy z kasy w sklepie, częściej można usłyszeć o kradzieży poprzez atak phishingowy. Co gorsza cyberprzestępstwa rozwijają się z zawrotną prędkością wraz z umiejętnościami, jakimi posługują się cyberprzestępcy i inżynierowie społeczni.

Każdy socjotechnik ma swoje metody działania oraz cele. Jeden atakujący będzie chciał swoim działaniem pozyskać dostęp do systemu firmy, aby dostrzec luki, a następnie pomóc firmie w stworzeniu odpowiednich zabezpieczeń, natomiast inny za cel postawi sobie wyłudzenie pieniędzy i zainfekowanie systemu złośliwym oprogramowaniem.

W pracy wskazano jak używana jest inżynieria społeczna w atakach prowadzonych w Internecie. W pracy przedstawiono aparat pojęciowy niezbędny do zrozumienia tematyki inżynierii społecznej oraz ataków hakerskich. Wyjaśniono, na jakiej zasadzie działają metody socjotechniczne i jaki wpływ mają one na ludzi. Przedstawiono ataki hakerskie, w których używane są techniki inżynierii społecznej. Dla zilustrowania wagi problemu przedstawiono typowe ataki, do których należą phishing, deep fake, fake news, dezinformacja oraz pretexting.

W pracy przedstawiono również metody, dzięki którym możemy zapobiec zderzeniu się z atakami. Budując skuteczne mechanizmy bezpieczeństwa należy pamiętać, że najsłabszym ogniwem jest człowiek i na nim trzeba się skoncentrować.

Bibliografia

Opracowania zwarte

1. Caldini R., *Wywieranie wpływu na ludzi. Teoria i praktyka,* GWP Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2018
2. Hadnagy C., *Socjotechnika. Sztuka zdobywania władzy nad umysłami*, Helion, Gliwice 2012

3. Trejderowski T., *Kradzież tożsamości. Terroryzm informatyczny*. Eneteia, Warszawa 2013

Źródła internetowe

1. https://mobirank.pl/2020/01/31/raport-digital-i-mobile-na-swiecie-w-2020-roku/, dostęp: 12.01.2021 r.
2. https://pl.wikipedia.org/wiki/ARPANET, dostęp: 12.01.2021 r.
3. http://nawokandzie.ms.gov.pl/numer-3/wokanda-3/paragraf-na-stalkera.html, dostęp: 10.12.2020 r.
4. http://uzaleznienie.com.pl/siecioholizm/poradnik-dla-rodzicow-d4/sexting-stalking-flaming-niebezpieczenstwa-czyhaja-w-sieci/, dostęp: 10.12.2020 r.
5. http://uzaleznienie.com.pl/siecioholizm/poradnik-dla-rodzicow-d4/sexting-stalking-flaming-niebezpieczenstwa-czyhaja-w-sieci/, dostęp: 09.12.2020 r.
6. http://uzaleznienie.com.pl/siecioholizm/poradnik-dla-rodzicow-d4/sexting-stalking-flaming-niebezpieczenstwa-czyhaja-w-sieci/, dostęp: 09.12.2020 r.
7. https://www.avast.com/pl-pl/c-malware, dostęp: 08.12.2020 r.
8. https://pl.malwarebytes.com/malware/, dostęp: 09.12.2020 r.
9. https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y, dostęp: 16.12.2020 r.
10. https://www.orange.pl/poradnik/twoj-internet/co-to-jest-phishing-i-jak-sie-przed-nim-bronic/, dostęp: 16.12.2020 r.

bsmt pchor. Bartłomiej GOSTKOWSKI

ŚWIADOMOŚĆ STUDENTÓW AKADEMII MARYNARKI WOJENNEJ W GDYNI NA TEMAT ZAGROŻEŃ WYNIKAJĄCYCH Z UŻYTKOWANIA CYBERPRZESTRZENI

Streszczenie

Występujące w cyberprzestrzeni zagrożenia, gdy trafią na podatność w postaci osoby niekompetentnej mogą wywołać znaczne szkody w postaci utraty integralności, dostępności czy niezaprzeczalności danych i informacji. W celu zbadania poziomu świadomości studentów Akademii Marynarki Wojennej w Gdyni na temat cyberzagrożeń przeprowadzono badanie metodą sondażu diagnostycznego, techniką ankiety z wykorzystaniem kwestionariusza ankiety jako narzędzia badawczego. Poddano analizie pojęcie cyberprzestrzeni, scharakteryzowano cyberzagrożenia oraz przedstawiono wybrane wyniki badania empirycznego, które przeprowadzono w grudniu 2020 roku.

Słowa kluczowe:
cyberzagrożenia, cyberprzestrzeń, świadomość użytkowników cyberprzestrzeni.

Abstract

Awareness of students of the Naval Academy in Gdynia about the threats resulting from the use of cyberspace

Summary:

Cyberspace threats when they hit a vulnerability in the form of an incompetent person can cause significant damage in the form of loss of integrity, availability, or non-repudiation of data. To test the level of awareness of students of the Naval Academy in Gdynia about cyber threats. The concept of cyberspace was analyzed, cyberthreats were characterized and some of the results of the survey that took place in December 2020 were presented.

Keywords:
cyber threats, cyberspace, awareness of cyberspace users.

Wstęp

Wielu ludzi, szczególnie młodego pokolenia, spędza znaczną część swojego dnia przed ekranem komputera czy smartfonu. Dzięki Internetowi użytkownicy mogą, między innymi utrzymywać kontakt ze znajomymi, robić zakupy, czy udostępniać na portalu społecznościowym swoje zdjęcia. Do Internetu przechodzą również negatywne zachowania występujące w społeczeństwie. Cyberprzestrzeń jest miejscem, w którym można napotkać się na zagrożenia. W dobie przenoszenia części życia ludzi do cyberprzestrzeni, między innymi z powodu pandemii wirusa SARS-CoV-2 należy pamiętać o zagrożeniach. Sytuacja na świecie wywołana owym wirusem jeszcze bardziej zwiększyła znaczenie cyberprzestrzeni w życiu codziennym, co skutkuje wzrostem znaczenia wartości, jaką jest świadomość użytkowników na temat cyberzagrożeń. W prawie rzymskim funkcjonuje termin „Nieznajomość prawa szkodzi[1]" (łac. *Ignorantia iuris nocet)* i tak samo jak w przypadku braku znajomości prawa, brak świadomości użytkowników na temat zagrożeń można traktować jako podatność, która może wpłynąć na zasoby informacyjne organizacji, jak i również danych samego użytkownika.

Według Macieja Marczyka cyberprzestrzeń jest wymiarem aktywności, w której wszelkie działania odbiegają do środowiska fizycznego. Jest dziełem człowieka, a użytkownicy mają kontrolę nad charakterem tego środowiska[2]. Można przez to rozumieć, że cyberprzestrzeń staje się wirtualnym odzwierciedleniem fizycznej rzeczywistości i w związku z tym przenikają do niej również negatywne formy ludzkiej działalności[3].

Cyberprzestrzeń – analiza pojęcia

Rozwój informatyczny społeczeństw na przełomie wieku XX i XXI charakteryzował się i nadal charakteryzuje dużą dynamiką. Przeskok techniczny i technologiczny, jakiego dokonała ludzkość w tym zakresie, można zobrazować na przykładzie komputera pokładowego programu Apollo 11. Komputer ten przyczynił się do udanego lądowania na księżycu w 1969 roku[4], a w obecnych czasach, noszone w kieszeni urządzenia posiadają moc obliczeniową niewyobrażalną dla ludzi z epoki lądowania na księżycu.

Przez lata definicje cyberprzestrzeni ewoluowały i powstawały nowe. Departament Obrony Stanów Zjednoczonych, cyberprzestrzeń definiuje jako „ogólnoświatową domenę środowiska informacyjnego składającą się z współzależnych sieci tworzonych przez infrastrukturę informatyczną oraz zawartych

[1] https://encyklopedia.pwn.pl/haslo/ignorantia-iuris-nocet-ignorantia-facti-non-nocet;3914000.html, dostęp: 09.01.2021 r.
[2] M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru* Przegląd Teleinformatyczny nr 1-2, 2018, s. 63.
[3] T. Hoffman, *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Wydawnictwo FNCE, Poznań 2018, str. 126.
[4] National Aeronautics and Space Administration Apollo Project Office, 15.12.1968 - 01.04.1971. s. 68.

w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także zawarte w nich procesory oraz kontrolery[5]". Definicja ta odnosi się tylko do aspektu technicznego (sprzętowego), jednakże oprogramowanie (ang. *Software)* można zrozumieć z kontekstu, a udział człowieka został w niej pominięty[6].

Definicje cyberprzestrzeni, od słownikowych po terminy zatwierdzone przez państwo w większości posiadają jako rdzeń cyberprzestrzeni globalnie połączoną sieć sprzętu, oprogramowania i danych. Kolejnym ważnym aspektem, który zwykle nie jest wyraźnie stwierdzony, jest to, że ludzie mogą kontaktować się w cyberprzestrzeni i robiąc to, stają się jej częścią[7].
Cyberprzestrzeń jest rozumiana również jako złożone środowisko powstałe w wyniku interakcji ludzi, oprogramowania i usług w Internecie za pomocą urządzeń technicznych i połączonych z nimi sieci, które nie istnieje w żadnej fizycznej postaci[8]. Wobec powyższych definicji celowe jest zdefiniowanie: Internetu, usług internetowych, oprogramowania oraz interakcji ludzkiej w Internecie.

Termin Internet możemy rozumieć jako ogólnoświatowy system połączeń między komputerami, określany również jako sieć sieci[9]. Dzięki niemu ludzie mogą komunikować się, szukać informacji, robić zakupy, a także dostarczać rozrywkę oraz szereg innych udogodnień prawie w każdym miejscu na Ziemi.

Komercjalizacja i rozwój Internetu nastąpił w latach 90 ubiegłego wieku. Wraz ze wzrostem rozwoju rośnie liczba jego użytkowników. Dzisiaj można mieć do niego dostęp za pomocą lodówek czy samochodów. Stał się zatem jednym z podstawowych mediów[10].

Usługi internetowe to usługi dostępu do Internetu świadczone przez przedsiębiorstwa telekomunikacyjne oraz wszelkie usługi (zwykle płatne) dostępne on-line polegające na dostarczeniu przez Internet filmów, plików muzycznych, programów komputerowych, gier i innych produktów, a także umożliwiają opracowywanie i utrzymanie firmowych serwisów WWW, aplikacji, baz danych i sklepów wirtualnych, rejestracje domen internetowych, hosting obejmujący dostęp do kont e-mailowych, a także reklamę i marketing[11].

Z usług internetowych korzystają ludzie, którzy mogą wchodzić ze sobą w interakcje. We wrześniu 2020 roku za pośrednictwem między innymi

[5] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms,* s. 58.
[6] R. Ottis, P. Lorents, *Cyberspace: Definition and Implications,* Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia s. 2.
[7] Tamże.
[8] ISO/IEC 27032:2012(en).
[9] A. S. Tanenbaum, *Sieci komputerowe*, Wydawnictwo Helion, Gliwice 2004, s. 59.
[10] T. Hoffman, *Wybrane aspekty cyberbezpieczeństwa w Polsce*, Wydawnictwo FNCE, Poznań 2018, str. 126.
[11] https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/1908,pojecie.html, dostęp: 17.11.2020 r.

telefonu z dostępem Internetu połączyło się 27,7 milionów internautów, a przeciętny internauta spędzał blisko 2 godziny i 4 minuty korzystając z Internetu[12].

Internauci mają możliwość zaspokajania zarówno potrzeb wyższego rzędu jak potrzeby afiliacji uznania czy samorealizacji poprzez własne blogi czy strony WWW (ang. *World Wide Web)*, aż po potrzeby hedonistyczne dzięki powszechnym grom sieciowym, czy możliwością zrobienia zakupów w Internecie[13].

Przedstawiając aspekty cyberprzestrzeni w ujęciu praktycznym przedstawiono elementy tworzące cyberprzestrzeń oraz podzielono ją na warstwy. Według Macieja Marczyka elementami tymi są: systemy i sieci teleinformatyczne, dane i informacje[14].

System to wyodrębniony zbiór elementów materialnych lub abstrakcyjnych, wzajemnie powiązanych, jako całość, zachowujący przy tym takie wartości, których nie posiadają inne elementy[15]. Biorąc pod uwagę technologię informacyjną systemem nazywamy zbiór powiązanych ze sobą elementów służących przetwarzaniu danych przez określone środki teleinformatyczne[16]. Doktryna systemów teleinformatycznych charakteryzuje cechy jakimi powinien się określać system teleinformatyczny. System ten powinien być: wydajny, interoperacyjny, elastyczny, skalowalny, żywotny, zorientowany na usługi, autonomiczny, dostępny w określonym czasie, gotowy do użycia, bezpieczny,[17]

Pojęcie systemu teleinformatycznego oznacza zespół współpracującego ze sobą oprogramowania i urządzeń informatycznych, zapewniający odbieranie, wysyłanie, a także przetwarzanie oraz przechowywanie danych za pomocą właściwego dla rodzaju sieci teleinformatycznej urządzenia końcowego przez sieci telekomunikacyjne[18].

W środowisku cybernetycznym[19] można wyróżnić sieci: teleinformatyczne, komputerowe lub telekomunikacyjne. Sieci telekomunikacyjne według

[12] https://pbi.org.pl/raporty/polscy-internauci-we-wrzesniu-2020/, dostęp: 17.11.2020 r.
[13] S. Juszczyk, *Internet -współczesne medium komunikacji społecznej*, Katedra Pedagogiki Wczesnoszkolnej i Pedagogiki Mediów, Uniwersytet Śląski, Katowice 2010, s. 1.
[14] M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru,* Przegląd Teleinformatyczny nr 1-2, 2018, s. 63.
[15] J. Michniak, *Dowodzenie i łączność*, AON, Warszawa, 2003 s.13.
[16] M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru* Przegląd Teleinformatyczny nr 1-2, 2018, s. 63.
[17] Doktryna systemów teleinformatycznych D-6(A), 2019, CDiSSZ, s. 17-21.
[18] Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną, art.2, ust. 3.
[19] Środowisko cybernetyczne to zespół wszelkich elementów i czynników będących w ścisłej współzależności, który wpływa na procesy informacyjne danego układu poprzez umacnianie stanów pożądanych i przeciwdziałanie owym stanom niepożądanym. Źródło: R. Janczewski, *Procesy informacyjne w systemie wspomagania dowodzenia w kontekście działania w środowisku cybernetycznym,* [w:] J. Wołejszo (red.) *Automatyzacja dowodzenia SZ RP w środowisku sieciocentrycznym, Monografia zbiorowa z konferencji naukowej*, Gdynia – Warszawa, czerwiec 2013, s. 99-112.

ustawy o prawie telekomunikacyjnym to systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju[20].

Sieci komputerowe określane są jako sieci informatyczne. Służą one przede wszystkim ułatwieniu komunikacji pomiędzy użytkownikami w sektorze prywatnym jak i w strukturach zhierarchizowanych. Ułatwiają szybki dostęp do zasobów informacyjnych organizacji jak i globalnych informacji przy wykorzystaniu Internetu[21].

Sieci komputerowe można podzielić na różne typy w zależności od ich skali działania. Podział tej skali wygląda następująco:

- LAN (ang. *Local Area Network)*, czyli sieci lokalne obejmują niewielki obszar fizyczny, taki jak dom, biuro lub niewielka grupa budynków, na przykład szkoła lub lotnisko.
- WLAN (ang. *Wireless Local Area Network),* czyli bezprzewodowa sieć lokalna, obejmująca niewielki obszar fizyczny, umożliwiająca użytkownikom poruszanie się w większym obszarze zasięgu, ale nadal są bezprzewodowo połączone z siecią.
- WAN (ang. *Wide Area Network),* czyli sieci rozległe obejmują rozległy obszar, taki jak łącza komunikacyjne, które przekraczają granice metropolitalne, regionalne lub krajowe. Internet jest najlepszym przykładem sieci WAN.
- MAN (ang. *Metropolitan Area Network),* czyli sieci metropolitalne obejmujące bardzo duże obszary obejmujące całe miasto.
- SAN (ang. *Storage Area Network)*, czyli sieci pamięci masowej pomagają podłączać zdalne urządzenia pamięci masowej komputera, takie jak macierze dyskowe, biblioteki taśmowe i optyczne szafy grające, do serwerów w taki sposób, że wydają się być lokalnie podłączone do systemu operacyjnego.
- CAN (ang. *Controller Area Network)*, czyli sieci kontrolerów pozwalają mikrokontrolerom i urządzeniom komunikować się ze sobą bez komputera głównego.
- PAN (ang. *Personal Area Network),* czyli sieci osobiste są używane do komunikacji między różnymi urządzeniami, takimi jak telefony, osobiste asystenci cyfrowi, faksy i drukarki, które znajdują się blisko jednego użytkownika.
- GAN (ang. *Global Area Network)*, czyli sieci ogólnoświatowe obsługują komunikację mobilną w dowolnej liczbie bezprzewodowych sieci LAN i obszarach zasięgu satelitarnego.

[20] Art. 2, pkt. 35 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne.
[21] M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru,* Przegląd Teleinformatyczny nr 1-2, 2018, s. 64.

– Intersieć (ang. *Internetwork)*, czyli połączone dwie lub więcej odrębnych sieci komputerowych lub segmentów sieci za pomocą wspólnej technologii routingu[22].

Kolejnymi elementami przedstawionymi w są dane i informację. Dane to obiekty, na których operują programy. Pojedyncza dana być grupą najprostszych danych, wtedy posiada określoną wewnętrzną strukturę związaną z usytuowaniem danych składowych oraz regułami dostępu do nich[23]. Systemy telekomunikacyjne i teleinformatyczne posiadają również dane osobowe, czyli wszystkie informacje, dzięki którym istnieje możliwość zidentyfikowania osoby fizycznej[24].

Pojęcie informacji w języku potocznym jest używane zamiennie z pojęciem danych co wpływa na precyzyjność tych pojęć i prowadzi do niewłaściwego ich zrozumienia. Informacja jest trudniejsza do zdefiniowania niż dane, ponieważ różne dziedziny nauki w zależności od charakteru i sposobu użycia informacji różnie je definiują. Jednakże, można przyjąć, że jest to nieokreślona treść przekazywana od nadawcy do odbiorcy przy pomocy określonego języka lub kodu[25].

Cyberprzestrzeń można podzielić na trzy połączone ze sobą warstwy. Są nimi: warstwa sieci fizycznej (ang. *Physical Network Layer)*, warstwa sieci logicznej (ang. *Logical Network Layer)*, oraz warstwa cyberosobowości (ang. *Cyber-Persona layer*)[26].

Warstwa sieci fizycznej (ang. *Physical Network Layer)* zawiera urządzenia informatyczne (ang. *Information Technology, IT*) oraz infrastrukturę w domenach fizycznych, aby zapewnić, składowanie, transport i przetwarzanie informacji wewnątrz cyberprzestrzeni w tym repozytoria danych i połączenia, które przenoszą dane między składniki sieci. Fizyczne składniki sieci obejmują sprzęt i infrastrukturę (np. urządzenia komputerowe, urządzenia pamięci masowej, sieciowe i przewodowe urządzenia oraz łącza bezprzewodowe). Składniki fizycznej warstwy sieciowej wymagają zabezpieczeń fizycznych, środków chroniących je przed uszkodzeniem fizycznym lub nieuprawnionym dostępem fizycznym, które można wykorzystać w celu uzyskania dostępu logicznego[27].

Elementami, które są ze sobą powiązane w sposób wyodrębniony z sieci fizycznej, w oparciu o programowanie logiczne (kod), który steruje komponentami sieci nazywa się warstwą logiczną (ang. *Logical Network Layer)*. Poszczególne łącza i węzły są reprezentowane w warstwie logicznej. Mogą to być także różne rozproszone elementy cyberprzestrzeni, w tym dane,

[22] https://wireless-network-support.blogspot.com/2009/08/what-is-lan-wlan-wan-man-san-canpan.html, dostęp: 10.01.2021 r.
[23] https://encyklopedia.pwn.pl/haslo/3890542/dane.html, dostęp: 10.01.2021 r.
[24] Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych, art. 6, ust. 1.
[25] M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru* Przegląd Teleinformatyczny nr 1-2, 2018, s. 66.
[26] Joint Publication 3-12, *Cyberspace Operations,* 2018, s. 23.
[27] Tamże, s. 23-24.

aplikacje i procesy sieciowe, które nie są powiązane z jednym węzłem. Przykładem jest Joint Knowledge Online Website[28], która znajduje się na serwerach w wielu lokacjach, lecz w domenie fizycznej istnieje pod jednym adresem domeny (ang. *Uniform Resource Locator*, skrót – *URL)*[29].

Warstwa cyberosobowości (ang. *Cyber-Persona Layer)* jest stworzona poprzez wyodrębnienie danych z logicznej warstwy sieciowej w cyberprzestrzeni z wykorzystaniem reguł, które obowiązują w warstwie logicznej w celu opracowania opisów cyfrowych reprezentacji tożsamości (użytkownika) w cyberprzestrzeni. Warstwa ta składa się z kont użytkowników zarówno ludzkich jak i automatycznych, oraz ich wzajemnych relacji[30].

Cyberprzestrzeń można rozumieć również, między innymi jako środowisko powstałe w wyniku interakcji ludzkich. Cyberprzestrzeń zaczęto traktować jako nową kategorią przestrzeni społecznej. W odróżnieniu od płaszczyzny realnej, dzięki Internetowi możliwe jest ominięcie ograniczeń czasu i przestrzeni narzucanych przez ludzką egzystencję[31].

Od strony technicznej fundamentem wspomnianych interakcji ludzkich stał się Internet[32]. Media społecznościowe (ang. *Social Media)* stały się integralną częścią życia ludzi, w szczególności osób młodych. Użytkownicy przy pomocy sieci społecznościowych mogą komunikować się ze znajomymi, dzielić się zdjęciami i nagraniami wideo[33].

Media społecznościowe mogą być określane jako ,,podlegające społecznej kontroli środki przekazu, które mogą być wykorzystywane na dowolną skalę. Zawierają zarówno treść przekazu, jak i możliwe punkty widzenia odnoszące się do informacji”[34].

Użytkownicy mediów społecznościowych są zaangażowani w budowanie dialogów na portalach społecznościowych. Wpływ na ich popularność ma stale rosnący i łatwy dostęp do Internetu[35]. W opozycji do mediów klasycznych ta-

[28] Joint Knowledge Online Website to szkoleniowa strona internetowa Departamentu Obrony Stanów Zjednoczonych. Źródło:
https://jko.jten.mil/docs/JKO_Fact_Sheet_(July%202020).pdf, dostęp: 16.01.2021 r.
[29] Joint Publication 3-12…, dz. cyt., s. 24.
[30] Joint Publication 3-12, *Cyberspace Operations*, 2018, s. 24.
[31] M. Ochab, *Cyberprzestrzeń jako środowisko społeczeństwa obywatelskiego w Brazylii,* Teka of Political Science and International Relations – OL PAN/UMCS, 2018, 13/2, s. 189.
[32] J. Wasilewski, *Zarys definicyjny cyberprzestrzeni* Przegląd bezpieczeństwa wewnętrznego 2013, s. 226.
[33] M. Kotyśko, *Nadmierne korzystanie z sieci społecznościowych*, Alkoholizm i Narkomania 2014, Tom 27, nr 2, s. 177.
[34] P. Tomczuk, *Social media jako element zintegrowanej komunikacji firm*, Szkolenie Social media w komunikacji zewnętrznej i wewnętrznej firm z dn. 29.04.2010 r. organizowane przez Ciszewski Financial Communications, Ciszewski Public Relations oraz portal PRoto.pl.
[35] K. Fabjaniak-Czerniak, *Internetowe media społecznościowe jako narzędzie public relations*, Wyższa Szkoła Promocji, Warszawa 2012, s. 174.

kich jak telewizja, radio czy prasa Internet umożliwia komunikację porozumiewawczą (jeden do jednego), rozsiewczą (jeden do wielu), oraz powszechną (wiele do wielu)[36].

Reasumując, cyberprzestrzeń to nie tylko pojęcia informatyczne, lecz również socjologiczne. Środowisko społeczne, w którym dochodzi do interakcji ludzkich, opiera się o media społecznościowe. Na przestrzeni lat powstawały i ewoluowały nowe definicje cyberprzestrzeni, w których wspólnym elementem są globalnie połączone sieci sprzętu, oprogramowania i danych, a niektóre uwzględniają w nich również ludzkie interakcje. Cyberprzestrzeń można podzielić również na trzy warstwy: fizyczną, logiczną i warstwę cyberosobowości.

Cyberzagrożenia – charakterystyka, podstawowe pojęcia, podział oraz częstotliwość występowania

Internet w dzisiejszych czasach jest bardzo powszechny. Jednak ogólnoświatowa sieć jaką jest Internet niesie ze sobą nie tylko korzyści, ale także zagrożenia. Zgodnie z definicją zawartą w słowniku języka polskiego cyberzagrożenie rozumiane jest jako zagrożenie mające związek z korzystaniem ze środków komunikacji elektronicznej, głównie Internetu[37].

Jak wskazuje praktyka nie ma aplikacji, czy przykładowo, systemu teleinformatycznego idealnego, a każdy program, który z pozoru ma ułatwić nasze życie swoimi funkcjonalnościami, może zostać skompromitowany, a dzięki lukom, wykorzystany przez cyberprzestępców.

Niewiedza, ignorancja czy brak właściwych zabezpieczeń potęgują skalę możliwości, którą osoby ze specjalistyczną wiedzą informatyczną mogą wykorzystać na swoją korzyść lub na niekorzyść użytkowników sieci teleinformatycznych. Główną motywacją ataku cyberprzestępców są pieniądze, zemsta, a także chęć pozyskania informacji, które w dzisiejszych czasach, odpowiednio szybko przetworzone mogą stanowić walutę. Co za tym idzie, im większe zasoby posiada podmiot atakowany tym bardziej musi podnosić swoje standardy bezpieczeństwa[38].

Cyberprzestępcy mogą przygotowywać ataki stricte na konkretnego użytkownika wykorzystując między innymi narzędzia rozpoznania z ogólnodostępnych źródeł (ang. *Open Source Intelligence*, skrót OSINT). Atakiem bezpośrednio przygotowywanym przeciwko danej osobie, organizacji lub biznesowi jest przykładowo spearphishing[3940].

---

[36] S. Juszczyk., *Internet -współczesne medium komunikacji społecznej,* Katedra Pedagogiki Wczesnoszkolnej i Pedagogiki Mediów, Uniwersytet Śląski, Katowice 2010, s. 2.
[37] https://sjp.pl/cyberzagro%C5%BCenie, dostęp: 07.12.2020 r.
[38] https://www.cyberdefence24.pl/zysk-finansowy-wazniejsza-motywacja-cyberatakow-niz-szpiegostwo, dostęp: 08.01.2021 r.
[39] https://www.kaspersky.com/resource-center/definitions/spear-phishing, dostęp: 08.01.2021 r.
[40] Spearphishing- to rodzaj oszustwa rozsyłanego za pomocą komunikatorów lub poczty e-mail, kierowane w konkretne podmioty. Mimo, że głównym celem spearphisingu jest kradzież

Zagrożenia można się spodziewać z kierunku nie tak oczywistego jak to się wydaje na pierwszy rzut oka. Część użytkowników Internetu ma niekompletną wiedzą w dziedzinie cyberbezpieczeństwa. Ta właśnie niewiedza jest podatnością, którą wykorzystują cyberprzestępcy, aby osiągnąć określony cel.

Analizując źródła można podzielić cyberzagrożenia na nietechniczne (społeczne) oraz techniczne. Oba te rodzaje zagrożeń w cyberprzestrzeni mogą pociągać za sobą szkody. Poniżej zostały wyszczególnione zagrożenia nietechniczne i techniczne. Zagrożenia nietechniczne (społeczne) dzielą się na: cyberstalking, trollowanie, flaming, cyberprostytucja, seksting, grooming,[41].

Cyberstalking jest to dręczenie indywidualnej osoby lub grupy osób przy wykorzystaniu środków przekazu, głównie Internetu. Trollowanie jest to zachowanie aspołeczne charakterystyczne dla internetowych grup, dyskusyjnych forów, sieci społecznościowych i czatów. Polega ono na rozmyślnym wpływaniu na użytkowników w celu ośmieszenia lub obrażenia poprzez wysłanie kontrowersyjnych, napastliwych i często nieprawdziwych przekazów[42]. Nazwa pochodzi od trolli. Troll w ujęciu cyberbezpieczeństwa to osoba, która celowo stara się obrazić lub wszcząć kłótnie z innym użytkownikiem Internetu między innymi przez publikowanie treści obraźliwych lub niemiłych w Internecie[43]. Zjawiskiem podobnym do trollowania jest flaming (ang. *flaming*), czyli zaognianie wymiany zdań użytkowników forów dyskusyjnych mające na celu eskalację agresji wypowiedzi. Pozostałe trzy zagrożenia wiążą się z seksualnością. Cyberprostytucja polega na udostępnianiu materiałów erotycznych lub pornograficznych z własnym udziałem w celu uzyskania korzyści materialnych. Mogą to być zdjęcia, filmy lub nawet pokaz na żywo przy wykorzystaniu kamerki internetowej. Seksting jest nieco łagodniejszą formą cyberprostytucji, które dotyczy wszystkich grup internautów. Termin ten powstał z połączenia angielskich słów „sex" i „texting". Jest on formą komunikacji elektronicznej, w której przekazem jest seksualnie sugestywny obraz lub treść[44]. Grooming (ang. *grooming*) z kolei jest to przestępstwo, które popełniają osoby składające nieletniemu propozycje seksualne przez Internet lub wprowadzające w błąd nieletniego w celu produkcji materiałów pornograficznych[45].

Zagrożenia techniczne dzielą się na: wirusy, robaki, kruegerware lub kruegerapps, spyware, broweser hijacker lub porywacz przeglądarek, jokes, riskware, poachware, malware, konie trojańskie, trojan dropper, trojan clicker,

danych cyberprzestępcy mogą również próbować zainstalować złośliwe oprogramowanie na komputerze użytkownika. Źródło: https://www.kaspersky.com/resource-center/definitions/spear-phishing, dostęp: 16.01.2021 r.

[41] https://www.gov.pl/web/baza-wiedzy/zagroz-nietechniczne-spoleczne, dostęp: 14.12.2020 r.

[42]https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html, dostęp: 11.01.2021 r.

[43] https://www.collinsdictionary.com/dictionary/english/troll, dostęp: 16.01.2021 r.

[44] https://pl.wikipedia.org/wiki/Sexting, dostęp: 16.01.2021 r.

[45] https://www.gov.pl/web/baza-wiedzy/zagroz-nietechniczne-spoleczne, dostęp: 14.12.2020 r.

trojan downloader, trojan proxy, crimeware, bundleware, DoS, rootkit, spam, phishing, likejacking, tabnapping, vishing, IP spoofing, hakowanie, BotNet[46], W celu ujednolicenia rozumienia przedstawionych terminów poniżej przedstawiono ich definicje.

Wirusy to programy zmieniające kod pliku w celu uzyskania nieautoryzowanego dostępu przy uruchomieniu zainfekowanego pliku[47]. Robaki natomiast to szkodliwe oprogramowanie, które wykorzystuje zasoby sieci telekomunikacyjnej do rozprzestrzeniania się, w stosunkowo szybkim tempie[48].

Kruegerware lub Kruegerapps (ang. *kruegerware, kruegerapps*) jest to oprogramowanie, które nie jest proste do usunięcia ze względu na jego zdolność powracania do istnienia. Właśnie stąd nazwa nawiązująca do postaci z filmu „Koszmar z ulicy Wiązów". Najczęściej zwykło się określać tym mianem wirusy komputerowe typu malware i spyware.

Oprogramowanie szpiegowskie (ang. *spyware*) pozwala na zbieranie informacji

o użytkowniku, a także całej organizacji przy braku świadomości posiadania złośliwego oprogramowania przez ofiarę. Malware natomiast pochodzi ze skróconych słów z języka angielskiego *malicious software*, czyli złośliwe oprogramowanie. Ma ono na celu wpływanie na dane lub informacje będące zasobem ich użytkowników lub na zainfekowane urządzenie. Obejmuje wirusy, robaki, konie trojańskie, spyware, nieuczciwe oprogramowanie typu adware (połączenie słów ang. *ad* - reklama, *software* - oprogramowanie)[49] oraz inne szkodliwe dla komputera oprogramowanie[50].

Porywacz przeglądarek (ang. *browser hijacker*) jest złośliwym oprogramowaniem zmieniającym ustawienia przeglądarki internetowe. Najczęściej wprowadza on zmiany domyślnej strony przeglądarki, a także tworzy niepożądane zakładki lub wyskakujące okna często o charakterze pornograficznym lub hazardowym[51].

Oprogramowanie zawierające w sobie potencjalne zagrożenie, jednakże nie będące wirusem jest riskware (połączenie słów ang. *risk* - ryzyko, *software* - oprogramowanie). W określonych warunkach sama obecność tego oprogramowania oznacza zagrożenie dla danych lub informacji użytkownika zapisanych na urządzeniu.

Poachware (połączenie słów ang. *poach* - kłusować, *software* - oprogramowanie) jest oprogramowaniem szpiegowskim mającym na celu zdobywanie wrażliwych danych użytkownika, przykładowo danych logowania do portali społecznościowych.

---

[46] https://www.gov.pl/web/baza-wiedzy/zagr-techniczne, dostęp: 14.12.2020 r.
[47] W. Stallings, *Computer security: principles and practice*. Boston: Pearson 2012. s. 182.
[48] https://www.gov.pl/web/baza-wiedzy/zagr-techniczne, dostęp: 14.12.2020 r.
[49] Adware to oprogramowanie złośliwe służące do wyświetlania reklam na ekranie, najczęściej w oknie przeglądarki internetowej, źródło: https://pl.malwarebytes.com/adware/, dostęp: 11.01.2021 r.
[50] https://www.gov.pl/web/baza-wiedzy/zagr-techniczne, dostęp: 14.12.2020 r.
[51] A. Pęczak, *Porywacze przeglądarek*, PC World, nr 4/2014, str. 72-77.

W odniesieniu do cyberzagrożeń konie trojańskie to programy wykonujące działania na zainfekowanych urządzeniach w sposób niekontrolowany przez użytkownika. Mogą one wykradać, usuwać lub modyfikować dane, a także powodować stany bezczynności systemu. W skład koni trojańskich wchodzi pięć wcześniej wymienionych trojanów. Trojan dropper (ang. *dropper Trojan*) to rodzaj wirusa, który na urządzeniu instaluje złośliwy kod. Trojany te aktualizują już zainstalowane wirusy lub instalują nowe. Trojan clicker (ang. *clicker Trojan*) ma za zadanie poinformować podmiot atakujący o instalacji złośliwego kodu oraz przekazać informację na przykład o otwartych portach czy adresie IP. Trojan downloader (ang. *downloader Trojan*) w specyfice działania jest podobny do trojan droppera, jednakże jego użyteczność jest większa z tego powodu, że jest mniejszy i może być wykorzystany do pobrania nieokreślonej liczby nowych wersji złośliwego oprogramowania. Trojan proxy (ang. proxy Trojan) śledzi aktywność użytkownika zainfekowanego urządzenia w celu zdobycia, przykładowo, loginu i hasła do bankowości internetowej. Zarejestrowana aktywność jest zapisywana i wysyłana do cyberprzestępcy. Piątym trojanem jest trojan backdoor (ang. *backdoor Trojan*), który pozwala na zdalne kontrolowanie urządzenia ofiary[52].

Crimeware (połączenie słów ang. *crime* - przestępstwo, *software* - oprogramowanie) jest kolejnym programem szpiegującym, który ma na celu zgromadzenie danych lub informacji niejawnych użytkownika, głównie danych logowania do usług finansowych[53]. Bundleware (połączenie słów ang. *bundle* - pakiet, *software* - oprogramowanie) jest to rodzaj dystrybucji złośliwego oprogramowania poprzez dołączenie go do innego popularnego programu. Dzięki temu zabiegowi nieświadomi użytkownicy sami instalują oprogramowanie szkodliwe na swoich urządzeniach[54]. Natomiast rootkit (ang. *rootkit*) jest narzędziem ukrywającym złośliwe działania przed programami antywirusowymi[55].

DoS (ang. *Denial-of-Service*), czyli odmowa usługi jest cyberatakiem, w którym cel jest „zalewany'' aż do momentu, gdy nie może odpowiedzieć lub ulega awarii uniemożliwiając dostęp uprawnionym użytkownikom[56]. Atak ten występuje również w wersji rozproszonej tak zwanej DDoS (ang. *Distributed Denial-of-Service*), która wykorzystuje sieć, BotNet, czyli urządzenia, nad którymi przejęto kontrolę, przez co trudniejszym zadaniem jest powstrzymać taki atak[57].

Atakiem bazującym na inżynierii społecznej jest phishing (ang. *phishing*), czyli metoda oszustwa internetowego polegająca na podszyciu się pod inną osobę lub instytucję w celu wyłudzenia, przykładowo, danych logowania.

---

[52] https://www.gov.pl/web/baza-wiedzy/zagr-techniczne, dostęp: 14.12.2020 r.
[53] https://www.gov.pl/web/baza-wiedzy/zagr-techniczne, dostęp: 14.12.2020 r.
[54] https://blog.malwarebytes.com/glossary/bundleware/, dostęp: 14.12.2020 r.
[55] https://www.gov.pl/web/baza-wiedzy/zagr-techniczne, dostęp: 14.12.2020 r.
[56] https://us-cert.cisa.gov/ncas/tips/ST04-015, dostęp: 22.12.2020 r.,.
[57] S. Taghavi Zargar, Sanan *A Survey of Defence Mechanisms Against Distributed Denial of Service (DDos) Flooding Attacks IEEE Communications Surveys & Tutorials* 2013 s. 1.

W tym ataku czasami wykorzystuje się spam (ang. *spam*). Spam jest to niepożądana masowa korespondencja docierająca na skrzynki poczty internetowej.

Jednym z rodzajów phishingu jest likejacking (ang. *likejacking*) polegający na zgromadzeniu fanów na danej stronie na Facebooku. Dana strona lub profil zachęca użytkownika, którego znajomy zamieścił pewną treść o atrakcyjnym temacie do przejścia na konkretną stronę internetową. Jednakże pod danym adresem nie znajduje się deklarowana zawartość, lecz skrypt, który automatycznie nadaje polubienie na stronie lub profilu bez wiedzy właściciela oraz umieszczana jest informacja o takiej reakcji użytkownika.

Tabnapping (ang. *tabnapping*), czyli porywanie zakładek także zalicza się do ataków phishingowych. Przy otwarciu wielu stron w przeglądarce podmieniana jest jedna spreparowaną przez cyberprzestępcę. Jeśli jest to strona do portalu społecznościowego lub bankowości elektronicznej, wpisując dane logowania przekazujemy je stronie, chcącej w nieuprawniony sposób je pozyskać.

Hakowanie (ang. *hacking*) jest często konieczny do popełnienia komputerowego czynu karalnego. Polega on na uzyskaniu dostępu do komputera, sieci komputerowej oraz danych w niej zawartych[58].

Cyberprzestępcy chcąc ukryć swoją tożsamość wykorzystują IP Spoofing (ang. *IP address spoofing*), czyli podszywanie się pod adresy IP (ang. *Internet Protocol*). W tym celu cyberprzestępcy używają narzędzi do modyfikowania źródła adresu w nagłówku pakietu, aby system urządzenia odczytał pakiet jako pochodzący z zaufanego źródła, takiego jak inny komputer i akceptuje go. Ponieważ dzieje się to na poziomie jednej sieci telekomunikacyjnej nie ma oznak manipulacji[59].

Cyberzagrożenia są nieodłączną częścią użytkowania sieci i systemów teleinformatycznych. Przeglądając portale aukcyjne można się natknąć, na próby wyłudzenia pieniędzy czy danych logowania do portalu lub bankowości elektronicznej. W niniejszym podrozdziale zwrócono uwagę na najczęściej spotykane cyberataki na użytkowników indywidualnych, firmy, korporacje czy organizacje.

Kryzys wywołany pandemią wirusa SARS-CoV-2 uwidocznił w jaki sposób cyberprzestępcy zdobywali przewagę nad nieświadomym społeczeństwem. Przestępcy internetowi dostosowali istniejące formy cyberprzestępczości do zaistniałej sytuacji. Ich działania nadużywały niepewności i zapotrzebowania opinii publicznej na wiarygodne informacje. We wszystkich dziedzinach funkcjonowania społeczeństw, od inżynierii społecznej do odmowy

[58] https://www.gov.pl/web/baza-wiedzy/zagr-techniczne, dostęp: 14.12.2020 r.
[59] https://www.kaspersky.com/resource-center/threats/ip-spoofing, dostęp: 16.01.2021 r.

usługi w wersji rozproszonej (DDoS), a także od oprogramowania ransomware[60] do dystrybucji materiałów przedstawiających seksualne wykorzystywanie dzieci, przestępcy nadużywali kryzysu, podczas gdy reszta społeczeństwa próbowała opanować sytuację[61].

Raport „Microsoft Digital Defence Report" z września 2020 roku zwraca uwagę na wyrafinowanie cyberataków w ciągu ostatniego roku. Do przeprowadzenia owych ataków przestępcy wykorzystali metody ułatwiające pozostanie anonimowym i zagrażające one nawet najbardziej odpornym celom. Grupy przestępcze przeniosły swoją działalność w chmury obliczeniowe, aby ukryć się wśród tysięcy legalnie działających firm. Napastnicy opracowali nowe sposoby przeszukiwania sieci w celu znalezienia systemów podatnych na oprogramowanie ransomware[62].

Kluczowymi statystykami, jeśli chodzi o trendy w obszarze cyberzagrożeń, według raportu firmy Microsoft są:

- zablokowanie dostępu użytkownikom do 13 miliardów złośliwych lub podejrzanych raportów z czego 1 miliard zawierał adresy URL utworzone w celu przeprowadzenia ataku phishingowego,
- w okresie od października 2019 roku do lipca 2020 roku najczęstszym powodem naruszenia bezpieczeństwa było złośliwe oprogramowanie typu ransomware,
- najpopularniejszymi technikami ataków stosowanych przez podmioty związane z poszczególnymi państwami w ostatnim roku to rozpoznanie, zbieranie danych logowania, złośliwe oprogramowanie i wykorzystanie wirtualnej sieci prywatnej (ang. *Virtual Private Network, skrót* VPN).

ENISA oraz Microsoft w swoich publikacjach są zgodne, że jednym z głównych zagrożeń cyberprzestrzeni w 2020 roku jest atak typu ransomware. Przestępcy wykorzystując kryzys wywołany pandemią wirusa SARS-CoV-2 skrócili czas przebywania w systemie ofiary ataku wierząc, że w wyniku wybuchu pandemii zwiększy się gotowość do zapłaty za zaszyfrowane pliki. Wzorce ataków pokazują, że przestępcy wiedzą, kiedy nastąpi moment zmniejszenia uwagi, który wpłynie na zdolność organizacji do wprowadzenia zmian zwiększenia odporności sieci teleinformatycznej. W niektórych przypadkach cyberprzestępcy przechodzili od pierwszego wejścia do systemu do żądania okupu w mniej niż 45 minut[63].

Kolejnym wyzwaniem 2020 roku stała się praca zdalna. Pandemia to dla cyberprzestępców wymarzony czas. O popularności ataków mających na

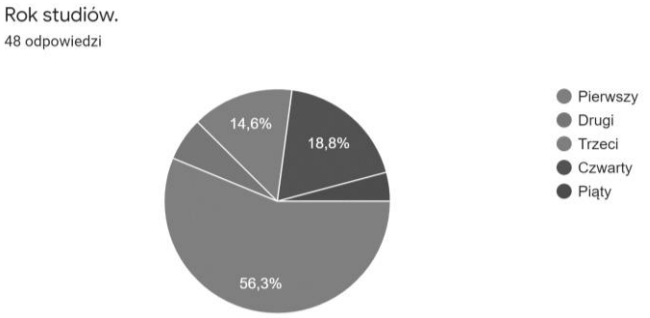
[60] Ransomware - (połączenie słów ang. *ransom* - okup software - *oprogramowanie*) złośliwe oprogramowanie wymuszające okup, szyfruje ono dostęp do systemu lub plików osobistych, a w zamian za odblokowanie ich żąda korzyści materialnych. Źródło: https://pl.malwarebytes.com/ransomware/, dostęp: 16.01.2021 r.
[61] EUROPOL *Internet Organised Crime Threat Assessment (IOCTA)* 2020 str.6.
[62] https://www.microsoft.com/en-us/security/business/security-intelligence-report, dostęp: 16.01.2021 r.
[63] Tamże

celu wyłudzanie danych logowania świadczy fakt, że aż 73% zbadanych przez CISO (ang. *Chief Information Security Officer*)[64] firmy Microsoft przyznaje, że w ciągu ostatnich 12 miesięcy doszło do wycieku danych w ich organizacji. W pierwszej połowie 2020 roku został zaobserwowany wzrost ataków polegających na przejęciu tożsamości użytkowników na kontach przedsiębiorstw[65]. Ważnym jest zatem, aby zadbać o właściwy poziom skomplikowania haseł i uwierzytelniania wieloskładnikowego[66].

Świadomość studentów Akademii Marynarki Wojennej w Gdyni na temat zagrożeń wynikających z użytkowania cyberprzestrzeni – wyniki badań

Badaniu diagnostycznemu poddano 49 ankietowanych w grupie studentów wojskowych. Uczestniczyli w nim podchorążowie Akademii Marynarki Wojennej, którzy w przyszłości mogą zostać oficerami Wojska Polskiego. Badanie przeprowadzono w grudniu 2020 roku z wykorzystaniem formularza ankiety za pośrednictwem narzędzia Formularze Google.

W jednym z pytań ustalono rozkład procentowy stażu studiów ankietowanych w Akademii Marynarki Wojennej. W większości na pytania zawarte w badaniu odpowiadali podchorążowie pierwszego roku (27 osób – 56,3%), kolejnymi grupami pod względem liczebności byli studenci czwartego roku (9 osób – 18,8%), trzeciego roku (7 osób – 14,6%), drugiego roku (3 osoby – 6,3%) oraz piątego roku (2 osoby – 4,2%). Procentowy rozkład roku studiów zaprezentowano na rysunku 5.1.



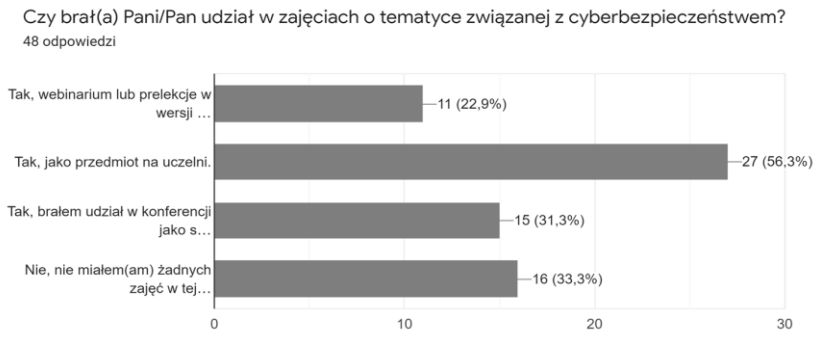
Źródło: Opracowanie własne na podstawie wyników badań.

[64] CISO (Chief Information Security Officer) to osoba, która odpowiedzialna jest w organizacji za całość działań, zasad oraz regulacji z ogólnie pojętym bezpieczeństwem informatycznym, źródło: https://ciso.org.pl/, dostęp: 11.01.2021 r.
[65] Microsoft *Digital Defence Report 2020*, źródło: https://www.microsoft.com/en-us/security/business/security-intelligence-report, dostęp: 16.01.2021 r.
[66] Uwierzytelnianie wieloskładnikowe - model uzyskania dostępu, w którym wymagane jest potwierdzenie tożsamości w sposób dodatkowy. Oprócz loginu i hasła jest potrzebne, przykładowo, zatwierdzenia logowania poprzez generowany kod przesłany na adres e-mail.

Rysunek 5.1. Rozkład procentowy odpowiedzi ankietowanych na pytanie , ,Rok studiów"

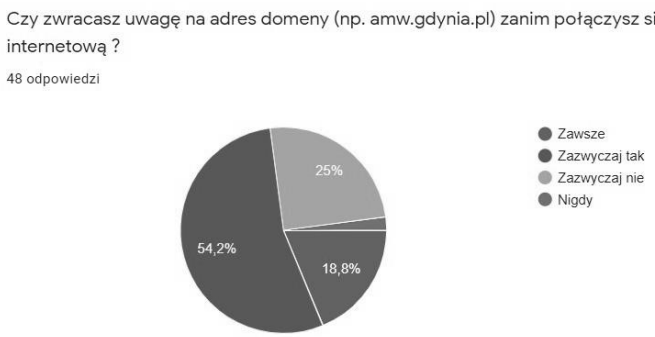
Badanych zapytano o uczestnictwo w zajęciach o tematyce związanej z cyberbezpieczeństwem. Pytanie to miało możliwość odpowiedzi wielokrotnego wyboru z jednoczesną możliwością udzielenia własnej odpowiedzi. Spośród 48 ankietowanych osób, 11 (22,9%) brało udział w webinarium lub prelekcji w wersji online, 27 osób (56,3%) jako przedmiot na uczelni, 15 osób (31,3%) brał udział w konferencji jako słuchacz, a 16 osób (33,3%) nie miało żadnych zajęć w tej tematyce. W pytaniu drugim zostało wykazane, że większość wypełniających to osoby znajdujące się na pierwszym roku. W tym przypadku mogło być to spowodowane brakiem odpowiednich zajęć we wcześniejszych etapach szkolnictwa, gdyż w programie nauczania obowiązkowym jest przedmiot z bezpieczeństwa cybernetycznego, jednakże odbywa się on na czwartym roku. Rozkład odpowiedzi ankietowanych przedstawiono na rysunku 5.2.

Pod jednym adresem domeny może znajdować się maksymalnie jedna strona internetowa, jednakże są znaki, które umieszczone obok siebie mogą wizualnie przypominać inna literę np., „rn" na pierwszy rzut oka może wyglądać jak litera „m". W przypadku, gdy nie zwraca się uwagi na adres domeny można połączyć się ze stroną internetową, która będzie pobierze złośliwe oprogramowanie na urządzenie użytkownika. Wobec tego ankietowanych zapytano, czy zwracają uwagę na adres domeny przed połączeniem się z nią. Ponad połowa, czyli 26 ankietowanych (54,2%) odpowiedziało, że zazwyczaj zwraca uwagę na adres domeny strony internetowej, 9 osób (18,8%) odpowiedziało, że zawsze zwraca na uwagę na adres domeny, 12 respondentów (25%) odpowiedziało, że zazwyczaj tego nie robi, a jedna osoba (2,1%) odpowiedziała, że nigdy nie zwraca uwagi na adres domeny. Rozkład odpowiedzi respondentów przedstawiono na rysunku 5.3.



Źródło: Opracowanie własne na podstawie wyników badań.

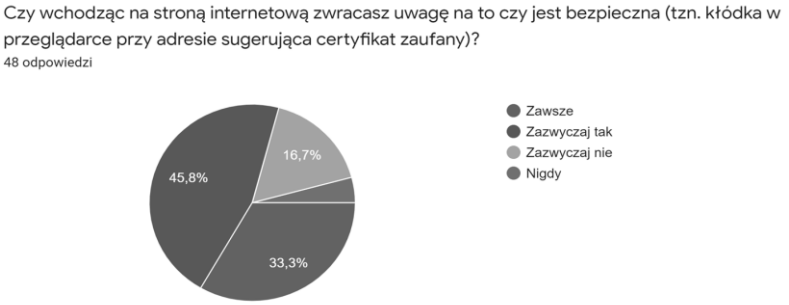
Rysunek 5.2. Rozkład procentowy odpowiedzi ankietowanych na pytanie ,,Czy brał(a) Pani/Pan udział w zajęciach o tematyce związanej z cyberbezpieczeństwem?"



Źródło: Opracowanie własne na podstawie wyników badań.

Rysunek 5.3. Rozkład procentowy odpowiedzi ankietowanych na pytanie ,,Czy zwracasz uwagę na adres domeny (np. amw.gdynia.pl) zanim połączysz się ze stroną internetową"

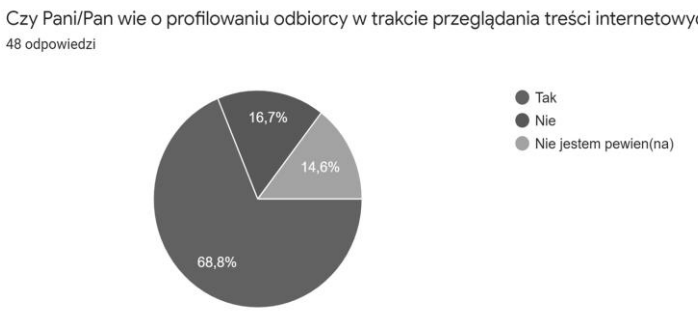
Wchodząc na stronę stosującą protokół HTTPS, jej serwer potwierdza jej tożsamość w przeglądarce. Można przez to rozumieć, że strony nie posiadające certyfikatu mogą być stronami niebezpiecznymi. Pytanie zbliżone tematycznie do poprzedniego pozwoliło poznać zwyczajowość ankietowanych przy zwracaniu uwagi na posiadanie certyfikatu zaufanego przez odwiedzaną stronę internetową. Spośród ankietowanych 22 osoby (45,8%) zazwyczaj zwracają uwagę na certyfikat zaufany, 16 osób (33,3%) robi to zawsze, 8 osób (16,7%) zazwyczaj nie zwraca uwagi na certyfikat zaufany, a 2 ankietowanych (4,2%) nigdy nie zwraca na to uwagi. Procentowy rozkład odpowiedzi ankietowanych przedstawiono na rysunku 5.4.



Źródło: Opracowanie własne na podstawie wyników badań.

Rysunek 5.4. Rozkład procentowy odpowiedzi ankietowanych na pytanie ,,Czy wchodząc na stronę internetową zwracasz uwagę na to czy jest bezpieczna (tzn. kłódka w przeglądarce przy adresie sugerująca certyfikat zaufany)?"

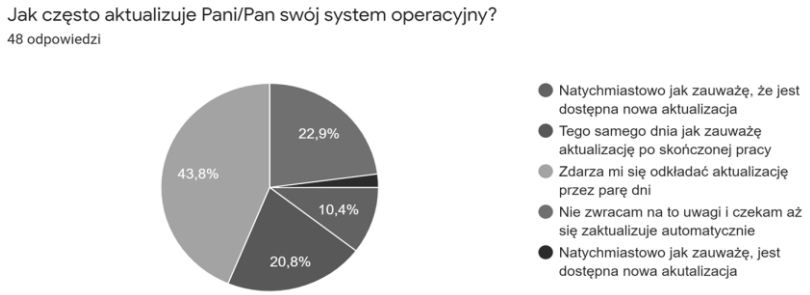
Respondentów zapytano również o świadomość na temat profilowania użytkownika treści internetowych w trakcie ich przeglądania. Większość respondentów (33 osoby - 68,8%) udzieliło odpowiedzi twierdzącej na zadane pytanie. Negatywnie odpowiedziało 8 (16,7%) ankietowanych, a 7 respondentów (14,6%) oświadczyło brak pewności swojej wiedzy, aby jednoznacznie odpowiedzieć na to pytanie. Odpowiedzi przedstawiono na rysunku 5.5.



Źródło: Opracowanie własne na podstawie wyników badań.

Rysunek 5.5. Rozkład procentowy odpowiedzi ankietowanych na pytanie ,,Czy Pan/Pani wie o profilowaniu odbiorcy w trakcie przeglądania treści internetowych?"

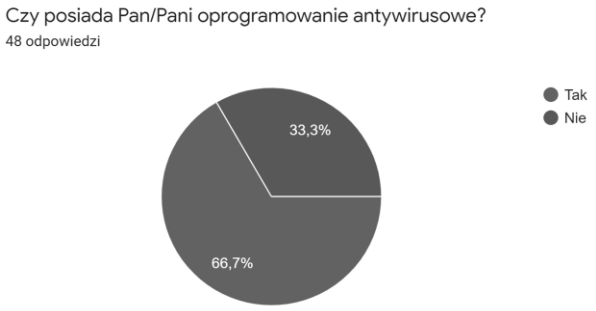
Aktualizowanie systemu operacyjnego pomaga podnieść poziom bezpieczeństwa użytkowania urządzenia. Wykorzystanie luki w systemie operacyjnym jest zagrożeniem, którego użytkownicy powinni się obawiać. Dostawcy oprogramowania aktualizując system często wprowadzają poprawki usuwające daną podatność systemu. Studenci nie aktualizujący swojego systemu operacyjnego są bardziej podatni na zagrożenia. Dlatego badanym zadano pytanie o częstotliwość aktualizowania swojego systemu operacyjnego. Z udzielonych odpowiedzi wynika, 6 osób (12,5%) na 48 respondentów aktualizuje swój system operacyjny natychmiastowo, 21 osobom (43,8%) zdarza się odkładać aktualizację parę dni, 10 osób (20,8%) aktualizuje system operacyjny tego samego dnia po skończonej pracy, a 11 osób (22,9%) nie zwraca na to uwagi na nowe aktualizacje i czeka aż system operacyjny sam się zaktualizuje. Odpowiedzi przedstawiono na rysunku 5.6.



Źródło: Opracowanie własne na podstawie wyników badań.

Rysunek 5.6. Rozkład procentowy odpowiedzi ankietowanych na pytanie ,,Jak często aktualizuję Pani/Pan swój system operacyjny?"

Brak oprogramowania antywirusowego może spowodować, że studenci są bardziej podatni na ataki cyberprzestępców. Wobec tego badanych zapytano, czy posiadają oprogramowanie przeznaczone do detekcji wirusów. Spośród 48 ankietowanych 32 (66,7%) odpowiedziało twierdząco na to pytanie, a 16 (33,3%) negatywnie. Rozkład odpowiedzi ankietowanych przedstawiono na rysunku 5.7.

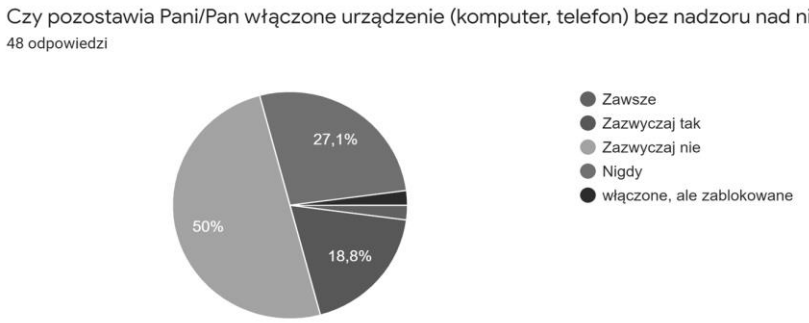


Źródło: Opracowanie własne na podstawie wyników badań.

Rysunek 5.7. Rozkład procentowy odpowiedzi ankietowanych na pytanie ,,Czy posiada Pani/Pan oprogramowanie antywirusowe?"

Pozostawienie urządzenia gotowego do użytku bez wcześniejszego zablokowania lub wyłączenia go może skutkować tym, że osoba nieuprawniona uzyska dostęp do zawartości urządzenia. Studenci, którzy zostawiają swoje urządzenia włączone, nie zablokowane i bez nadzoru muszą się liczyć z nieupoważnionym dostępem do niego. Dlatego respondentom zadano pytanie, czy pozostawiają włączone urządzenie (telefon, komputer) bez nadzoru na nim. Spośród ankietowanych 48 osób, 24 stwierdziło, że zazwyczaj nie pozostawia urządzenia włączonego bez jakiegokolwiek nadzoru nad nim, a 27,1% (13

osób), że nigdy tego nie robi, 9 osób (18,8%) zazwyczaj zostawia swoje włączone urządzenia bez jakiegokolwiek nadzoru, a po 1 osobie (2,1%) stwierdziło, że zawsze zostawia swoje urządzenie bez nadzoru oraz, że pozostawia je włączone, ale zablokowane. Rozkład odpowiedzi przedstawiono na rysunku 5.8.

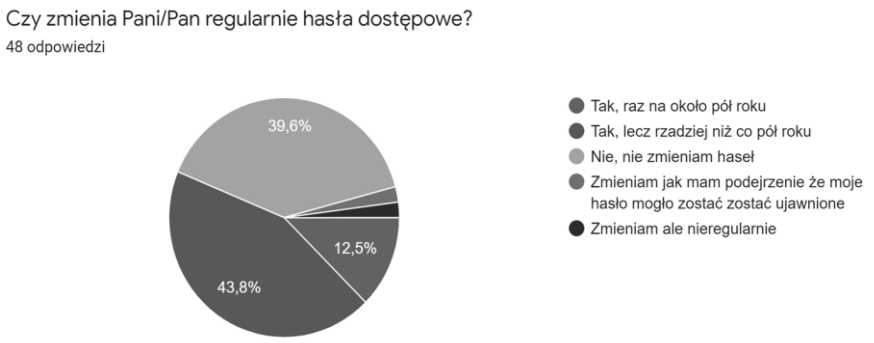


Źródło: Opracowanie własne na podstawie wyników badań.

Rysunek 5.8. Rozkład procentowy odpowiedzi ankietowanych na pytanie ,,Czy pozostawia Pani/Pan włączone urządzenie (komputer, telefon) bez nadzoru nad nim?"

Badanym zadano pytanie, czy regularnie zmieniają hasła dostępowe. Norma ISO/IEC zaleca zmianę hasła w regularnym odstępie czasowym i w każdym przypadku wzbudzającym podejrzenie ujawnienia hasła[67]. Spośród 48 ankietowanych osób, 19 (39,6%) nie zmienia swoich haseł dostępowych, a 43,8% (21 osób) robi to rzadziej niż co pół roku, 6 osób, czyli 12,5% ankietowanych zmienia swoje hasła raz na około pół roku oraz po jednej osobie odpowiedziało, że zmienia hasła, ale nieregularnie i jak posiada podejrzenie, że hasło mogło zostać ujawnione. Rozkład odpowiedzi przedstawiono na rysunku 5.9.

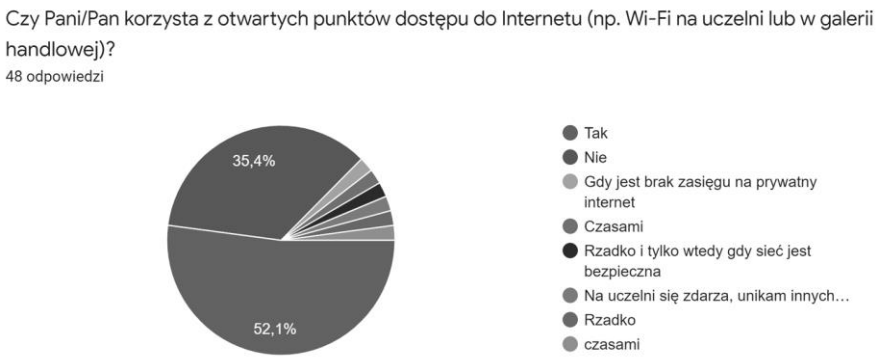
[67] ISO/IEC 27032:2012(en).



Źródło: Opracowanie własne na podstawie wyników badań.

Rysunek 5.9. Rozkład procentowy odpowiedzi ankietowanych na pytanie ,,Czy zmienia Pani/Pan regularnie hasła dostępowe?"

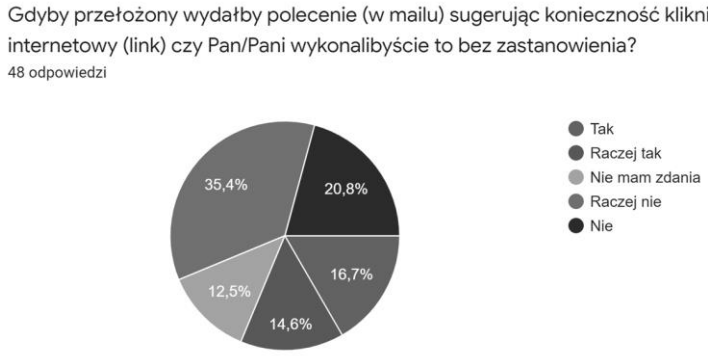
Użytkownicy Internetu korzystający z otwartych punków dostępowych narażają się na podsłuchanie przez cyberprzestępcę, a co za tym idzie na utratę np. danych logowania. Wobec tego respondentom zadano pytanie odnośnie do korzystania z otwartych punktów dostępu do Internetu. Ponad połowa (25 osób - 52,1%) odpowiedziała, że korzysta z otwartych punktów dostępu oraz w sumie co ósmy ankietowany przyznał się, że zdarza mu się okresowo. 17 osób zadeklarowało, że nie korzysta z otwartych punktów dostępu do Internetu. Rozkład procentowy odpowiedzi ankietowanych przedstawiono na rysunku 5.10.



Źródło: Opracowanie własne na podstawie wyników badań.

Rysunek 5.10. Rozkład procentowy odpowiedzi ankietowanych na pytanie ,,Czy Pani/Pan korzysta z otwartych punktów dostępu do Internetu (np. Wi-Fi na uczelni lub w galerii handlowej)?"

Ankietowanych poproszono o odpowiedź na pytanie „Gdyby przełożony wydałby polecenie (w mailu) sugerując konieczność kliknięcia na odnośnik internetowy (link) czy Pan/Pani wykonalibyście to bez zastanowienia?". Spośród 48 ankietowanych odpowiedzi „Nie" udzieliło 10 osób, co stanowi 20,8%, odpowiedzi „Raczej nie" udzieliło 17 osób, co stanowi 35,4%, odpowiedzi „Nie mam zdania" udzieliło 6 osób, co stanowi 12,5%, odpowiedzi „Raczej tak" udzieliło 7 osób, co stanowi 14,6%, odpowiedzi „Tak" udzieliło 8 osób, co stanowi 16,7%. Odpowiedzi przedstawiono na rysunku 5.11.



Źródło: Opracowanie własne na podstawie wyników badań.

Rysunek 5.11. Rozkład procentowy odpowiedzi ankietowanych na pytanie „Gdyby przełożony wydałby polecenie (w mailu) sugerując konieczności kliknięcia na odnośnik internetowy (link) czy Pan/Pani wykonalibyście to bez zastanowienia?"

Metodologia

Praca została napisana na podstawie dokładnej analizy materiałów zwartych, artykułów naukowych oraz rzetelnych stron internetowych na podstawie, których poddano analizie pojęcie cyberprzestrzeni, zdefiniowano również cyberzagrożenia, przedstawiono najczęściej występujące oraz podzielono je na techniczne i społeczne. Badanie zostało przeprowadzone metodą sondażu diagnostycznego, techniką ankiety. Celem ankiety było poznanie poziomu świadomości studentów Akademii Marynarki Wojennej w Gdyni ta temat zagrożeń idących z użytkowania cyberprzestrzeni. Niniejsze badanie było istotnym przyczynkiem do identyfikacji i charakterystyki poziomu bezpieczeństwa użytkowania oraz świadomości na temat zagrożeń wynikających z korzystania z cyberprzestrzeni.

Przegląd literatury

W celu analizy pojęcia cyberprzestrzeni wykorzystano pozycje tj.: „*Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru"* Macieja Marczyka, „*Department of Defense Dictionary of Military and Associated Terms"* Joint Publication 1-02. Wpływ na przedstawienie cyberzagrożeń miały wpływ raporty „ *Digital Defence Report"* firmy Microsoft z 2020 roku oraz „ *Internet Organised Crime Threat Assessment (IOCTA)"* Europolu również z 2020 roku. Na podstawie wiedzy zgromadzonej, między innymi, w tych pozycjach przeprowadzone zostało badanie ankietowe.

Wnioski

Celem było poznanie poziomu świadomości studentów Akademii Marynarki Wojennej w Gdyni na temat zagrożeń w cyberprzestrzeni. Analiza materiałów źródłowych, rzetelnych stron internetowych oraz artykułów naukowych była istotnym przyczynkiem do analizy pojęcia cyberprzestrzeni, cyberzagrożeń oraz pozwoliła stworzyć ankietę, dzięki której możliwe było poznanie poziomu świadomości studentów Akademii Marynarki Wojennej w Gdyni na temat cyberzagrożeń.

Badanie ankietowe zostało przeprowadzone na grupie 48 studentów Akademii Marynarki Wojennej wykazało, że stan wiedzy na temat cyberzagrożeń wynikających z użytkowania cyberprzestrzeni jest na niewystarczający. Spośród 48 respondentów poszczególne jednostki nie wykazały się wiedzą, co potwierdza przyjętą hipotezę. Między innymi brak aktualizowania systemu operacyjnego czy posiadania programu antywirusowego wskazuje na niekompletną widzę w dziedzinie cyberbezpieczeństwa. Ankietę wypełnili w większości podchorążowie pierwszego roku aspirujący do bycia oficerem Sił Zbrojnych Rzeczypospolitej Polskiej. Proces nauczania, dzięki któremu świadomość może zostać podniesiona jest w toku, jednakże faktem jest, że osoby nieposiadające dostatecznego poziomu wiedzy nadal mogą być użytkownikami Internetu.

Reasumując, studenci Akademii Marynarki Wojennej powinni pracować nad praktykami zapewniającymi im bezpieczeństwo w cyberprzestrzeni. Dynamicznie zmieniający się charakter zagrożeń wymusza konieczność stałego śledzenia, poszerzania i uzupełniania wiedzy. Obok oprogramowania chroniącego użytkownika cyberprzestrzeni powinna stać świadomość zagrożeń. Opracowanie wyników badań stanowi bazę wiedzy dla studentów wskazując istotność problemu, umożliwiającą poszerzanie swojej wiedzy oraz analizy własnych działań w cyberprzestrzeni.

Bibliografia

Opracowania zwarte

1. Hoffman T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*, FNCE, Poznań 2018.
2. Juszczyk S., *Internet -współczesne medium komunikacji społecznej*, Uniwersytet Śląski, Katowice 2010.
3. Michniak J., *Dowodzenie i łączność,* AON, Warszawa 2003.
4. Ottis R., Lorents P., *Cyberspace: Definition and Implications,* Cooperative Cyber Defence Centre of Excellence, Tallinn, Tallinn 2010.
5. Stallings W., *Computer security: principles and practice*, Pearson, Boston 2012.
6. Tanenbaum A. S., *Sieci komputerowe*, Helion, Gliwice 2004.

Artykuły

1. Fabjaniak-Czerniak K., *Internetowe media społecznościowe jako* narzędzie *public relations* [w:] K. Kubiak, *Zarządzanie w sytuacjach kryzysowych niepewności*, Wyższa Szkoła Promocji Warszawa 2012.
2. Kotyśko M., *Nadmierne korzystanie z sieci społecznościowych*, „Alkoholizm i Narkomania", nr 27(2)/2014.
3. Marczyk M., *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru, „*Przegląd Teleinformatyczny" nr 1-2/2018.
4. Ochab M., *Cyberprzestrzeń jako środowisko społeczeństwa obywatelskiego w Brazylii,* „Teka of Political Science and International Relations – OL PAN/UMCS", nr 13(2)/2018.
5. Pęczak A., *Porywacze przeglądarek*, PC World, nr 4/2014.
6. Taghavi Zargar S., *A Survey of Defence Mechanisms Against Distributed Denial of Service (DDos) Flooding Attacks IEEE Communications Surveys & Tutorials,* Chiao Tung, 2013.
7. Terebiński B., *Bezpieczeństwo teleinformatyczne jako podstawa funkcjonowania współczesnego państwa,* „Obronność" nr 1(25)/2018.

Źródła internetowe

1. http://maryl.org/wp-content/uploads/2013/12/Gumkowska-Maryl-i-Toczyski-2009-Blog-to-blog.pdf, dostęp: 16.01.2021 r.
2. https://azure.microsoft.com/pl-pl/overview/what-is-cloud-computing/, dostęp: 16.01.2021 r.
3. https://blog.malwarebytes.com/glossary/bundleware/, dostęp: 14.12.2020 r.
4. https://ciso.org.pl/, dostęp: 11.01.2021 r.

5. https://dictionary.cambridge.org/pl/dictionary/english/hosting, dostęp: 15.01.2021 r.
6. https://encyklopedia.pwn.pl/haslo/3890542/dane.html, dostęp: 10.01.2021 r.
7. https://encyklopedia.pwn.pl/haslo/ignorantia-iuris-nocet-ignorantia-facti-non-nocet;3914000.html, dostęp: 09.01.2021 r.
8. https://jko.jten.mil/docs/JKO_Fact_Sheet_(July%202020).pdf, dostęp: 16.01.2021 r.
9. https://pbi.org.pl/raporty/polscy-internauci-we-wrzesniu-2020/, dostęp: 17.11.2020 r.
10. https://pl.malwarebytes.com/adware/, dostęp: 11.01.2021 r.
11. https://pl.wikipedia.org/wiki/Sexting, dostęp: 16.01.2021 r.
12. https://sjp.pl/cyberzagro%C5%BCenie, dostęp: 07.12.2020 r.
13. https://sjp.pwn.pl/sjp/afiliacja;2548962.html, dostęp: 09.01.2021 r.
14. https://sjp.pwn.pl/szukaj/hedonizm.html, dostęp: 09.01.2021 r.
15. https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/1908,pojecie.html, dostęp: 17.11.2020 r.
16. https://tools.ietf.org/html/rfc760, dostęp: 11.01.2021 r.
17. https://us-cert.cisa.gov/ncas/tips/ST04-015, dostęp: 22.12.2020 r.
18. https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media, dostęp: 11.01.2021 r.
19. https://wearesocial-net.s3.amazonaws.com/uk/wp-content/uploads/sites/2/2020/01/11-Social-Platform-Ranking-%E2%80%93-DataReportal-Digital-2020-Global-Digital-Overview-Slide-95.png, dostęp: 12.01.2021 r.
20. https://wireless-network-support.blogspot.com/2009/08/what-is-lan-wlan-wan-man-san-can-pan.html, dostęp: 10.01.2021 r.
21. https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html, dostęp: 11.01.2021 r.
22. https://www.collinsdictionary.com/dictionary/english/troll, dostęp: 16.01.2021 r.
23. https://www.cyberdefence24.pl/zysk-finansowy-wazniejsza-motywacja-cyberatakow-niz-szpiegostwo, dostęp: 08.01.2021 r.
24. https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020, dostęp: 31.12.2020 r.
25. https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/botnets, dostęp: 11.01.2021 r.
26. https://www.gov.pl/web/baza-wiedzy/zagroz-nietechniczne-spoleczne, dostęp: 14.12.2020 r.

27. https://www.gov.pl/web/baza-wiedzy/zagr-techniczne, dostęp: 14.12.2020 r.
28. https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024, dostęp: 16.01.2021 r.
29. https://www.kaspersky.com/resource-center/definitions/spear-phishing, dostęp: 08.01.2021 r.
30. https://www.kaspersky.com/resource-center/definitions/spear-phishing, dostęp: 16.01.2021 r.
31. https://www.kaspersky.com/resource-center/threats/ip-spoofing, dostęp: 16.01.2021 r.
32. https://www.microsoft.com/en-us/security/business/security-intelligence-report, dostęp: 16.01.2021 r.

Inne

1. DOD *Standard Internet Protocol*, DARPA, Information Sciences Institute.
2. Doktryna systemów teleinformatycznych D-6(A), 2019, CDiSSZ.
3. EUROPOL Internet Organised Crime Threat Assessment (IOCTA) 2020.
4. ISO/IEC 27032:2012(en).
5. Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms, 2020.
6. Joint Publication 3-12, Cyberspace Operations, 2018.
7. Tomczuk P., Social media jako element zintegrowanej komunikacji firm, Szkolenie Social media w komunikacji zewnętrznej i wewnętrznej firm z dn. 29.04.2010 r. organizowane przez Ciszewski Financial Communications, Ciszewski Public Relations oraz portal PRoto.pl.
8. Microsoft Digital Defence Report 2020.

bsm. pchor. Dawid JUTRZENKA TRZEBIATOWSKI

BEZPIECZEŃSTWO INFORMACJI NIEJAWNYCH W SYSTEMACH TELEINFORMATYCZNYCH SIŁ ZBROJNYCH RZECZYPOSPOLITEJ POLSKIEJ

Streszczenie

Ochrona informacji niejawnych jest nieodłącznym elementem funkcjonowania instytucji wojskowych we współczesnym świecie. Zawarte w artykule aspekty zarówno prawne jak i praktyczne funkcjonują w systemach teleinformatycznych Sił Zbrojnych Rzeczypospolitej Polskiej. Opisano zasady i metody bezpiecznego przetwarzania danych niejawnych. Została przedstawiona struktura organizacyjna oraz wskazane i scharakteryzowane podmioty odpowiedzialne za ich bezpieczeństwo. Zobrazowano klasyfikację informacji niejawnych poprzez klauzule tajności. Omówione zostały wybrane zagrożenia dla systemów przetwarzających informacje niejawne. Przytoczono wybrane metody zwalczania zagrożeń. Wskazano również dobre praktyki dla prawidłowego funkcjonowania systemów teleinformatycznych.

Słowa kluczowe:
informacje niejawne, systemy teleinformatyczne, sieci telekomunikacyjne, zagrożenia.

Abstract

Security of classified information in ICT systems of the Armed Forces of the Republic of Poland

The protection of classified information is an integral part of the functioning of military institutions in the modern world. The legal and practical aspects contained in the article function in the ICT systems of the Armed Forces of the Republic of Poland. Principles and methods of safe processing of classified data are described. The organizational structure was presented, as well as the indicated and characterized entities responsible for their safety. The classification of classified information by the confidentiality clauses was depicted. Selected threats to systems processing classified information were discussed. Selected methods of fighting threats are presented. Good practices for the proper functioning of ICT systems were also indicated.

Keywords:
Classified information, ICT systems, telecommunications networks, threats.

Wstęp

Ochrona informacji niejawnych od zawsze była istotna w aspekcie zapewnienia bezpieczeństwa państwa. Ich ochrona jest nieodzownym elementem funkcjonowania instytucji wojskowych we współczesnym świecie. Szczególnie w Siłach Zbrojnych Rzeczypospolitej Polskiej (SZ RP), informacje te przetwarzane są na wiele różnych sposobów, nie tylko za pośrednictwem drogi papierowej, lecz również w nieustannie rozwijających się systemach teleinformatycznych, które stanowią dzisiaj podstawę do podjęcia jakichkolwiek działań. *„System bezpieczeństwa informacji opiera się na normach prawa oraz tworzonych na jego podstawie metodykach działań ochronnych”*[1]. Wszelkie informacje niejawne w siłach zbrojnych są objęte przepisami prawnymi i aktami normatywnymi, które w jasny sposób dyktują warunki ich przetwarzania oraz są zintegrowane w jednolity system ochrony. Należy jednak zauważyć, że ustawy, czy wynikające z nich rozporządzenia muszą być stale nowelizowane i aktualizowane, gdyż rozwój technologii często wyprzedza zapisy prawne. Ekspansja w obszarze informatyki stale tworzy nowe sposoby przekazywania informacji, chociażby za pośrednictwem wydzielonych sieci komputerowych. Rozwój w sposobach elektronicznego przekazu danych wywołuje bezpośrednią potrzebę wprowadzania pionierskich rozwiązań ich ochrony.

Bezpieczeństwo informacji niejawnych wymaga nie tylko odpowiedniego zabezpieczenia systemowego, prawnego czy fizycznego, ale również odpowiedniego poziomu świadomości osób, które mają z nimi styczność.

Niniejsze opracowanie oparto głównie o analizę i krytykę Ustawy z dnia 5 sierpnia 2010 r. oraz wynikających z niej rozporządzeń, literatury naukowej, publikacji naukowych jak i również źródeł internetowych.

System zarządzania bezpieczeństwem informacji niejawnych

Właściwe przedstawienie pojęcia informacji niejawnej należy zacząć od przedstawienia ogólnego pojęcia informacji, często przyjmowanej za termin powszechnie rozumiany przez ludzi nauki. Informacja zależnie od kontekstu, w którym występuje może być rozpatrywana w różnorodny sposób. Definicję, w podejściu infologicznym Börje Langefors przedstawia wzorem:

$$I = i(D, S, t)$$

gdzie:
I - informacja
i - proces interpretacji
D - dane
S - przedwiedza
t – czas

[1] S. Zalewski, *Ochrona informacji niejawnych wybrane zagadnienia bezpieczeństwa osobowego,* Wydawnictwo Naukowe NOVUM, Płock 2014, s. 7.

W oparciu o taki wzór, stwierdzono, że *„informacja to proces interpretacji danych w oparciu o posiadaną wiedzę a priori w czasie”*[2]. Jak przedstawiono w definicji pojęcie „priori”, w bezpośrednim tłumaczeniu z łac. *„z założenia”*[3], można rozumieć jako coś wrodzonego, nie wynikającego z wcześniejszego doświadczenia. Wnioski jakie wysunięto przedstawiają się następująco: w zależności od konkretnej osoby, z określonych danych informacja będzie odbierana w różny sposób.

W aspekcie systemów teleinformatycznych i przetwarzanych w nich informacji zostało to zdefiniowane przez normę ISO, w której zapisano: *„Przez określenie informacja (w przetwarzaniu informacji rozumie się wiedzę dotyczącą obiektów takich jak fakty, zdarzenia, przedmioty, procesy lub idee zawierające koncepcje, mające w określonym kontekście określone znaczenie”*[4]. Z podanej definicji wywnioskowano, że w przetwarzaniu informacji samą informację definiuje wiedza, która dotyczy konkretnych kwestii oraz zawiera w ustalonym kontekście dane znaczenie.

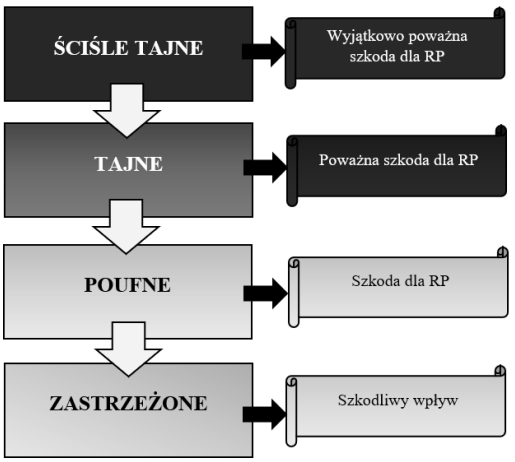
Informacje niejawne to nie tylko takie, które same w sobie zawierają czynniki mogące mieć zły wpływ na przykład dla danej jednostki organizacyjnej, ale jak zapisał Krzysztof Liderman takie *„które stają się takie w powiązaniu z innymi informacjami, pozwalając wyciągnąć prawidłowe wnioski…”*[5].

Klasyfikowanie informacji niejawnych

Informacja, aby mogła być objęta ochroną oraz żeby można jej było nadać klauzulę tajności musi zostać zaklasyfikowana przez uprawnioną do tego osobę. *„Informacja niejawna to informacja, której nadano klauzulę”*[6]. Poprzez osobę uprawioną dana informacja jest oceniana oraz klasyfikowana pod względem potencjalnych szkód jakie niesie za sobą jej ujawnienie dla interesów Rzeczypospolitej Polskiej lub danej jednostki organizacyjnej, która ją wpuściła do systemu, a następnie nadawana jest jej jedna z trzech klauzuli tajności. Rozpoczynając klasyfikacje informacji rozważa się najpierw jej istotność i przeznaczenie. Istotne jest wykluczenie incydentalnych osób w dostępie do takich informacji i określenie potrzeb ich współdzielenia. Taka fragmentacja informacji pozwala na dobranie odpowiedniej klauzuli, co za tym idzie odpowiednich środków zabezpieczenia, ochrony, przetwarzania i niszczenia[7].

[2] https://r.uek.krakow.pl/bitstream/123456789/2297/1/164861786.pdf, dostęp: 03.12.2020 r.
[3] https://iep.utm.edu/apriori/, dostęp: 27.10.2020 r.
[4] M. Kowalewski, J. Kowalewski, *Polityka bezpieczeństwa informacji w praktyce,* Wydawnictwo PRESSCOM Sp. z o. o., Wrocław 2014 r., s. 19.
[5] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa 2009, s. 11.
[6] M. Jabłoński, T. Radziszewski, *„Bezpieczeństwo fizyczne i teleinformatyczne informacji niejawnych”*, Wydawnictwo PRESSCOM Sp. z o. o., Wrocław 2012, s. 29-30.
[7] T. Polaczek, *Audyt bezpieczeństwa informacji w praktyce*, Wyd. Helion, 2014 r., s. 37.

Ustawa o ochronie informacji niejawnych wprowadziła nowy podział klauzul, kolejno od najwyższej ściśle tajne, tajne, poufne i zastrzeżone[8]. Rysunek 6.1 graficznie obrazuje klauzule informacji niejawnych.



Źródło: Opracowanie własne na podstawie Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych

Rysunek 6.1. Klauzule informacji niejawnych.

W rozporządzeniu Prezesa Rady Ministrów z dnia z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności określono w §4 poszczególne symbole i oznaczenia dla danej klauzuli tajności, są to kolejno[9]:

- „00" - ściśle tajne;
- „0" - tajne;
- „Pf" - poufne;
- „Z" - zastrzeżone.

Struktura organizacyjna systemu ochrony informacji niejawnych w Siłach Zbrojnych Rzeczypospolitej Polskiej

Formalizacja, hierarchiczny podział elementów i osób odpowiedzialnych to nieodzowny element organizacji wszelkich systemów, a zwłaszcza systemu ochrony informacji niejawnych bez których nie byłby w stanie funkcjonować prawidłowo. W SZ RP taka struktura stanowi podstawy do jego funkcjonowania i podjęcia jakichkolwiek działań. Struktury kształtowane są

[8] Ustawa z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych.
[9] Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności.

poprzez wypełnianie pewnych zasad, są to m.in. zasada jednolitości, zasada sprawnego działania i zasada fachowości[10].

W Polsce struktura organizacyjna systemu ochrony informacji niejawnych jest w głównej części definiowana poprzez ustawę o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. i rozporządzenia Prezesa Rady Ministrów. Ustawa reguluje istnienie pionu ochrony w Ministerstwie Obrony Narodowej jako Departament Ochrony Informacji Niejawnych, który odpowiada za system ochrony informacji niejawnych w resorcie zgodnie z decyzją nr 40 Ministra Obrony Narodowej z dnia 22 listopada 2006 r.[11]. Departament pełni funkcję zapewnienia jednolitego i sprawnego systemu ochrony informacji niejawnych poprzez wsparcie pełnomocnika MON w Ministerstwie i jednostkach jemu podległych oraz przez niego nadzorowanych. Ministrowi Obrony Narodowej podporządkowany jest pełnomocnik, który wykonuje szereg zadań mających na celu między innymi, zapewnienie ochrony systemom teleinformatycznym do przetwarzania informacji niejawnych. W aspekcie omawianego tematu została zwrócona szczególna uwaga na Oddział Ochrony Systemów Teleinformatycznych, który wchodzi w skład Departamentu Ochrony Informacji Niejawnych. Na czele oddziału stoi Szef, który ma pod swoją jurysdykcją specjalistów w zakresie tworzenia norm, nadzorowania prowadzenia kontroli czynności związanych z ochroną informacji niejawnych w systemach teleinformatycznych poprzez resort obrony narodowej oraz podległe jemu jednostki[12].

Zgodnie z rozdziałem 3 art. 10 ust. 2 Ustawy o ochronie informacji niejawnych dla Ministerstwa Obrony Narodowej i dla jednostek podległych Ministrowi organem nadzorującym jest Służba Kontrwywiadu Wojskowego jako delegatura Agencji Bezpieczeństwa Wojskowego. Współpraca tych dwóch organów jest określona na drodze rozporządzenia Prezesa Rady Ministrów. Art. 11 ust. 3 przedstawia Szefa SKW jako osobę odpowiedzialną za krajową władzę bezpieczeństwa w zakresie bezpieczeństwa systemów teleinformatycznych przetwarzających informacje niejawne.

W świetle prawa obowiązującego w Polsce ochrona informacji niejawnych w jednostce organizacyjnej spoczywa na jej kierowniku, który jest zgodnie z art.14 tej ustawy odpowiedzialny za ochronę przetwarzanych informacji niejawnych, a w szczególności za jej zorganizowanie i niezakłócone funkcjonowanie. Co więcej kierownik jednostki organizacyjnej jest zobowiązany do przejścia szeregu szkoleń co opisuje art. 19 ustawy. W zakresie egzekwowania przestrzegania obowiązujących przepisów kierownikowi podporządkowuje się pełnomocnika ochrony, który posiada zaświadczenie o przejściu szkolenia w zakresie informacji niejawnych wystawianym przez SKW lub ABW, czy też

[10] S. Topolewski, *Ochrona informacji niejawnych w Siłach Zbrojnych Rzeczypospolitej Polskiej*, Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego, Siedlce 2017, s. 290.
[11] Tamże, str. 290
[12] Tamże, s. 309.

byłe Wojskowe Służby Informacyjne[13]. W rozporządzeniu Ministra Obrony Narodowej z dnia 19 grudnia 2013 r. opisano pełnomocnika ochrony w danej jednostce organizacyjnej jako osobę realizującą szereg działań związanych między innymi z planowaniem, określaniem zadań dla pionów ochrony, kierowaniem pracami nad projektami ochrony informacji niejawnych czy opiniowaniem i uzgadnianiem dokumentów organizacyjno-etatowych[14]. W przypadku systemów teleinformatycznych, kierownik jednostki organizacyjnej wyznacza również administratora systemu, odpowiedzialnego w szczególności za utrzymywanie jego w zgodności z ustaloną dokumentacją bezpieczeństwa oraz inicjowanie zabezpieczeń. Kierownik wyznacza dodatkowo inspektora bezpieczeństwa teleinformatycznego, który jako pracownik pionu ochrony odpowiedzialny jest za nadzór i aktualną kontrolę w sprawdzaniu zgodności działania systemu z procedurami bezpiecznej eksploatacji i szczególnymi wymaganiami bezpieczeństwa. Niezwykle istotną osobą w strukturze ochrony informacji niejawnych jest kierownik kancelarii tajnej, którego opisano w rozporządzeniu Rady Ministrów z dnia 7 grudnia 2011 r., w którym to jest przedstawiono go jako osobę sprawującą przede wszystkim opiekę nad dokumentami niejawnymi przechowywanymi w jednostce. Właściwa struktura organizacyjna ma za zadanie zapewnienie zdolności kancelarii do utrzymania właściwego funkcjonowania jednostki organizacyjnej w czasie pokoju, kryzysu oraz wojny[15].

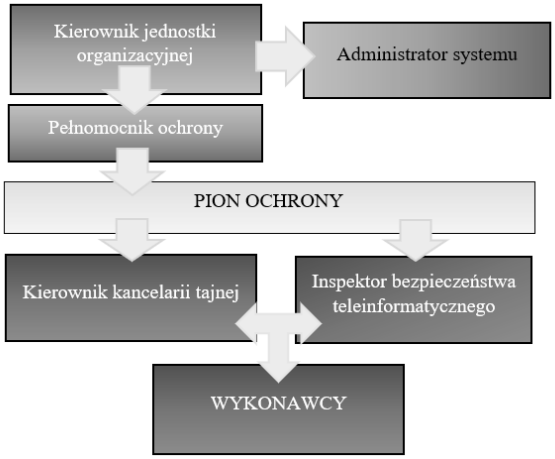
„Jednak obowiązki kierownika jednostki organizacyjnej nie kończą się na wyznaczeniu ww. osób funkcyjnych”[16], jest on odpowiedzialny za całokształt ochrony i czynności związanych z bezpieczeństwem teleinformatycznym w danej jednostce. Reasumując do wykorzystania przez pełnomocnika ochrony jest bezpośrednio cały pion ochrony, który pomaga mu w koordynowaniu wszelkich działań również tych związanych z bezpieczeństwem fizycznym informacji w danej jednostce. Rysunek 6.2 obrazuje elementy składowe przykładowej struktury systemu ochrony informacji niejawnej w jednostce organizacyjnej wykorzystującej systemy teleinformatyczne.

[13] Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010r. (Dz. U. z 2010 r., nr 182, poz. 1228), art. 14 ust. 3 pkt. 4.

[14] Rozporządzenie Ministra Obrony Narodowej z dnia 19 grudnia 2013 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych.

[15] Zarządzenie Nr 58/MON z dnia 11 grudnia 2017 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, sposobu i trybu przetwarzania informacji niejawnych.

[16] T. Sobczyński, *Bezpieczeństwo informacji niejawnych w aspekcie przetwarzania w chmurze obliczeniowej*, Wydawnictwo BP, Gdynia 2018, s. 84.



Źródło: Opracowanie własne na podstawie Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych

Rysunek 6.2. Organizacja systemu ochrony w jednostce organizacyjnej.

Systemy bezpieczeństwa teleinformatycznego z zakresu ochrony informacji niejawnych

Stały rozwój technologii informatycznej i wysoka dynamika działań wiążąca się z przechowywaniem i przetwarzaniem dokumentów niejawnych w Siłach Zbrojnych Rzeczypospolitej Polskiej przyczyniają się do wdrażania coraz to kolejnych systemów teleinformatycznych. Czym właściwie jest system teleinformatyczny? Definicyjne ujęcie systemu teleinformacyjnego w ustawie z dnia 16 lipca 2004r. o prawie komunikacyjnym zostało zaprezentowane jako: *„zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego”*[17]. Zatem na dany system składa się wiele różnych elementów, które ściśle ze sobą współpracują i poprzez złączenie odpowiednim oprogramowaniem tworzą jednolitą całość. Jednakże, użytkownik końcowy korzystający z takiego systemu widzi wyłącznie indykatywny interfejs służący jemu do wykonania określonych zadań. Jeżeli mówimy o bezpieczeństwie teleinformatycznym, jest ono definiowane jako wysokie stadium świadomości. Mianowicie, cechuje się, brakiem potencjalnych incydentów będących skutkiem niepowołanego, świadomego lub nieświadomego ujawnienia, zmodyfikowania,

[17] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U.2019.2460) (Dz. U. z 2018 r. poz. 1954, 2245 i 2354); (Dz.U.2020.346 j.t.).

zniszczenia lub przerwania możności przetwarzania informacji. Zatem jak zapisano, chociażby w normie ISO/IEC 27002, bezpieczeństwa teleinformatycznego nie można analizować w wąskim zakresie, skupiając się wyłącznie na elemencie systemu, czy sieciach komputerowych. Wykluczenie z pola zainteresowania szeroko rozumianego pojęcia bezpieczeństwa informacji prowadzi bezpośrednio do kreowania dziurawego systemu[18].

Systemy teleinformatyczne w SZ RP są klasyfikowane w oparciu o klauzule tajności, jeżeli chodzi o ich wykorzystanie przeważającą grupę stanowią systemy dopuszczone do przetwarzania informacji zastrzeżonych. Użytkowane są w szerokim aspekcie chociażby do przesyłania wiadomości pocztą elektroniczną, przesyłania meldunków czy też łączności VOIP działającej w wydzielonej strefie zdemilitaryzowanej (DMZ). Systemy te funkcjonują w oparciu o odseparowaną sieć Milnet-Z. Teleinformatyka jest również wykorzystywana w aspekcie EDZ tj. Elektronicznego zarzadzania dokumentacją poprzez ułatwienie organizowania czynności kancelaryjnych, dokumentowanie i nadzorowanie przebiegu realizowanych zadań oraz przy tworzeniu i gromadzeniu dokumentów elektronicznych. Do takiego zastosowania w obszarze informacji niejawnych w SZ RP wykorzystywany jest między innymi system teleinformatyczny ARCUS.

Bezpieczeństwo informacji w systemach teleinformatycznych jest ściśle uwarunkowane od formalnych modeli związanych z ich bezpieczeństwem zapisywanych w literaturze naukowej. Dotyczą one, niestety, tylko wybranych aspektów bezpieczeństwa w systemach i są to np.[19]:

- Modele kontroli dostępu do informacji.
- Modele ochrony informacji w bazach danych.
- Modele teoretycznych ograniczeń systemów ochrony informacji.

Najskuteczniejszym modelem kontroli dostępu w przypadku wyżej wymienionych systemów jest Mandatory Access Control, co tłumaczone jest jako obowiązkowa kontrola dostępu. Została ona opisana przez Narodowy Instytut Standaryzacji i Technologii, NIST, jako: sposób ograniczania dostępu do systemu w oparciu o analizę (reprezentowaną przez etykietę bezpieczeństwa) informacji zawartych w przedmiotach oraz formalne upoważnienie (tj. zezwolenie, formalne zezwolenia na dostęp i konieczność użycia konkretnych danych) osób do dostępu do informacji o konkretnej wrażliwości. Obowiązkowa kontrola dostępu obowiązuje wszystkich chcących skorzystać z danego systemu[20].

Bezpieczeństwo informacji jest ściśle związane z polem walki, na którym jest ona prowadzona, wymienione przykładowe modele ich ochrony w

[18] https://docplayer.pl/2802164-Warszawska-wyzsza-szkola-informatyki-systemy-wykrywania-wlaman-w-aspekcie-poglebionej-architektury-systemu-bezpieczenstwa-teleinformatycznego.html, dostęp: 27.10.2020 r.

[19] K. Liderman, *System bezpieczeństwa teleinformatycznego,* „Biuletyn instytutu automatyki i robotyki" nr 17/2002, s.77.

[20] NIST SP 800-53 Rev. 4 w ramach Obowiązkowej kontroli dostępu CNSSI 4009.

systemach teleinformatycznych są niezwykle istotne. W dokumencie „Wizja Sił Zbrojnych RP-2030", wskazano, że przyszłość prowadzonych działań należy do pola pozbawionego tradycyjnej geoprzestrzeni, a wykorzystywane będą głównie sfery pozbawione parametrów geograficznych, takie jak, wirtualna przestrzeń cybernetyczna czy właśnie sfera informacyjna. Opisano w nim również, że oddziaływanie przeciwnika stale rośnie w obszarze systemów informatycznych, kluczowe zatem jest określenie i spełnienie zadań związanych z utrzymywaniem odpowiedniego poziomu bezpieczeństwa[21].

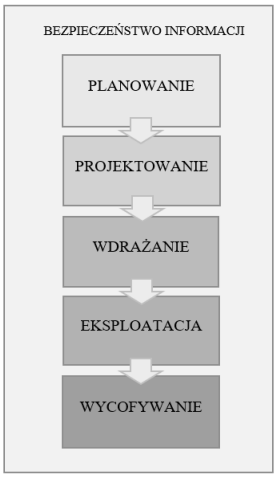
Cykl życia systemu teleinformatycznego

Definicja cyklu życia systemu „określa koncepcję rozłożenia w czasie głównych czynności wykonywanych podczas pracy nad opracowaniem i wyprodukowaniem systemu określonego typu oraz podczas jego eksploatacji"[22]. Natomiast zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego cykl jego funkcjonowania składa się z etapów, które przedstawia rysunek 6.3.

We wszystkich etapach za cel nadrzędny przyjęto bezpieczeństwo przetwarzanych informacji. Pierwszym z etapów jest planowanie systemu teleinformatycznego, który rozpoczyna się od ustalenia potrzeb w zakresie zamierzonego przetwarzania w nim informacji. Zaczynając od określenia przeznaczenia systemu poprzez zdefiniowanie klauzul tajności, które będą przetwarzane za jego pomocą, ze wskazaniem najwyższej występującej. Następnie, jak opisano w rozporządzeniu BTI określa się tryby bezpieczeństwa pracy systemu, które determinowane są między innymi poprzez planowaną liczbę użytkowników oraz definiowane cele systemu. Kolejno, dobierana jest odpowiednia, spełniająca określone wymagania, lokalizacja systemu, aby zostały zapewnione optymalne funkcjonalności dla użytkowników oraz tryby bezpieczeństwa pracy. Na etapie planowania niezwykle istotnym aspektem jest określenie odpowiednich wymagań co do budowanego systemu pod kątem sprzętu komputerowego. Poprzez określenie najwyższej przetwarzanej klauzuli tajności, liczby użytkowników oraz samej lokalizacji systemu determinowany jest rodzaj sprzętu pod względem wymaganych certyfikatów. Mimo, iż budżet w aspekcie planowania systemów teleinformatycznych w SZ RP schodzi na dalszy plan, uwaga jest skupiana na dobraniu odpowiednich rozwiązań dostosowanych do indywidualnych potrzeb jednostki, w której ma się on znajdować. Jednym z najczęstszych rozwiązań systemowych jest planowanie architektury systemowej opartej na zasadzie klient-serwer. Takie rozwiązanie pozwala na dostęp wielu użytkowników za pośrednictwem odpowiedniego komputera do

[21] https://www.bbn.gov.pl/pl/prace-biura/publikacje/inne-wydawnictwa/biblioteka-bezpieczenst/tom-2/1000,Wizja-Sil-Zbrojnych-RP.html, dostęp: 27.10.2020 r.
[22] K. Liderman, *Bezpieczeństwo informacyjne - nowe wyzwania*, Wydawnictwo Naukowe PWN, Warszawa 2017, s. 65.

bazy danych, znajdującej się na serwerze, w celu skorzystania z zasobów niezbędnych do wykonania postawionego zadania. Podczas planowania systemów przetwarzających określone klauzule tajności rozważane jest jego umiejscowienie względem stosowanych środków ochronnych oraz stref bezpieczeństwa.



Źródło: Opracowanie własne na podstawie Rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego.

Rysunek 6.3. Etapy w cyklu funkcjonowania systemu teleinformatycznego

Następnym etapem, jest etap projektowania, na którym po uprzednim zaplanowaniu działań rozpoczyna się od wstępnego szacowania ryzyka dla bezpieczeństwa przetwarzanych informacji niejawnych w systemie. Następnie, jak zapisano w pkt. 3 rozporządzenia BTI określane są poszczególne wymagania istotne przy doborze zabezpieczeń dla określonego systemu. Kolejno, po określeniu wymagań oraz przeprowadzonym wstępnym szacowaniu ryzyka, zgodnie z jego wynikami, dobierane są odpowiednie zabezpieczenia dla danego systemu. W porozumieniu z podmiotem akredytującym w przypadku SZ RP, SKW, uzgadnia się plan przedsięwzięć i harmonogram działań obejmujący istotne elementy niezbędne do uzyskania akredytacji bezpieczeństwa teleinformatycznego. Cała wykonana praca jest spinana w ramach opracowania dokumentu szczególnych wymagań bezpieczeństwa (SWB), projektowanego systemu teleinformatycznego.

Na etapie wdrażania rozpoczynany jest proces pozyskiwania sprzętu wchodzącego w skład zabezpieczenia budowanego systemu oraz przeprowadzana jest instalacja i konfiguracja narzędzi odpowiedzialnych za bezpieczeństwo. Kolejno, w zgodności z ostatnio przeprowadzoną analizą ryzyka dokonywane są testy bezpieczeństwa danego systemu teleinformatycznego. W sy-

tuacji, kiedy zaistnieje znaczna dywergencja pomiędzy przeprowadzoną analizą ryzyka, a testami bezpieczeństwa, należy przeprowadzić ją ponownie wraz z wprowadzonymi zabezpieczeniami systemu. Kolejnym krokiem jest sporządzenie dokumentu procedur bezpiecznej eksploatacji (PBE) oraz uzupełnienie wcześniej sporządzonego SWB. Następnie obydwa dokumenty w przypadku opisywanych systemów teleinformatycznych SZ RP wysyłane są do SKW celem ich zatwierdzenia. W sytuacji, gdy wysokość klauzuli przetwarzanej w danym systemie tego wymaga, przeprowadzany jest audyt bezpieczeństwa systemu prowadzony przez SKW. Elementem kończącym etap wdrażania jest przeprowadzenie akredytacji systemu i uzyskanie świadectwa akredytacji bezpieczeństwa teleinformatycznego.

Kolejnym z etapów jest etap eksploatacji, kluczowym aspektem jest stałe utrzymywanie zgodności systemu z wcześniej ustalaną dokumentacją bezpieczeństwa. Niezwykle istotne jest sprawowanie kontroli, nadzoru nad użytkownikami danego systemu w zakresie bezpieczeństwa. Do takiego nadzorczego zadania powoływany jest pion ochrony, w którym znajduje się odpowiednio wyszkolony personel. Podczas etapu eksploatacji jest stale utrzymywany proces zarządzania ryzykiem oraz wspierany jest o okresowe testy bezpieczeństwa. Testy prowadzone są w celu sprawdzania aktualnego stanu zabezpieczeń systemu teleinformatycznego, w przypadku wykrycia i stwierdzenia nieprawidłowości są one niezwłocznie usuwane w sposób zapewniający możliwie najmniejsze zakłócenie jego pracy. Dodatkowo wprowadza się również, wynikające z potrzeby, modyfikacje do systemu. W przypadku, kiedy wprowadzone modyfikacje nie odnoszą się do zmian od strony bezpieczeństwa systemu, wystarczające jest uaktualnienie dokumentacji oraz zawiadomienie, podmiotu, który udzielił akredytacji. Natomiast jeżeli chodzi o zmiany, które ingerują w zabezpieczenia systemu teleinformatycznego, przed ich wprowadzeniem niezbędna jest zgoda odpowiednich organów akredytujących, w tym przypadku SKW. Niemniej, należy wprowadzić zmiany do dokumentacji bezpieczeństwa w formie aneksów. Dodatkowo, przeprowadzane są kolejne testy bezpieczeństwa teleinformatycznego w oparciu o zapewniony w ciągłości proces zarządzania ryzykiem.

Ostatnim etapem w cyklu życia systemu teleinformatycznego, jest etap wycofywania, w którym przerywa się jego dalszą eksploatację. W tym celu, należy powiadomić SKW za pośrednictwem drogi pisemnej. Jeżeli wycofywany system teleinformatyczny służył do przetwarzania informacji niejawnych o klauzuli tajności, poufna lub wyższej, należy odesłać uzyskane uprzednio świadectwo akredytacji do podmiotu, który jego udzielił. Pozostałe dane niejawne przechowywane w wycofywanym systemie teleinformatycznym poddaje się odpowiednim procesom. Procesy te rozumiane są poprzez przeniesienie ich do innego, tożsamego systemu przeznaczonego do przetwarzania informacji niejawnych o takich samych lub wyższych klauzulach. Rozumiane są również, poprzez odpowiednie zarchiwizowanie takowych danych niejaw-

nych. W przypadku niezaistnienia powyższych możliwości, dane te są niszczone. Dokładne procedury i zalecenia zapisano w wytycznych SKW, które w przejrzysty sposób dyktują dostosowane do danej klauzuli i nośnika sposoby ich niszczenia[23].

Wymagania bezpieczeństwa stawiane wojskowym sieciom teleinformatycznym

Działanie współczesnych systemów teleinformatycznych przetwarzających informacje niejawne odbywa się przy wykorzystaniu odpowiednich sieci telekomunikacyjnych. Na etapie projektowania i budowania takich systemów, między innymi dobierane są odpowiednie drogi komunikacji, po których będzie odbywało się przetwarzanie danych niejawnych w niezawodny i bezpieczny sposób. W przypadku Sił Zbrojnych RP większość przesyłanych informacji pomiędzy urządzeniami posiada określoną klauzulę tajności. W celu zapewnienia odpowiedniej jakości usług i zgodności z atrybutami bezpieczeństwa informacji przetwarzanych w systemie, budowane są odseparowane, autonomiczne oraz niezależne od innych sieci, infrastruktury teleinformatyczne. Czym zatem jest opisywana sieć? Otóż sieć w systemach teleinformatycznych jest siecią telekomunikacyjną, zapewniającą przesyłanie im przesyłanie danych. Opisano ją w ustawie z dnia 16 lipca 2004 r. o prawie telekomunikacyjnym jako: *„systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię”*[24]. W Siłach Zbrojnych Rzeczypospolitej Polskiej odseparowane autonomiczne sieci budowane są w oparciu o własne rozwiązania infrastruktury na potrzeby prowadzonych działań lub *„poprzez dzierżawienie od operatorów telekomunikacyjnych wydzielonej linii”*[25]. Przekłada się to na wszechstronne zastosowania systemów teleinformatycznych w oparciu o takie sieci chociażby w zakresie wspierania dowodzenia czy sposobów kierowania środkami walki[26]. Przykładem odseparowanej i niezależnej sieci dla informacji niejawnych jest Milnet-Z. Dodatkowo sieć ta tworzy „DMZ”, czyli strefę zdemilitaryzowaną, która charakteryzuje się wydzieloną przestrzenią z sieci komputerowej zarówno zewnętrznej jak i wewnętrznej. Objęta jest specjalnymi zabezpieczeniami przy wykorzystaniu miejsca znajdującego się bezpośrednio w zaporze

[23] Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, rozdział 2, §18.
[24] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U.2019.2460), rozdział 1, art. 2, pkt 35.
[25] *https://www.bbn.gov.pl/download/1/1005/wymaganiatechnologiczne2.pdf,* dostęp: 03.12.2020 r.
[26] R. Janczewski, *Procesy militarne w działaniach militarnych w cyberprzestrzeni*, [w:] B. Biernacik, L. Kalman (red.), *Systemy i sieci teleinformatyczne Sił Zbrojnych RP- wielorakie aspekty bezpieczeństwa cyberprzestrzeni,* Wydawnictwo ASzWoj, Warszawa 2016, s. 291.

sieciowej. Blokuje do niej dostęp osób z zewnątrz przez co atak hakerski nie jest możliwy do przeprowadzenia. Takie działania są wykluczone, poprzez odseparowanie Milnet-Z od sieci Internet. Przedstawiane rozwiązanie sieciowe, pozwala w SZ RP na szerokie zastosowania różnych systemów wewnętrznych np. telekomunikacyjnych, pocztowych, magazynowych czy planistycznych. Dodatkowo dzięki temu systemy do niej podłączone są właściwie zabezpieczone przed ingerencją osób nieuprawnionych, gdyż dostęp do Milnet-Z jest możliwy tylko po uzyskaniu odpowiedniego poświadczenia bezpieczeństwa. Jednostki wojskowe oraz współpracujące z SZ RP przedsiębiorstwa z sektora prywatnego są przyłączane do tej sieci poprzez uzyskanie odpowiednich zezwoleń nadawanych przez służby. Architektura wewnętrzna sieci w rozumieniu organizacji, jej komponentów jest budowana na poszczególnych jednostkach w oparciu o indywidualne potrzeby i zakres wykorzystywania.

Budowa wojskowych sieci nie różni się zasadniczo pod względem technologicznym od budowy sieci cywilnych tj. sieci transmisyjne SDH, ATM czy też sieci rozległe. W celu jej zabezpieczenia przed nieuprawnionym przejęciem lub nieautoryzowanym dostępem do przetwarzanych informacji niejawnych stosowane są odpowiednie mechanizmy *„elektromagnetycznej separacji urządzeń”*[27], które zabezpieczają w znacznym stopniu komputery wraz z podłączonymi do nich urządzeniami peryferyjnymi. W celu zapewnienia dodatkowej ochrony dla atrybutów poufności i integralności informacji przetwarzanych
w separowanej sieci, stosowane są zabezpieczenia kryptograficzne, które zapewniają ich utajnienie w warstwie łącza danych. Natomiast, do obsługi takich zabezpieczeń kryptograficznych, czy też do pracy przy bezpieczeństwie sieci wojskowych dobierane są określone osoby, posiadające szereg odpowiednich kompetencji i przeszkoleń z tego zakresu.

Najprężniej rozwijanymi sieciami wojskowymi są obecnie sieci mobilne opierające się między innymi na technologii ATM tj. „*sieć szkieletowa z gwarantowanym poziomem jakości usług”*[28], jak i również stale rozwijanych sieciach światłowodowych. W przypadku technologii światłowodowych przesyłane informacje niejawne są odporne na zakłócenia elektromagnetyczne.

Ochrona fizyczna i techniczna

Jednym z elementów wielopoziomowej ochrony informacji niejawnych przetwarzanych w systemach teleinformatycznych jest stosowanie zabezpieczeń fizycznych i technicznych. Co składa się na mechanizmy ochrony podnoszącej poziom bezpieczeństwa, zwłaszcza pod kątem identyfikacji osób próbujących zakłócić funkcjonowanie systemu? Otóż jeżeli mowa o ochronie fi-

[27] https://www.bbn.gov.pl/download/1/1005/wymaganiatechnologiczne2.pdf, dostęp: 03.12.2020 r.
[28] Tamże, str. 106

zycznej, składają się na nią odpowiednio przeszkolone osoby nadzorujące bezpieczeństwo danego systemu np. patrole, warty. Natomiast ochrona techniczna dzieli się na dwa zasadnicze rodzaje mianowicie[29]:

- zabezpieczenia mechaniczne,
- zabezpieczenia elektroniczne.

W skład zabezpieczeń mechanicznych wchodzą wszelkiego rodzaju rozwiązania konstrukcyjne takie jak szafy pancerne, utwardzane ściany czy zakratowane okna. Na zabezpieczenia elektroniczne rozwiązania związane z kontrolą dostępu, elektrycznego alarmowania w przypadku włamania jak i również systemy sygnalizacji zdarzeń.

W celu stworzenia jednolitego, szczelnego systemu ochrony, wyżej wymienione zabezpieczenia powinny ze sobą współpracować. Stosowane środki takiej ochrony zawierane są w specjalnie opracowywanym planie ochrony dla danej jednostki organizacyjnej[30].

Środki zabezpieczeń fizycznych ujęto w rozporządzeniu Prezesa Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego sosowanych do zabezpieczenia informacji niejawnych[31], które wraz z rozwojem technologicznym jest uaktualniane i nowelizowane. Ostatnia zmiana miała miejsce w 2017 r. i wprowadziła modyfikacje dotyczące stosowania zabezpieczeń zgodnych z „Polskimi Normami" oraz narzuciła wymagania spełniania poświadczeń zgodności, z tymi zawartymi w rozporządzeniu.

Wybrane metody ochrony sprzętowo-programowej

Elementem systemu ochrony informacji niejawnych na jednym z jego poziomów są tzw. metody sprzętowo-programowe. Takie sposoby zabezpieczania informacji niejawnych w systemie właściwie odpowiadają pożądanym standardom bezpieczeństwa teleinformatycznego na zidentyfikowane i zdefiniowane zagrożenia. Jedynie poprzez odpowiedni poziom zabezpieczeń na każdym z etapów, od ochrony fizycznej po świadomość użytkowników, możliwe jest osiągnięcie zamierzonego wskaźnika bezpieczeństwa przetwarzanych informacji.

Przykładowymi metodami ochrony sprzętowo-programowej są:

- pewne i certyfikowane oprogramowanie systemowe oraz uzupełniające (oprogramowanie antywirusowe);
- zdefiniowane procedury tworzenia oprogramowania;

[29] K. Liderman, *Bezpieczeństwo informacyjne…*, dz. cyt., s. 42.

[30] Rozporządzenie MON z dnia 19 grudnia 2013 r. w sprawie szczegółowych zadań pełnomocników ochrony
w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, rozdział 7.

[31] Rozporządzenie Prezesa Rady Ministrów z dnia 29 maja 2012r. w sprawie środków bezpieczeństwa fizycznego sosowanych do zabezpieczenia informacji niejawnych (Dz.U 2012 poz. 683).

- programowe szyfrowanie danych i filtrowanie ruchu sieciowego (zapory sieciowe);
- właściwa z zaleceniami konfiguracja sprzętowa;
- zabezpieczające mechanizmy składowania i odczytu.

Metody takiej ochrony przetwarzanych danych niejawnych w systemach teleinformatycznych polegają zazwyczaj na częściowym lub całkowitym aspekcie zabezpieczenia. Mianowicie, sposób tego rodzaju ochrony może ograniczać się do przeciwdziałania w określonych sytuacjach lub zabezpieczać poziom bezpieczeństwa systemu w sposób globalny.

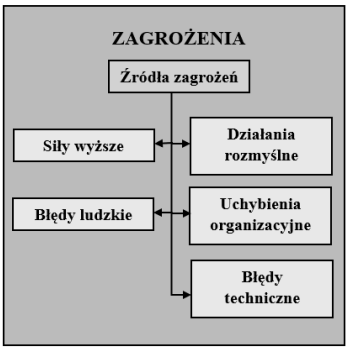
Zagrożenia dla systemu przetwarzającego informacje niejawne

Czym tak naprawdę jest zagrożenie? Otóż zdefiniowano je w Polskich Normach w odniesieniu do systemów informatycznych jako *„potencjalne naruszenie zabezpieczenia systemu..."*[32]. Natomiast w normie standaryzującej ISO/IEC 27000:2009 jako *„potencjalną przyczynę niepożądanego incydentu, która może spowodować szkodę dla systemu lub organizacji"*[33]. Co więcej, zagrożenie w odniesieniu do informacji w nim przetwarzanych, przedstawiono w literaturze jako: *„materialny i/lub niematerialny czynnik mogący spowodować niepożądaną zmianę wymaganych wartości istotnych kryteriów informacji"*[34].

Zagrożenia zarówno dla samych informacji niejawnych jak i dla systemów teleinformatycznych, w których są przetwarzane powstają poprzez wykorzystanie pewnych „niedoskonałości" systemu, które nazywane są podatnościami. Definiowane są również w standaryzacji ISO/IEC 27000:2009, która formułuje je jako: *„słabość zasobu lub mechanizmu kontrolnego, która może być wykorzystana przez zagrożenie"*[35]. Środkiem służącym identyfikacji zagrożeń jest wcześniej wspomniana analiza, a dokładniej jeden z jej etapów. W procesie określenia zagrożeń, rozważana jest cała infrastruktura badanego systemu teleinformatycznego, w szerokim aspekcie. Analiza ryzyka jest prowadzona na podstawie wybranej metody. Cały proces ujęto w zaleceniach SKW, które nie określają dokładnej klasyfikacji zagrożeń. Natomiast, przed wykonaniem szacowania ryzyka dla systemu teleinformatycznego, które pozwoli na określenie ryzyka związanego z potencjalnymi zagrożeniami, kluczowe jest przeprowadzenie tzw. „modelowania zagrożeń"[36]. Procedura mo-

[32] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Wydawnictwo Naukowe PWN, Warszawa 2009, s. 40.
[33] https://www.knf.gov.pl/knf/pl/komponenty/img/knf_125701_PTE_Wytyczne_IT_16_12_2014_40005.pdf, dostęp: 27.10.2020 r.
[34] K. Liderman, *Bezpieczeństwo informacyjne…*, dz. cyt., str. 22.
[35] https://www.knf.gov.pl/knf/pl/komponenty/img/knf_125701_PTE_Wytyczne_IT_16_12_2014_40005.pdf, dostęp: 27.10.2020 r.
[36] A. Shostack, *Threat modeling: Design for security*, John Wiley & Sons, Inc., Indianapolis 2014, p. xxi.

delowania zagrożeń, podobnie jak szacowanie ryzyka, jest możliwa do przeprowadzenia na różne sposoby. Istnieje wiele metodyk odpowiadających na różnorodność i specyfikę prowadzonych działań w obrębie danego systemu w jednostce organizacyjnej. Na etapie identyfikacji można wyróżnić między innymi dwa aspekty, formułowane jako *„attacker-centric"* oraz *„asset-centric"*[37].



Źródło: Opracowanie własne na podstawie: J. Kowalewski, M. Kowalewski, *Polityka bezpieczeństwa informacji w praktyce*, Wydawnictwo PRESSCOM, Warszawa 2014, s. 28.

Rysunek 6.4. Klasyfikacja zagrożeń dla systemów teleinformatycznych

Praktyki stosowane przy identyfikacji zagrożeń na drodze modelowania w jednym z etapów procesu szacowania ryzyka, pozwalają na stworzenie ich klasyfikacji. Natomiast, ze względu na różnorodność zagrożeń chociażby pod względem na podział: celowe, niecelowe, wewnętrzne, zewnętrzne, wywołane skutkami siły natury, związane ze słabością danego systemu teleinformatycznego czy też przez zmieniające się prawne regulacje[38], nie istnieje jeden prawidłowy sposób ich klasyfikacji. Indykatywnym przykładem jest zatem, przedstawiona w literaturze przedmiotu[39], klasyfikacja widoczna na rysunku 6.4.

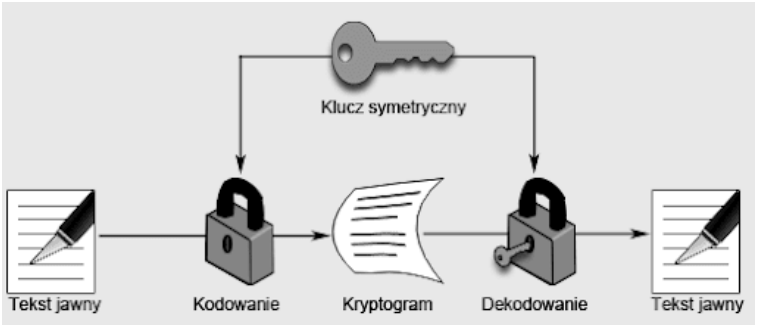
Wybrane metody przeciwdziałania zagrożeniom dla systemu teleinformatycznego przetwarzającego informacje niejawne w SZ RP

Przykładem ściśle związanym z systemami jest ochrona poprzez metody kryptograficzne. Czym zatem jest kryptografia? Jak przedstawia definicja, *„Współcześnie kryptografia stanowi podstawę nowoczesnych technologii*

[37] L. O. Nweke, S. D. Wolthusen, *A Review of Asset-Centric Threat Modelling Approaches*, „International Journal of Advanced Computer Science and Applications", Vol. 11(2)/2020, p. 1-6.
[38] J. Syta, *Metoda ABCDEF podziału cyberzagrożeń*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna 2019*, Akademia Marynarki Wojennej, Gdynia 2020 r., s. 34-35.
[39] J. Kowalewski, *Polityka bezpieczeństwa informacji w praktyce*, Wydawnictwo PRESSCOM Sp. z o. o., Wrocław 2014, s. 28.

bezpieczeństwa stosowanych do ochrony informacji i zasobów zarówno w sieciach otwartych, jak i zamkniętych"[40]. Czy też jak stanowi zapis zawarty w Polskich Normach, *„zawiera w sobie zasady, metody oraz środki adaptowania danych w celu ukrycia ich zawartości semantycznych, zapobiegania przeciw nieuprawnionemu dostępowi oraz utajnionej modyfikacji"*[41]. Za pośrednictwem metod kryptograficznych odpierane są zatem zagrożenia związane między innymi z utratą poufności przesyłanych danych pomiędzy urządzeniami systemowymi oraz wykluczenie nieuprawnionej modyfikacji zasobów znajdujących się na komputerach. Metody szyfrowania wykonywane według dwóch różnych koncepcji. Rysunek 6.5 przedstawia metodę szyfrowania symetrycznego. Natomiast rysunek 6.6 metodę szyfrowania asymetrycznego.

Zobrazowane metody szyfrowania służą do zabezpieczenia przetwarzanych informacji oraz tworzą *możliwość sprawowania kontroli nad poufnością danych*[42].



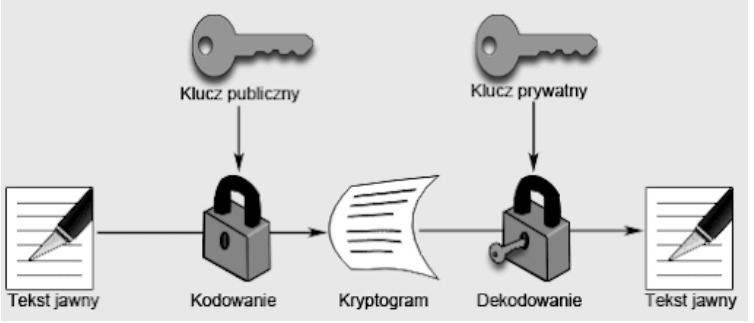
Źródło: http://ekryptografia.pl/kryptografia/szyfry-symetryczne/, dostęp: 02.12.2020 r.

Rysunek 6.5. Metoda szyfrowania symetryczna

Powołując się na przykłady stosowanych rozwiązań w SZ RP w systemach teleinformatycznych jednym z opracowanych urządzeń certyfikowanym przez SKW służącym do szyfrowania, *jest urządzenie przeznaczone do ochrony danych pakietowych w sieciach IP7*[43]. Zostało opracowane w Zakładzie Kryptologii Wojskowego Instytutu Łączności i służy do zabezpieczania informacji niejawnych do klauzuli *tajne.* Urządzenie zbudowane jest w oparciu o optyczne interfejsy budowania sieci lokalnych umożliwiające tym samym tworzenie tuneli kryptograficznych zapewniających bezpieczne przetwarzanie

[40] https://edu.pjwstk.edu.pl/wyklady/bsi/scb/index45.html, dostęp: 03.12.2020 r.
[41] PN-ISO/IEC 2382-8:2001 - wersja polska
[42] Współczesne rozwiązania kryptograficzne (część 1), Polish-Japanese Academy of Information Technology, Warszawa 2009, E. Głowacki, str. 52
[43] https://docplayer.pl/13356618-Kryptograficzne-aspekty-ochrony-informacji-niejawnych.html, 02.12.2020 r.

danych. Rozwiązanie to dodatkowo wzmocnione jest o elementy ochrony elektromagnetycznej oraz fizycznej zapewniające jemu odporność na czynniki zewnętrzne. W odniesieniu do użytych protokołów kryptograficznych zastosowano autorskie rozwiązania wsparte dedykowanymi mechanizmami *„monitorowania i zarządzania oraz planowania, generacji i dystrybucji danych kryptograficznych”*[44].



Źródło: http://ekryptografia.pl/kryptografia/szyfry-asymetryczne/, dostęp: 02.12.2020 r.

Rysunek 6.6. Metoda szyfrowania asymetryczna

Kolejnym przykładem wpisującym się w rolę przeciwdziałania zagrożeniom występującym przy przetwarzaniu informacji niejawnych w systemach teleinformatycznych w SZ RP, są rozwiązania typu *firewall*, tj. zapory sieciowe. Rozwiązania tego typu występują zarówno w formie sprzętowej, jak i programowej. Zapory sieciowe, tzw. sprzętowe, są to dedykowane urządzenia umiejscowione zazwyczaj w przypadku systemów teleinformatycznych SZ RP na granicy sieci wojskowej z siecią zewnętrzną. Pozwalają między innymi na filtrowanie pakietów sieciowych poprzez sprawdzanie ich nagłówków oraz podejmowanie decyzji, czy zezwolenie na dany pakiet jest zgodne z polityką narzuconą przez firewall[45]. Co więcej, wykorzystywane są również w przypadku oddzielenia w sieci wewnętrznej specjalnych stref, dostosowanych do przetwarzania określonych klauzul tajności i zapewnienia im odpowiedniej ochrony. Poprzez zaimplementowane specjalne oprogramowanie przeznaczone do monitorowania, weryfikowania i ewentualnego blokowania przesyłanych zasobów. Zabezpiecza ono system przed podatnościami związanymi z nieuprawnionym dostępem do niego. Ponadto takie rozwiązania zapewniają możliwość stworzenia tzw. stref zdemilitaryzowanych.

[44] https://docplayer.pl/13356618-Kryptograficzne-aspekty-ochrony-informacji-niejawnych.html, 02.12.2020 r.
[45] https://www.researchgate.net/publication/228394375_Network_Firewalls, dostęp: 04.12.2020 r.

Przykładem zapory sieciowej w oparciu o urządzenie, jest „Firewall Cisco PIX". Z informacji dostępnych na stronie producenta wynika, że zapewnia on ochronę sieci wewnętrznej ukrywając jej architekturę. Rozwiązanie to umożliwia bezpieczny dostęp do Internetu z istniejącej sieci wojskowej oraz zapewnia możliwość rozbudowy i rekonfiguracji sieci TCP/IP bez obawy o brak adresów IP[46].

Natomiast, jeżeli chodzi o zapory sieciowe w oparciu o rozwiązania oprogramowania dla komputerów definiowanych jako urządzenia końcowe w systemie teleinformatycznym firmą wiodącą i wykorzystywaną przez SZ RP jest Microsoft. Oprogramowaniem zgrywającym za pośrednictwem, którego odbywa się przetwarzanie informacji w systemie, jest między innymi odpowiednio skonfigurowany MS Windows. Wyposażony w rozwiązania programowej zapory sieciowej *Windows Firewall*. Jest to aplikacja zabezpieczająca system, stworzona przez firmę Microsoft zaimplementowana bezpośrednio do systemu. Została zaprojektowana do filtrowania transmisji danych w sieci, zarówno wchodzących i wychodzących pakietów. Kolejno, wyposażona jest w mechanizmy blokowania szkodliwej komunikacji i/lub programów, które je inicjują.

Firewalle dokładnie analizują ruch sieciowy na podstawie wcześniej ustalonych reguł. Prawidłowo skonfigurowane zapory, filtrują ruch pochodzący z niezabezpieczonych lub podejrzanych źródeł, w celu zapobiegania intensyfikowaniu się zagrożeń. Takowe rozwiązania pozwalają na skanowanie pakietów w poszukiwaniu szkodliwego kodu lub wektorów ataków, które zostały już zidentyfikowane jako zagrożenia. Monitorowanie i regulowanie ruchu sieciowego przez zapory odbywa się w oparciu o różne metody. Przykładowe z nich to:

- Filtrowanie pakietów. Otóż, pakiety to niewielkie ilości danych. Gdy zapora używa takiego filtrowania, pakiety próbujące dostać się do sieci poddawane są grupie tzw. filtrów. Usuwają one te pasujące do określonych zidentyfikowanych zagrożeń i pozwalają właściwym na dotarcie do docelowego punktu.
- Usługa proxy. Jest to rodzaj bezpiecznego rozwiązania w oparciu o serwer pośredniczący. Minusem jest czas trwania przesyłania zasobów. Dodatkowo występują ograniczenia ze względu na rodzaj obsługiwanych aplikacji. Serwery proxy działają na zasadzie pośrednika zasadniczo tworząc lustro komputera za zaporą. W związku z tym zapobiegają bezpośrednim połączeniom między urządzeniem klienta a przychodzącymi pakietami, chroniąc lokalizację sieciową przed potencjalnymi złymi aktorami.
- Stateful inspection. To metoda dynamicznego filtrowania pakietów, która monitoruje stan aktywnych połączeń i wykorzystuje te

[46] https://www.cisco.com/en/US/docs/security/pix/pix30/user/guide/pixugint.html, dostęp: 04.12.2020 r.

informacje do określenia, które pakiety sieciowe przepuszczać przez zaporę. Mianowicie zapory stateful inspection sprawdzają różne elementy każdego pakietu danych i porównują je z bazą danych zawierających zaufane informacje. Działają w oparciu o tabele sesji, której wpisy zazwyczaj rejestrują źródłowe i docelowe adresy IP oraz numery portów[47]. Obejmują źródłowe i docelowe adresy IP, porty i aplikacje. Przychodzące pakiety danych muszą w wystarczającym stopniu pasować do zaufanych informacji, aby mogły zostać przepuszczone przez zaporę. Stateful Inspection to nowsza metoda filtrowania zapory stosowana m. in. w przytoczonym Cisco PIX[48].

Istotną kwestią przy utrzymaniu eksploatowanego systemu teleinformatycznego
w należytym porządku jest stosowanie tzw. dobrych praktyk. Zdefiniowanymi praktykami są między innymi:

- dynamiczne dostosowywanie potrzeb w zakresie zmieniających się prowadzonych działań w oparciu o wdrażany system, współpraca administratora systemu z inspektorem bezpieczeństwa teleinformatycznego;
- prowadzenie regularnych testów eksploatowanego systemu, szczególnie po podłączeniu nowych urządzeń czy przeprowadzeniu aktualizacji oprogramowania;
- przeprowadzanie okresowych szkoleń dla personelu i kadry zarządczej oraz administratora systemu;
- realizowanie stałej obserwacji systemu pod kątem podatności i ewentualnych zagrożeń z nich wynikających, wdrożenie testów penetracyjnych;
- wypracowywanie zasad i reguł bezpieczeństwa przy uwzględnianiu potrzeb użytkowników systemu;
- nadzorowanie działań wykonywanych w systemie, monitorowanie ruchu sieciowego oraz stała obserwacja stosowanych mechanizmów bezpieczeństwa pod kątem ich sprawności i wersji.

Metodologia

Praca została napisana na podstawie dokładnej analizy materiałów zwartych, artykułów naukowych oraz rzetelnych stron internetowych. Praca została napisana na podstawie dokładnej analizy materiałów zwartych, artykułów naukowych oraz rzetelnych stron internetowych. Dodatkowo zgłębienie

[47] X. Li, Z-Z. Ji, M-Z. Hu, *Stateful inspection firewall session table processing*, "International Journal
of Information Technology", Vol. 11(2)/2005 p. 21.
[48] https://www.solarwindsmsp.com/blog/how-do-firewalls-work#:~:text=Packets%20are%20small%20amounts%20of,Proxy%20service, dostęp: 06.12.2020 r.

obowiązujących przepisów prawa z dziedziny ochrony informacji niejawnych pozwoliło na zwrócenie uwagi na zagrożenia występujące przy przetwarzaniu ich w systemach teleinformatycznych. Przedmiotem badań było bezpieczeństwo informacji niejawnych w systemach teleinformatycznych Sił Zbrojnych Rzeczypospolitej Polskiej. Natomiast celem pracy poddanie analizie zasad organizacji systemów teleinformatycznych Sił Zbrojnych Rzeczypospolitej Polskiej oraz bezpieczeństwo informacji niejawnych w nich przetwarzanych. Ponadto zostały przedstawione wybrane zagrożenia dla funkcjonowania systemów Teleinformatycznych oraz metody ich eliminacji. Dokonane badanie i analiza literatury oraz zapisów prawnych pozwoliła na uzyskanie odpowiedzi na następujące pytania:

- Jak wygląda system zarządzania bezpieczeństwem informacji niejawnych?
- Jak ukształtowana jest struktura organizacyjna ochrony informacji niejawnych w SZ RP?
- Jakie przepisy prawne obowiązują w aspektach ochrony informacji niejawnych?
- Co składa się na system teleinformatyczny do przetwarzania informacji?
- Jakie są potencjalne zagrożenia i metody ich eliminacji pod względem przetwarzania, przechowywania danych niejawnych za pomocą technik teleinformatycznych?

Przegląd literatury

Autor w pracy opierał się głównie na ustawie z dnia 5 sierpnia 2010r. oraz wynikających z niej rozporządzeniach, literaturze naukowej, publikacjach naukowych jak i również źródłach internetowych były to między innymi: K. Liderman (2009 r.); S. Topolewski (2017 r.); M. Jabłoński, T. Radziszewski (2012 r.); B. Iwaszko (2012 r.); T. Sobczyński (2018 r.). Rozporządzenia wynikające z ustawy przyczyniły się do analizy i przedstawienia systemu ochrony informacji niejawnych w Siłach Zbrojnych Rzeczypospolitej Polskiej i wyciągnięcia wniosków odnoszących się do ich prawidłowości.

Wnioski

Przeprowadzona analiza i badanie literatury pozwoliły na sformułowanie następujących wniosków:

1. Bezpieczeństwo informacji niejawnych przetwarzanych w systemach teleinformatycznych SZRP jest współcześnie niezwykle istotną kwestią. Rozwój technologii informatycznych spowodował przeniesienie prowadzenia dokumentacji z tradycyjnych form „papierowych", na formy elektroniczne. Konwencjonalne metody zostały wyparte przez urządzenia peryferyjne wchodzące w skład

systemów teleinformatycznych, a przesyłanie danych odbywa się głównie z wykorzystaniem sieci telekomunikacyjnych.
2. Stały postęp w implementacji nowych systemów na potrzeby SZ RP w jednostkach organizacyjnych pozwala na prowadzenie wielu działań wiążących się z przetwarzaniem dokumentów niejawnych. Interpretacje aktów i regulacji prawnych związanych z ochroną informacji niejawnych oraz systemami teleinformatycznymi pozwoliła na stwierdzenie, że analizowane systemy odgrywają kluczową rolę w prowadzeniu działań w SZRP.
3. Obecny rozwój technologii, systemów teleinformatycznych w SZ RP znacząco usprawnia proces dowodzenia. Rekapitulując, pojawiające się nieustannie zagrożenia wykorzystujące podatności systemów, są skutecznie zwalczane przy użyciu konsekwentnie wprowadzanych mechanizmów bezpieczeństwa. Dodatkowo właściwie uformowane struktury definiują organy odpowiedzialne za nadzorowanie i kontrolowanie prawidłowego przetwarzania informacji niejawnych.

Bibliografia

Opracowania zwarte

1. Biernacik B., Kalman L. (red.), „*Systemy i sieci teleinformatyczne Sił Zbrojnych RP- wielorakie aspekty bezpieczeństwa cyberprzestrzeni*", Wydawnictwo ASzWoj, Warszawa 2016.
2. Jabłoński M., Radziszewski T.*, „Bezpieczeństwo fizyczne i teleinformatyczne informacji niejawnych",* Wydawnictwo PRESSCOM Sp. z o. o., Wrocław 2012.
3. Kowalewski J., *Polityka bezpieczeństwa informacji w praktyce*, Wydawnictwo PRESSCOM Sp. z o. o., Wrocław 2014.
4. Kowalewski M., Kowalewski J., *„Polityka bezpieczeństwa informacji w praktyce"*, Wydawnictwo PRESSCOM Sp. z o. o., Wrocław 2014.
5. Liderman K., „*Analiza ryzyka i ochrona informacji w systemach komputerowych*", Wydawnictwo Naukowe PWN, Warszawa 2009.
6. Liderman K., „*Bezpieczeństwo informacyjne- nowe wyzwania*", Wydawnictwo Naukowe PWN, Warszawa 2017.
7. Polaczek T.*, „Audyt bezpieczeństwa informacji w praktyce",* Helion, Gliwice 2014.
8. Shostack A., *Threat modeling: Design for security,* John Wiley & Sons, Inc., Indianapolis 2014.
9. Sobczyński T.*, „Bezpieczeństwo informacji niejawnych w aspekcie przetwarzania w chmurze obliczeniowej",* Wydawnictwo BP, Gdynia 2018.

10. Topolewski S., „*Ochrona informacji niejawnych w Siłach Zbrojnych Rzeczypospolitej Polskiej*", Wydawnictwo Uniwersytet Przyrodniczo-Humanistyczny, Siedlce 2017.

Artykuły

1. Janczewski R., *Procesy militarne w działaniach militarnych w cyberprzestrzeni*, [w:] B. Biernacik, L. Kalman (red.), *Systemy i sieci teleinformatyczne Sił Zbrojnych RP - wielorakie aspekty bezpieczeństwa cyberprzestrzeni*, Wydawnictwo ASzWoj, Warszawa 2016, s. 291.
2. Li X., Ji Z-Z, Hu M-Z., *Stateful inspection firewall session table processing*, "International Journal of Information Technology", Vol. 11(2)/2005.
3. Nweke L. O., Wolthusen S. D., *A Review of Asset-Centric Threat Modelling Approaches*, „International Journal of Advanced Computer Science and Applications", Vol. 11(2)/2020.
4. Syta J., *Metoda ABCDEF podziału cyberzagrożeń*, [w:] J. Kosiński (red.), *Przestępczość teleinformatyczna 2019,* Akademia Marynarki Wojennej,Gdynia 2020 r.

Dokumenty normatywne

1. Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U.2019.2460) (Dz. U. z 2018 r. poz. 1954, 2245 i 2354); (Dz.U.2020.346 j.t.).
2. Ustawa z dnia 5 sierpnia 2010r. o ochronie informacji niejawnych (Dz.U. 2010 nr 182 poz. 1228)
3. Rozporządzenie Prezesa Rady Ministrów z dnia 22 grudnia 2011 r. w sprawie sposobu oznaczania materiałów i umieszczania na nich klauzul tajności.
4. Rozporządzenie Ministra Obrony Narodowej z dnia 19 grudnia 2013 r. w sprawie szczegółowych zadań pełnomocników ochrony w zakresie ochrony informacji niejawnych w jednostkach organizacyjnych podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych.
5. Zarządzenie Nr 58/MON z dnia 11 grudnia 2017 r. w sprawie szczególnego sposobu organizacji i funkcjonowania kancelarii tajnych oraz innych niż kancelaria tajna komórek organizacyjnych odpowiedzialnych za przetwarzanie informacji niejawnych, sposobu i trybu przetwarzania informacji niejawnych.

Źródła internetowe

1. https://docplayer.pl/13356618-Kryptograficzne-aspekty-ochrony-informacji-niejawnych.html, 02.12.2020 r.

2. https://docplayer.pl/2802164-Warszawska-wyzsza-szkola-informatyki-systemy-wykrywania-wlaman-w-aspekcie-poglebionej-architektury-systemu-bezpieczenstwa-teleinformatycznego.html
3. https://iep.utm.edu/apriori/
4. https://r.uek.krakow.pl/bitstream/123456789/2297/1/164861786.pdf, dostęp: 03.12.2020 r.
5. https://www.bbn.gov.pl/download/1/1005/wymaganiatechnologiczne2.pdf, dostęp: 03.12.2020 r.
6. https://www.bbn.gov.pl/pl/prace-biura/publikacje/inne-wydawnictwa/biblioteka-bezpieczenst/tom-2/1000,Wizja-Sil-Zbrojnych-RP.html, dostęp: 27.10.2020 r.
7. https://www.cisco.com/en/US/docs/security/pix/pix30/user/guide/pixugint.html, dostęp: 04.12.2020 r.
8. https://www.knf.gov.pl/knf/pl/komponenty/img/knf_125701_PTE_Wytyczne_IT_16_12_2014_40005.pdf, dostęp: 27.10.2020 r.
9. https://www.researchgate.net/publication/228394375_Network_Firewalls, dostęp: 04.12.2020 r.

bsm. pchor. Marcin KAŹMIERCZAK

BIAŁY WYWIAD INTERNETOWY

Streszczenie

W niniejszym opracowaniu przedstawiono teoretyczny i praktyczny opis białego wywiadu, jego działań, roli i sposobu wykorzystywania. Opisano podstawowe zagadnienia związane z białym wywiadem, jego definicję, potencjał i zagrożenia. W dalszej części pracy zawarto opis białego wywiadu (ang. *Open Source Intelligence*, skrót OSINT) w prywatnym i publicznym sektorze. Rozwinięto specyfikę działalności białego wywiadu w Internecie. W końcowych podrozdziałach przedstawiono i opisano możliwości praktycznego wykorzystania białego wywiadu na przykładzie wybranych narzędzi, takich jak: OsintFramework, Maltego oraz Oryon OSINT Browser. W wymienionych narzędziach przybliżono i zilustrowano przykładowe sposoby pozyskiwania przez owe oprogramowania informacji na rzeczywistym przykładzie.

Słowa kluczowe:
biały wywiad, OSINT, wywiad, Internet, dane.

Abstract

Open-Source Intelligence

The paper provides both a theoretical and practical description of OSINT, its activities, role and use. Basic issues related to OSINT, its definition, potential and threats are described. In the following part of the work a description of OSINT in the private dimension and the public sector is included. The specificity of OSINT activities on the Internet was developed. The final subsections present and describe the possibilities of practical use of OSINT on the example of selected tools such as: OsintFramework, Maltego and Oryon OSINT Browser. In the tools, examples of ways in which this software can obtain information were presented and illustrated using a real-life example.

Keywords:
OSINT, intelligence, internet, data.

Wstęp

Świat, w którym żyjemy, rozwija się z niespotykaną dotychczas prędkością. Postęp technologiczny, w tym powszechny dostęp do Internetu, znacząco wpłynął na wzrost wytwarzanych przez ludzkość informacji. Produkowana i udostępniana coraz większa ilość informacji o upodobaniach użytkowników w sieci, pozwala na ich szczegółową analizę i wykorzystywanie przez osoby poszukujące danych. Do eksploracji danych i informacji wykorzystywane są techniki białego wywiadu, umożliwiające filtrowanie znacznej ilości informacji.

Biały wywiad jest elementem wykorzystywanym do pozyskiwania informacji z ogólnodostępnych źródeł, często niejasnych i wymagających weryfikacji. Przy występującej różnorodności internetowych źródeł informacji w wymiarze prywatnym i publicznym kluczowym jest znalezienie sposobu ich wykorzystania.

OSINT, czyli biały wywiad

Przystępując do omówienia pojęcia białego wywiadu należy rozpocząć od definicji wywiadu. W niniejszej pracy przyjęto definicję wywiadu jako wiedzę, którą musi posiadać państwo, w celu potwierdzenia, że interesy państwa nie są narażone na uszczerbek w żadnym stopniu, a działania podjęte przez odpowiednie instancje nie będą z góry skazane na niepowodzenie. Oznacza to, iż uzyskanie wiedzy wymaga funkcjonalnej organizacji składającej się z ludzi i określonych struktur, które otrzymają produkt informacyjny złożony z baz wiedzy, informacji o bieżących wydarzeniach i zjawiskach oraz bardzo cennych prognoz i ocen wywiadowczych[1].

Podanie dokładnej definicji pojęcia białego wywiadu nie powinno stanowić problemu. Wyrażenie to jest znane i długo używane w naszym języku. Wykorzystywane jest zarówno w żargonie służb specjalnych, jak i literaturze. Pojęcie biały wywiad występuje tylko w polskiej nomenklaturze. Z tłumaczenia rozwinięcia OSINT otrzymujemy określenie – wywiad ze źródeł otwartych. „Należy pamiętać jednak, iż akronim ten jest znacznie młodszy niż polskie pojęcie białego wywiadu. Wcześniej w literaturze anglojęzycznej używano raczej określenia wywiad jawny”[2]. Można więc postawić znak równości między pojęciami biały wywiad i OSINT. W niniejszej pracy sformułowania biały wywiad oraz Open Source Intelligence (OSINT) przyjęto jako tożsame. Biały wywiad jest metodą wykorzystywaną na przykład w pracy wywiadowczej, która w znacznym stopniu polega na analizie publikowanych oficjalnie materiałów. Polega również na jawnym nadzorowaniu i studiowaniu prasy codziennej, sprawozdań rządu, audycji radiowych i telewizyjnych i innych wielu ogólnodostępnych baz danych.

[1] M. Minkina, *Sztuka wywiadu w państwie współczesnym*, Bellona, Warszawa, 2014, s. 27
[2] B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej*, Uniwersytet Warszawski, Warszawa, 2015 s. 15

Sfomułowania biały wywiad czy OSINT są coraz powszechniejsze w codziennym użytkowaniu. Pod pojęciem biały wywiad można rozumieć wszelkie formy zdobywania informacji z wykorzystaniem różnego rodzaju, ogólnodostępnych oraz przede wszystkim jawnych źródeł[3]. Definicja ta ukazuje, iż w białym wywiadzie wykorzystywane są legalne i publiczne źródła informacji. Z ich ogólnodostępności korzystają służby specjalne i organy ścigania do szybkiego i sprawdzonego pozyskiwania informacji. W dobie powszechnego dostępu do Internetu oraz olbrzymiej popularności mediów społecznościowych, wykorzystywanie technik białego wywiadu przez służby, organy ścigania oraz osoby prywatne może przynieść im wiele korzyści i być niekończącym się źródłem informacji.

Niezależnie od tego, iż informacje zdobywane przy wykorzystaniu białego wywiadu są jawne, to działania i czynności umożliwiające pozyskanie wyznaczonych informacji mają charakter niejawny. W polskim ustawodawstwie nie zdefiniowano pojęcia biały wywiad czy otwarte źródła informacji. Określnie definicji OSINT można znaleźć w dokumencie NATO Open Source Intelligence Reader z 2002 roku. OSINT, to wynik przeprowadzenia pewnych czynności w stosunku do informacji. Są one specjalnie poszukiwane, porównywane ze sobą co do treści i wybierane są te najważniejsze dla odbiorcy procesu[4].

Biały wywiad jest bezpośrednio powiązany z czterema etapami analizowania źródeł otwartych, który w literaturze przedmiotu jest przedstawiany w następujący sposób[5]:

4. OSD (ang. *Open Source Data*) – są do dane pochodzące z pierwotnego źródła informacji, w postaci drukowanej, nośników, wystąpień, mediów społecznościowych, stron internetowych. Są to dane w stanie surowym.
5. OSIF (ang. *Open Source Information*) – dane zebrane w pierwszym etapie zostają zgromadzone w jednym dokumencie następnie poddane wstępnej analizie i rozpowszechnione.
6. OSINT (ang. *Open Source Intelligence*) – dane zostają przekazane wyselekcjonowanej grupie odbiorców, zgodnie z założeniami określonymi przez składającego zapytanie.
7. OSINT-V (ang. *Validated OSINT*) – zweryfikowane dane mające wysoki poziom pewności, potwierdzone przez inne rzetelne informacje.

[3] https://www.zawszeczujni.pl/2015/09/biay-wywiad-czyli-otwarte-zroda.html, dostęp: 30.10.2020 r.
[4] http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf, dostęp: 06, 12. 2020 r.
[5] B. Stromczyński, P. Waszkiewicz, *Biały wywiad w praktyce organów ścigania na przykładzie wykorzystania NATO Open Source Intelligence Reader serwisów społecznościowych,* „Prokuratura i Prawo" nr 5/2014, s. 4.

Główną zaletą białego wywiadu jest prędkość pozyskiwania informacji, w tym ich ilość, jakość, różnorodność i co najważniejsze niskie koszty pozyskiwania i analizy. Wzrost ilości pozyskiwanych informacji oraz coraz większej przydatności białego wywiadu jest wynikiem rewolucji w zakresie technologii informacyjnej oraz upowszechnienia Internetu. „Dzięki narzędziom inwigilacyjnym, tj. urządzeniom mobilnym i szerokopasmowemu łączu, śledzenie i analizowanie podmiotów są dostępne z każdego miejsca na ziemi”[6]. Wszyscy mają dostęp do ogólnodostępnych informacji, dlatego tak ważnym jest, aby służby specjalne monitorowały informacje z OSINT.

Potencjał i ograniczenia białego wywiadu

Działania wywiadowcze posiadają swoje unikalne cechy charakterystyczne, zalety oraz wady. Biały wywiad jest formą działalności wywiadowczej, która również posiada swoją niepowtarzalną specyfikę. Jedną z podstawowych cech białego wywiadu jest szybkość z jaką pozyskuje informacje do dalszej analizy. Pozwala to na szerokie zobrazowanie tła prowadzonych działań. Dane rozpowszechniane przez środki masowego przekazu dostarczają wiedzę, która już wcześniej była wstępnie przetworzona i potwierdzona. Według Bartosza Saramaka „pozwala to na bardzo szybkie i sprawne zapoznanie się z kontekstem społecznym, kulturowym, historycznym czy religijnym zaistniałej sytuacji”[7]. Otwarte źródła informacji wielokrotnie są na tyle szczegółowe i pewne, iż nie jest wymagane potwierdzanie tych danych innymi kosztowniejszymi metodami.

Biały wywiad posiada cały szereg zalet, dla którego warto go wykorzystywać. Podstawową przewagą jaką wywiad jawnoźródłowy posiada nad resztą dyscyplin wywiadowczych to: ilość pozyskiwanych informacji, różnorodność, jakość, szybkość i łatwość ich pozyskiwania oraz niewielkie koszty ich przetwarzania[8]. W efekcie rewolucji technologii informacyjnych oraz upowszechnionemu dostępowi do Internetu informacje z ogólnodostępnych pozyskuje się z ogromną szybkością. Szeroka informatyzacja pozwoliła na śledzenie i analizowanie w czasie rzeczywistym aktualności z drugiej strony świata. Prędkość obiegu informacji spowodowana przez szybką prace dziennikarzy powoduje, że często, w krótszym okresie media mają większą wiedzę na dany temat od służb wywiadowczych. „Niejednokrotnie najważniejsze decyzje w państwie nie są podejmowane na podstawie raportów wywiadowczych, ale

[6] A. Ziółkowska, *Biały wywiad jako element rozpoznania wojskowego*, [w:] S. Topolewski, K. Karwacka, J. Sekuła, T. Sobczyński (red.), *Aspekty bezpieczeństwa informacyjnego w obszarze cyberprzestrzeni wymiar teoretyczny i praktyczny*, Akademia Marynarki Wojennej, Gdynia 2018, s. 130.
[7] Tamże, s. 30.
[8] https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/Vol49no2/reexamining_the_distinction_3.html, dostęp: 12.11.2020 r.

informacji przekazywanych przez media (fenomen ten nazwany został „efektem CNN-u")"[9]. Niemniej celem służb specjalnych nie jest rywalizacja z mediami. Ważnym aspektem w prowadzeniu działań jest ciągły monitoring mediów.

Obecnie biały wywiad zapewnia nieograniczoną ilość źródeł pozyskiwania informacji. Kolejną ważną zaletą jest różnorodność pozyskiwanych danych. Cecha ta wpływa na możliwość wielopłaszczyznowego zarysowania bieżącej sytuacji co nie jest takie łatwe przy wykorzystaniu innych dyscyplin wywiadowczych. Różnorodność otwartych źródeł informacji jest skutkiem działalności znacznej ilości dziennikarzy, reporterów, blogerów i naukowców gotowych do podzielenia się wynikami swojej pracy. Różnorodność i ilość dostępnych informacji wzmacnia rywalizacje między konkurencją co wpływa na jakość i rzetelność informacji.

Jakość informacji jest najczęściej negowaną zaletą białego wywiadu. Jednakże istnieje wiele rzetelnych źródeł informacji, które zostały kilkukrotnie zweryfikowane. Obecna dociekliwość dziennikarzy wpływa na jakość materiałów przez nich publikowanych, których pozyskanie przy użyciu służb specjalnych byłoby znacznie droższe. Cyfryzacja wpłynęła na zniwelowanie kosztów wytwarzania i utrzymywania baz danych, wytwarzając kolejną zaletę jaka jest łatwość analizy i przetwarzania danych.

Kolejną zaletą białego wywiadu jest szeroka dystrybucja raportów opracowanych przy jego wykorzystaniu z możliwością pominięcia ochrony dotyczącej informacji niejawnych. Brak wymagań dotyczących objęcia informacji klauzulami tajności ułatwia dystrybucję i przechowywanie takowych informacji. Możliwość ta rodzi kolejne korzyści takie jak: możliwość szerszej wymiany informacji ze służbami sojuszniczymi, współpracę z podmiotami prywatnymi.

Należy również zauważyć, że biały wywiad posiada realne i dostrzegalne ograniczenia. Jedną z głównych wad, która jednocześnie może być jego zaletą jest nadmiar informacji. Różnorodność otwartych źródeł informacji skutkuje trudnościami w analizie uzyskanego materiału. Szum informacyjny jest dodatkową komplikacją utrudniającą wyselekcjonowanie prawdziwych informacji, z którą specjaliści się borykają.

Innym problemem jest trudność w zweryfikowaniu, kiedy dana informacja została opublikowana. „Bardzo trudno zweryfikować termin umieszczenia danej informacji w sieci, co utrudnia sprawdzenie ich wiarygodności oraz rzutuje na ich aktualność i przydatność"[10].

Ocenę źródła informacji dokonuje osoba dostarczającą informacje w celu określenia ich wiarygodności. Proces ten ma na celu ustalenie wiarygodności informacji oraz wpływa na proporcjonalność opcji taktycznych. Każdy kto dostarcza dane wywiadowcze zobowiązany jest do potwierdzenia

[9] B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej*, Uniwersytet Warszawski, Warszawa, 2015, s. 32.
[10] M. Minkina, *Wywiad w państwie współczesnym*, Bellona, Warszawa, 2014, s.195.

ich poprawności, w każdym możliwym źródle. Istnieje klasyfikacja uwzględniająca trzy źródła[11]:

1. wiarygodne – klasyfikacja ta jest używana, kiedy źródło jest uważane za poprawne i uzyskane informacje są wiarygodne. Obejmuje informacje podchodzące z rozpoznania osobowego, źródeł technicznych, naukowych oraz kryminalistycznych,
2. niesprawdzone – odnosi się do źródeł, które wcześniej nie dostarczyło żadnych informacji osobie, która je uzyskała lub dostarczone informacje nie zostały sprawdzone. Źródło nie musi być traktowane jako niewiarygodne, lecz do informacji dostarczonych przy pomocy tego źródła trzeba podchodzić z rozwaga,
3. niewiarygodne – źródło to powinno być wykorzystywane tylko kiedy istnieją uzasadnione podstawy, aby wątpić w wiarygodność innych źródeł. Powinny one być wyszczególnione w analizie ryzyka i zawierać obawy co do ich autentyczności, wiarygodności, kompetencji lub motywu źródła.

Przykładową ocenę źródła informacji przedstawia rysunek 7.1.

Ocena źródła	**1. Wiarygodne**	**2. Niesprawdzone**	**3. Niewiarygodne**

Źródło: Opracowanie własne na podstawie: https://www.app.college.police.uk/app-content/intelligence-management/intelligence-report/, dostęp: 07.12.2020 r.

Rysunek 7.1. Ocena źródła

Bariera językowa jest nieodłącznym ograniczeniem białego wywiadu. W świecie, w którym język angielski pełni uprzywilejowaną rolę problem nadzorowania serwisów społecznościowych staje się coraz silniejszy. Poprzez dominację języka angielskiego brakuje specjalistów posługujących się takimi językami jak: rosyjski, arabski czy chiński co wpływa na ograniczenie pozyskiwania danych z tamtych regionów, danych, które są dostępne cały czas w Internecie.

Dezinformacja jest jednym z największych mankamentów OSINT-u. Duża podatność na tego typu działania wpływa na potrzebę posiadania wyspecjalizowanego warsztatu analitycznego oraz ogromnej wiedzy ogólnej. Wymaganym jest, aby specjaliści potrafili wytworzyć dystans wobec analizowanych danych i byli obiektywni w ich ocenianiu. Wywiad jawnoźrodłowy dysponuje wieloma zaletami jak i ograniczeniami. Niemniej jednak nie ma aktualnie innej metody, która oferuje takie możliwości, przy tak niskim prawdopodobieństwie wykrycia działalności i kosztach.

[11] https://www.app.college.police.uk/app-content/intelligence-management/intelligence-report, dostęp: 07.12. 2020 r.

Biały wywiad w wymiarze prywatnym i sektorze publicznym

Z ekonomicznego punktu widzenia bezpieczeństwo narodowe to dobro publiczne wydajnie zapewniane przez rząd lub pod jego ścisłym nadzorem. Pomimo znaczącej wartości OSINT nie wymaga specjalnych uprawnień. Użytkownicy niepaństwowi mogą być lepszą alternatywą w zakresie swoich możliwości i wielkości źródeł w celu dostarczania produktów końcowych OSINT. Działanie takie przyczynia się do wzrostu bezpieczeństwa narodowego. Informacji wywiadowczych pochodzących ze źródeł ogólnodostępnych, ale uzyskanych nielegalnie nie powinno się klasyfikować jako OSINT, np. wycieków informacji niejawnych. Kluczowym punktem działalności białego wywiadu w sektorze rządowo-prywatnym jest konieczność nieujawniania informacji objętych klauzulami bezpieczeństwa, których upublicznienie mogłoby wpłynąć na bezpieczeństwo narodowe państwa. Niekiedy produkt wywiadowczy oparty wyłącznie na ogólnodostępnych informacjach musi zostać objęty klauzulą bezpieczeństwa. Czynności te wykonywane są w celu ochronienia tajnych informacji rządowym przed ujawnieniem. Agencje wywiadowcze zobligowane są do integrowania i kontrolowania działań informacyjnych oraz wysiłków innych osób w celu zapobiegania zagrożeniom bezpieczeństwa narodowego. Współpraca państwa ze środowiskami akademickimi pozwala na uniknięcie konfliktów między rządem, a podmiotem publicznym. Uczelnie są kreatywne w zdobywaniu wiedzy specjalistycznej, która istnieje w sferze publicznej. Uczelnie akademickie są idealnymi partnerami agencji wywiadowczych.

Fakt, że otwarte źródła informacji często dostarczają większość danych wywiadowczych sprawia, że biały wywiad jest niezbędnym elementem w działalności wywiadowczej. Każdy specjalista zajmujący się wywiadem powinien posiadać odpowiednią wiedzę o źródłach białego wywiadu, a w szczególności o zbieraniu oraz analizowaniu pozyskanych informacji. Niemniej jednak działalność oparta na otwartych źródłach informacji musi być wsparta specjalnymi elementami analitycznymi, by nadążyć za nowymi technologiami i sytuacją na rynku. Eksperci zajmujący się białym wywiadem są odpowiednio wyszkoleni, aby identyfikować informacje w celu zapobiegania dezinformacji. Sposobem na integrację wiedzy i umiejętności sektora prywatnego z wywiadem jest program certyfikacji OSINT-u działający w Stanach Zjednoczonych[12]. Jest to idealny sposób na osiągniecie odpowiedniego zaświadczenia przez sektor prywatny, które potwierdza wiedzę danego podmiotu na temat białego wywiadu oraz certyfikuje jego możliwości praktycznego wykorzystania.

W dzisiejszych czasach zauważyć można postępującą prywatyzację działalności wywiadowczej. Proces ten ukazuje dwa zjawiska. „Po pierwsze –

[12] https://niccs.cisa.gov/training/search/mcafee-institute/certified-open-source-intelligence-cosint, dostęp: 13.12.2020 r.

rozwój prywatnych usług wywiadowczych. Po drugie – rozwój autonomicznych struktur wywiadu biznesowego w korporacjach transnarodowych”[13]. Firmy działające na potrzeby sektora prywatnego, które zajmują się pozyskiwaniem informacji, wygenerowały kilka obszarów wywiadu. Pierwszym z nich jest wywiad, który można sformułować jako gospodarczy. W Polsce firmy zajmujące się takim wywiadem, są określane jako wywiadownie gospodarcze. Zajmują się one pozyskiwaniem informacji o spółkach i przedsiębiorstwach. Podstawowymi źródłami wywiadowni gospodarczych w Polsce są ogólnodostępne bazy danych i rejestry. Kolejnym obszarem wywiadu komercyjnego jest działalność firm polegająca no tworzeniu szczegółowych analiz wywiadowczych na płaszczyźnie strategicznej. Wiele służb specjalnych współpracuje obecnie z takimi podmiotami. Opisując obszary wywiady, należy wspomnieć o infobrokeringu. Jest to usługa zapewniająca wyszukiwanie, ocenianie, selekcję, analizę oraz udostępnianie informacji na zlecenie.

Zgodnie z definicją Głównego Urzędu Statystycznego sektor publiczny to: „Ogół podmiotów gospodarki narodowej grupujących własność państwową, własność jednostek samorządu terytorialnego lub samorządowych osób prawnych oraz „własność mieszaną” z przewagą kapitału sektora publicznego”[14]. Postęp doprowadził do zwiększenia się ogólnodostępnych źródeł informacji. Ogrom informacji uzyskiwanych przy pomocy otwartych źródłach umożliwił wspieranie procesu dowodzenia. Proces ten dzięki możliwie dużej ilości informacji, stał się względnie prostszy i ułatwił podejmowanie decyzji przez osoby funkcyjne. Przykładem instytucji korzystających z tego postępu są wszystkie urzędy administracji publicznej i ośrodki analityczne. Są to organa, które nie posiadają uprawnień w płaszczyźnie pozyskiwania informacji.

Policja, prokuratura, służby specjalne to instytucje, które w znaczący sposób skorzystały z postępu technologicznego, który wpłynął na zastosowanie najnowocześniejszych technologii w działalności wywiadowczej. Owe instytucje te wykorzystywały wcześniej biały wywiad do prowadzenia działalności, lecz nie posiadały dostępu do tak wielu otwartych źródeł informacji jak w dzisiejszych czasach. Ewolucja przemysłu informatycznego oraz technologii informacyjnych zmieniła podejście do białego wywiadu w obszarze publicznym. Zmiana ta przyczyniła się do zwiększenia wykorzystania otwartych źródeł informacji przez ten sektor.

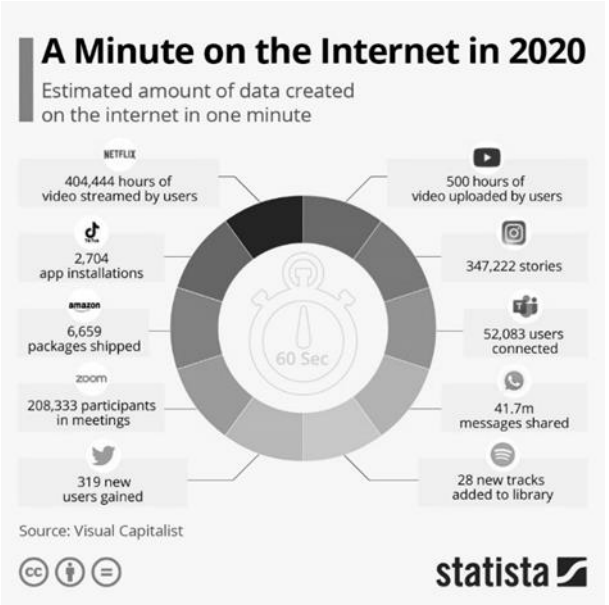
Internet a OSINT

Dostęp do Internetu jest powszechny. W 2020 roku świat zmienił się radykalnie, co wpłynęło na ilość rzeczy, która wydarzyła w nim się wydarzyła. Z powodu globalnej pandemii zmieniło się wiele aspektów życia. Praca, rozrywka, nauka to jedne z wielu przykładów, które przeniosły się do Internetu z

[13] B. Saramak, *Wykorzystanie…, dz. cyt.*, s 95.
[14] https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/2961,pojecie.html, dostęp: 21.11.2020 r.

powodu pandemii[15]. W Internecie w ciągu jednej minuty dzieje się wiele rzeczy. Minuta w Internecie w 2020 roku przedstawia rysunek 7.2.

Według Przemysława. Maciołka „Można zaryzykować nawet dość śmiałe twierdzenie, że jesteśmy świadkami rewolucji na miarę Gutenberga”[16]. Postępująca rewolucja technologii informacyjnych, przyczyniła się do zwiększenia ilości informacji oraz ich dostępności.



Źródło: https://www.statista.com/chart/17518/data-created-in-an-internet-minute/, dostęp: 13.12.2020 r.

Rysunek 7.2. Minuta w Internecie w 2020 roku

Internetu nie należy definiować jedynie jako jednego wielkiego zbioru danych, który jest kompendium wiedzy. Globalna sieć to również: zwirtualizowane biblioteki, sklepy internetowe, fora internetowe, wszelakie platformy służące do wymiany informacji. Wszechobecna informatyzacja przyczyniła się do transferu prywatnych informacji ogółu do Internetu. Dzięki sieci internetowej posiadamy dostęp do szerokiego spektrum informacji. W zależności od postawionych kryteriów wyszukiwanych danych możliwym jest odnalezienie informacji na temat przetargów skarbu państwa czy poglądów politycznych

[15] https://www.statista.com/chart/17518/data-created-in-an-internet-minute/, dostęp: 13.12.2020 r.

[16] P. Maciołek, *Internet a OSINT – Szanse i praktyczne zastosowania,* [w:] W. Filipkowski, W. Mądrzejowski (red.), *Biały wywiad Otwarte źródła informacji – wokół teorii i praktyki*, C. H. Beck, Warszawa 2012, s. 223

wybranego obywatela. Aspekty te przyczyniają się do globalizacji sieci jako pełnowartościowego źródła różnego typu informacji. Sytuacja ta stwarza możliwości dla metodyki OSINT do pozyskania informacji, dzięki którym specjaliści będą w stanie analizować bieżącą sytuacje.

Powszechny dostęp do Internetu niesie za sobą wiele korzyści jak i również zagrożeń. Fora internetowe oraz inne środki wymiany informacji są wykorzystywane przez organizacje np. terrorystyczne. Wykorzystują one globalną sieć, na przykład do rekrutowania nowych członków, rozpowszechniania materiałów propagandowych, wykorzystywania wiedzy zawartej w sieci w celu skonstruowania i wytwarzania ładunków wybuchowych. Dostęp do owych informacji jest ukryty, a dotarcie do nich może zająć wiele czasu. „Jest to kolejne zastosowanie, w którym świetnie mogą sobie poradzić komputerowe narzędzia do zbierania informacji”[17]. Zwiększona ilość informacji znajdujących się w Internecie, pozwoliła na rozwinięcie metod wydobywania informacji. Skomputeryzowanie narzędzi służących do pozyskiwania informacji jest znacznie wydajniejszą metodą w porównaniu do ręcznego zdobywania informacji. Automatyzacja takiego procesu ułatwia pracę analityka oraz udostępnia dokładne informacje jakich oczekiwał użytkownik. Proces pozyskiwania informacji znacząco się skraca oraz jakość pozyskanych informacji jest wyższa. Źródłami informacji w ogólnoświatowej sieci są nie tylko znane serwisy WWW (ang. *World Wide Web*) ale wiele różnych usług działających w ramach Internetu. Źródłami informacji w Internecie mogą być: serwisy informacyjne, portale społecznościowe, blogi, otwarte serwisy chat oraz inne źródła internetowe.

Serwisy informacyjne to jedne ze źródeł informacji przydatnych w prowadzeniu białego wywiadu w sieci. Ich zróżnicowanie pod względem ilości publikowanych informacji dziennie jest duża. W większości przypadków, takowe serwisy są zbiorem wiadomości pochodzących z wielu pras. Ponadto istnieje wiele mniejszych serwisów, które są wspierane przez większe korporacje informacyjne. Mniejsze serwisy prowadzą również dziennikarstwo obywatelskie czy portale prowadzące działalność w zakresie teorii spiskowych. Serwisy informacyjne, wraz z wyszukiwarkami, serwisami społecznościowymi oraz sklepami internetowymi należą do najczęściej odwiedzanych miejsc w Internecie. Informacje rozpowszechniane na tych stronach są jawne i ogólnodostępne, co sprzyja prowadzeniu białego wywiadu.

Następnym źródłem informacji są portale społecznościowe. Zgodnie z definicją zawartą w encyklopedii zarządzania portal społecznościowy to: „inaczej zwany serwisem społecznościowym, to witryna będąca internetowym miejscem spotkań ludzi poszukujący nowych znajomości, w których uczestnicy wymieniają się wszelkimi informacjami na podstawie swoich indywidualnych profili”[18]. Niemniej jednak, portale społecznościowe nie są najlepszym

[17] Tamże, s. 224
[18] https://mfiles.pl/pl/index.php/Portal_spo%C5%82eczno%C5%9Bciowy, dostęp: 01.12.2020 r.

źródłem informacji dla OSINT. Od niedawna pozyskiwanie informacji z serwisów społecznościowych zostało utrudnione przez wprowadzenie polityki prywatności. Powodem tej sytuacji stało się wprowadzenie Rozporządzenia o ochronie danych osobowych (RODO). „Rozporządzenie zawiera szczegółowe wymogi dla przedsiębiorstw i organizacji dotyczące gromadzenia i przechowywania danych osobowych i zarządzania nimi. Ma ono zastosowanie zarówno do europejskich organizacji przetwarzających dane osobowe osób fizycznych w UE, jak i do organizacji spoza UE kierujących swoją ofertę do mieszkańców Unii”[19]. Również użytkownicy domagali się zaostrzenia aspektu prywatności na portalach w celu chronienia swoich danych. Informacje znajdujące się na portalach mogą zostać wykorzystane do personalizowania reklam oraz profilowania użytkowników, tak jak w przypadku Cambridge Analytica[20]. Możliwości wydobywania danych z serwisów społecznościowych zostały znacząco zmniejszone z powodu ustawy o ochronie danych osobowych, które ogranicza wykorzystanie narzędzi OSINT. Jednakże, nie oznacza to braku możliwości pozyskiwania danych, lecz jego ograniczenie.

Kolejnym przykładem źródeł informacji w globalnej sieci są blogi. „Blog jest to rodzaj strony internetowej składający się z samodzielnych, specyficznych, różnorodnych, odrębnych oraz uporządkowanych chronologicznie wpisów”[21]. Na przestrzeni ostatnich lat, blogi pozyskały dużą popularność wśród użytkowników. Obecnie można wyszczególnić kilka rodzajów blogów[22]:

- blogi korporacyjne, organizacyjne – są wykorzystywane i publikowane przez organizację, w celu osiągnięcia celów organizacyjnych lub na potrzeby komunikacji wewnątrz firmy,
- internetowe pamiętniki – najpopularniejszy rodzaj blogów, w których autor dzieli się swoimi problemami czy też przemyśleniami,
- wideoblogi, fotoblogi – są publikowane w formie zdjęć lub video,
- blogi tematyczne – dotyczące danego zakresu tematów np. polityczne, edukacyjne, filmowe.

Informacje na blogu mogą być publikowane przez jednego autora lub wielu. Taka forma publikowania wiadomości cieszy się dużą popularnością. Pod kątem wykorzystania metod OSINT, blogi dostarczają wiele pełnowartościowych informacji, ponieważ mogą być kolejnym źródłem informacji, szczególnie w wąskich dziedzinach. Mogą być one również idealnym źródłem do określania obecnych trendów. Na blogach znaleźć można na przykład opisane aktualnie wydarzenia polityczne, co pozwala na uzupełnienie wiedzy w tym zakresie

[19] https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pl.html, dostęp: 13.12. 2020 r.
[20] https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie, dostęp: 13.12. 2020 r.
[21] https://kursy.operon.pl/Blogi/Co-to-jest-blog, dostęp: 01.12.2020 r.
[22] P. Maciołek, *Internet a OSINT…*, dz. cyt., s. 226.

Największa popularnością w ostatnich latach cieszy się Twitter. Jest to serwis typu microbloging, można na nim publikować jedynie wiadomości do 160 znaków. Dzięki połączeniu z wieloma innymi platformami, przepływ informacji i odwoływanie się do innych źródeł jest natychmiastowy. Blogi są rzetelnym oraz pełnowartościowym źródłem informacji.

Serwisy chat to: „najczęściej serwisy internetowe lub część strony internetowej, umożliwiająca prowadzenie rozmów między aktualnie zalogowanymi użytkownikami”[23]. Natomiast IRC są to narzędzia służące do porozumiewania się w sieci Internet. Serwisy chat IRC cieszą się ogromną popularnością wśród użytkowników. Niemniej jednak, dostęp do nich jest trudniejszy niż do blogów, gdyż wymagają założenia konta oraz jego aktywowania. Z punktu widzenia białego wywiadu, koniecznym jest stałe monitorowanie serwisów chat oraz IRC z powodu nietrwałości zawartych tamże informacji. Według Przemysława Maciołka „w praktyce źródła informacji są stosowane raczej w sposób ukierunkowany, w konkretnych, uzasadnionych przypadkach”[24]. Pozyskiwanie informacji z serwisów chat oraz IRC jest utrudnione pod wieloma względami, co prowadzi do rzadszego wykorzystania takowych źródeł.

Rozważając źródła informacji znajdujące się w globalnej sieci Internet należy przytoczyć również inne źródła, których wartość nie jest taka wysoka lub nie są tak różnorodne. Wymienione wcześniej źródła informacji nie są jedynymi źródłami białego wywiadu. Innymi źródłami są:

- bazy danych;
- serwisy aukcyjne np. eBay, Allegro;
- strony domowe;
- sieci wymiany plików.

Poddając analizie źródła informacji znajdujące się w Internecie, należy wspomnieć o pojęciu deep webu. Zgodnie z definicją zawartą w encyklopedii zarządzania deep web to: „głęboka sieć, zwana inaczej siecią ukrytą lub niewidzialną, stanowi tę część WWW, która nie jest indeksowana przez standardowe wyszukiwarki”[25]. Zgodnie z badaniami Michaela K. Bergmana z 2001 r. deep web jest od 400 do 500 razy większy od widocznej części sieci. Z badań wynika, że blisko 95% zasobów z deep webu jest powszechnie dostępna, bez konieczności uiszczania opłat, a połowa z nich to tematyczne bazy danych.[26] Rozbieżność ilości informacji wynika przede wszystkim z braku wiedzy wyszukiwarek internetowych o ograniczeniach dostępu do danych zasobów. Kolejnym z powodów jest fakt, iż poszczególne strony internetowe posiadają prężnie rozwijającą treść, która zmienia się bardzo często, w krótkich odstępach czasu. Deep web jest wartościowym źródłem informacji na potrzeby zastosowania białego wywiadu.

[23] https://slownik.intensys.pl/definicja/chat/, dostęp: 03.12.2020 r.
[24] P. Maciołek, *Internet a OSINT…*, dz. cyt., s. 229.
[25] https://mfiles.pl/pl/index.php/Deep_Web, dostęp: 03.12.2020 r.
[26] https://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104, dostęp: 03.12.2020 r.

Możliwości wykorzystania białego wywiadu na przykładzie wybranych narzędzi

Wydobywanie informacji z pozyskanych źródeł tworzy wiele możliwości ich analizowania. Zaczynając od podstawowego przeglądania, kończąc na wnikliwym budowaniu sieci powiązań, które są niezauważalne na samym początku. Niemniej jednak, aby OSINT dostarczył jakichkolwiek informacji do analizy, należy określić wymagania, skąd mają zostać pobrane. Określenie źródeł, jakie będą wykorzystywane podczas OSINT-u, wymaga wiedzy specjalistycznej. Istotnym jest sprecyzowanie adresów startowych oraz zasad przemieszczania się po otwartych źródłach. Takimi zasadami mogą być[27]:

- ograniczenia, co do zagłębiania się w odnośnikach zawartych w źródle;
- ograniczenia, co do wykraczania poza określoną domenę;
- ograniczenia rozmiarów;
- filtrowanie pobranych plików.

Podczas gromadzenia danych, wymagane jest zwrócenie uwagi, czy przetwarzane dane nie naruszają RODO (tj. adresy e-mail, nazwiska i imiona).

Proces pobierania i ekstrakcji informacji z Internetu, odbywa się w większości przypadków przy użyciu robota internetowego (ang. *crawlera*). „Crawler to program, który wykorzystywany jest przez wyszukiwarki internetowe. Jego celem jest gromadzenie informacji o strukturze oraz zawartości stron znajdujących się w Internecie, aby móc je indeksować”[28]. Zadaniami robota internetowego są między innymi: weryfikowanie kodu witryny, sprawdzanie aktualizacji informacji dostępnych w Internecie, analizowanie zawartości strony oraz kumulowanie wszelkich dodatkowych i przydatnych informacji. Jednym z najbardziej znanych crawlerów jest Googlebot. Jest to bot internetowy, który służy do indeksowania stron internetowych. Roboty firmy Google przenoszą się ze strony na kolejną stronę przy użyciu linków. Taka metoda pozwala na pobranie większej ilości danych, w krótkim okresie czasu.

W celu powstrzymania automatycznego przetwarzania strony, twórcy stron internetowych definiują w odpowiedni sposób plik robots.txt[29]. Plik ten służy do określenia, które pliki i treści mają zostać pominięte w trakcie tworzenia indeksu przeznaczonego dla wyszukiwarki. Istotnym elementem działalności OSINT jest pozyskiwanie z pierwotnie pobranego pliku informacji, które nas interesują. Proces ten jest skomplikowany, z powodu braku usystematyzowanego standardu budowy stron internetowych. Strony napisane w języku HTML[30] zawierają wiele niepotrzebnej zawartości, np. reklamy. Proces przetwarzania danych w OSINT jest bardzo ważnym składnikiem, ponieważ

[27] P. Maciołek, *Internet a a OSINT…*, dz. cyt., s. 232.
[28] https://delante.pl/definicje/crawler/, dostęp: 10.12.2020 r.
[29] http://www.robotstxt.org/robotstxt.html, dostęp: 13.12.2020 r.
[30] HTML jest to kod używany do tworzenia struktury strony i jej zawartości, źródło: https://developer.mozilla.org/pl/docs/Learn/Getting_started_with_the_web/HTML_basics, dostęp: 23.06.2021 r.

pozyskiwane są podczas niego wszelkie informacje przydatne do dalszej analizy.

Analiza sieci powiązań umożliwia ukazywanie relacji między rozpoznanymi podmiotami. Jest to kluczowa zaleta OSINT, która pozwala na badanie relacji między jednostkami. Wykorzystując zasoby z dostępnych baz danych oraz metod automatycznego rozpoznawania nazw, uzyskać można bogaty zasób informacji. Graf ukazujący relacje, ułatwia analizowanie danych, które zostały uzyskane przy użyciu białego wywiadu.

Wykorzystując sieci powiązań, analityk korzysta jedynie z interesującego go wycinka informacji, który jest przydatny w prowadzeniu badań. Na podstawie pojedynczych danych wejściowych, takich jak imię i nazwisko, analityk jest w stanie powiązać osobę między innymi: z adresami mailowymi, stronami internetowymi, portalami społecznościowymi czy numerem telefonu. „Oprócz automatycznego rozpoznawania relacji, pożądana jest możliwość ręcznego oznaczania i edycji takich danych przez eksperta oraz zapisywania, importowania, eksportowania”[31].

Kolejną metodą badania pozyskanych danych jest analiza sentymentu. Zgodnie z definicją zawartą w encyklopedii zarządzania, analiza sentymentu jest to „metoda analizy tekstu. Jej zadaniem jest wyszukać i zaklasyfikować w wypowiedzi słowa naznaczone emocjonalnie.”[32]. Jako wypowiedzi emocjonalne należy rozumieć takie wypowiedzi, które są dowodem na stan emocjonalny autora tekstu oraz takie, które wskazują na efekt emocjonalny, jaki wypowiedź ma uzyskać u odbiorcy. Istnieją dwie techniki analizy sentymentu. Są to metody[33]:

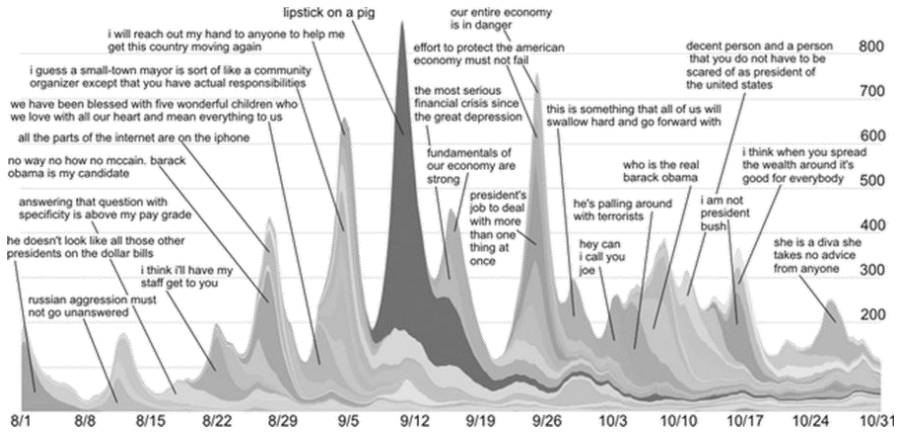
- statystyczna – polega na definiowaniu tekstu, wykorzystując przy tym dane ilościowe, takie jak liczba słow. Metoda ta wykorzystuje również drzewa decyzyjne oraz sieci neuronowe,
- słownikowa – polega na klasyfikacji wypowiedzi ze względu na istnienie słów i wyrażeń kluczowych, oraz kategoryzuje wypowiedzi ze względu na reguły leksykalne, które wskazują między innymi podobieństwa i dysonans w znaczeniach.

Wynikiem analizy sentymentu może być informacja przedstawiająca statystki związane z opiniami na dany temat. Raport taki zawiera również spis wyrażeń, które częstokrotnie zostały wykorzystane. Podczas wykorzystywania metod białego wywiadu, wyniki analizy sentymentu mogą okazać się przydatnym, dodatkowych źródłem informacji, które ułatwią pozyskanie dalszych danych. Powszechny dostęp do Internetu przyczynił się do wzrostu ilości informacji w globalnej sieci. Ciągłe monitorowanie otwartych źródeł, wraz z danymi w nich zawartymi, pozwala na badanie aktualnych trendów i nowości

[31] P. Maciołek, *Internet a OSINT…*, dz. cyt., s. 238.
[32] https://mfiles.pl/pl/index.php/Analiza_sentymentu, dostęp: 12.12.2020 r.
[33] K. Tomanek, *Analiza sentymentu - metoda analizy danych jakościowych: przykład zastosowania oraz ewaluacja słownika RID i metody klasyfikacji Bayesa w analizie danych jakościowych.* „Przegląd Socjologii Jakościowej” nr 10/2, 2014, s. 120.

w Internecie. Monitorowanie pozwala również na analizowanie zmieniających się trendów. Przykładowym narzędziem, pozwalającym na śledzenie trendów jest Google Trends, który „jest usługą, która umożliwia wgląd w informacje i statystyki na temat trendów w najpopularniejszej wyszukiwarce internetowej”[34].

Narzędzie to umożliwia porównanie popularności wielu wyszukiwanych fraz. Istnieje możliwość zawężenia obszaru porównywania, na przykład do danego kraju czy okresu. Śledzenie trendów może okazać się potrzebne podczas oceny istotności pozyskanych informacji. Aspektem śledzenia krótkich, niepowtarzalnych fraz, które przemieszczają się w Internecie, we względnie nienaruszonym stanie, zajął się zespół Cornell i Stanford University. Opracowali oni algorytmy do grupowania wariantów tekstowych poszczególnych fraz oraz identyfikację memów[35] na szeroką skalę. Badanie pokazało, że śledzenie memów jest w stanie zapewnić logiczną reprezentację cyklu wiadomości[36]. Autorzy tekstu poddali badaniu rozprzestrzenianie się popularnych fraz podczas kampanii prezydenckiej w 2008 r. w Stanach Zjednoczonych. Rysunek 7.3 obrazuje przykład śledzenia najpopularniejszych fraz podczas kampanii prezydenckiej w 2008 roku.



Źródło: http://www.memetracker.org/, dostęp: 14.12.2020 r.

Rysunek 7.3. Przykład śledzenia najpopularniejszych fraz w czasie kampanii prezydenckiej w 2008 r.

Śledzenie trendów jest skomplikowanym procesem, ponieważ występują sytuacje ewolucji cytatów znajdujących się w poszczególnych artykułach.

[34] https://www.empressia.pl/blog/172-google-trends-jak-korzystac-aby-osiagnac-najlepsze-efekty, dostęp: 12.12.2020 r.
[35] Mem to połączenie grafiki i tekstu, będące humorystycznym komentarzem do bieżących wydarzeń, prezentacją poglądów czy emocji, źródło: https://www.semtec.pl/slownik-seo/mem/, dostęp: 23.06.2021 r.
[36] https://www.cs.cornell.edu/home/kleinber/kdd09-quotes.pdf, dostęp: 31.12.2020 r.

Sytuacja ta utrudnia znalezienie początku i końca frazy oraz związku z treścią artykułu[37].

Wyróżnione możliwości zastosowania narzędzi białego wywiadu nie są jedynymi spośród tych, jakimi dysponuje OSINT. Istnieje wiele metod statystycznych, takich jak analiza czynnikowa. Występuje również wiele metod, których wykorzystywanie wymaga zgody prawnej. Takimi czynnościami mogą być: wykrywanie terrorystów przy wykorzystaniu analizy ruchu sieciowego użytkownika oraz informacji przez niego zamieszczanych i śledzenie publikacji związanych z terroryzmem[38].

OsintFramework

OsintFramework to bezpłatne narzędzie stworzone przez Justina Nordina[39]. Narzędzie służy zbieraniu informacji, głównie z bezpłatnych zasobów. Jego celem jest wspomaganie procesu pozyskiwania bezpłatnych informacji dla białego wywiadu. Niektóre usługi zawarte na stronie mogą wymagać rejestracji lub oferować większą ilość informacji po zapłacie, ale większość informacji uzyskanych za pomocą OsintFramework jest dostępna bezpłatnie. Pierwotnie narzędzie stworzone zostało w celu zwiększenia bezpieczeństwa informacji[40]. Narzędzie to jest najczęściej wykorzystywane przez analityków bezpieczeństwa oraz testerów penetracyjnych, w celu prowadzenia i pozyskiwania niezbędnych informacji dla działalności białego wywiadu. OSINT Framework kategoryzuje niektóre narzędzia poszczególnymi wskaźnikami takimi jak:

- (T) – zawiera hiperłącze do narzędzia, które wymaga instalacji na zasobach lokalnych,
- (D) – Google Dork,
- (R) – wymagana jest rejestracja,
- (M) – wskazuje adres URL zawierający wyszukiwane hasło, adres URL należy edytować samemu.

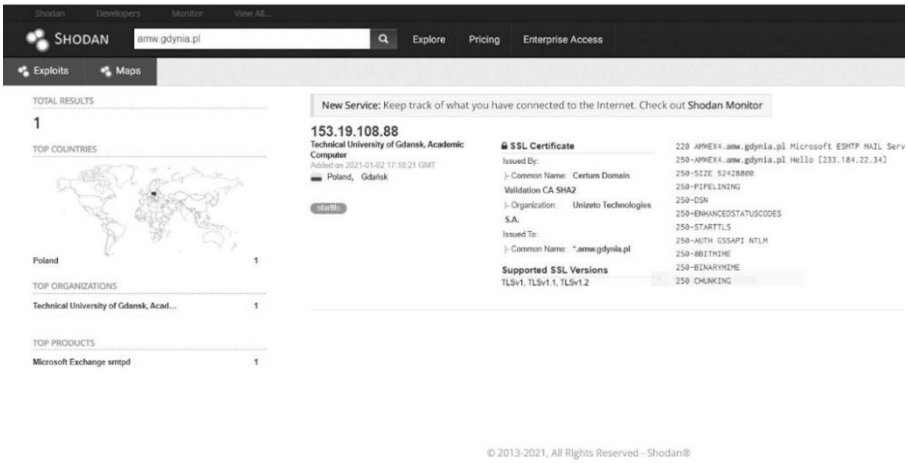
Narzędzie to jest wielką, podzieloną na poszczególne kategorie, biblioteką OSINT. Po wybraniu dowolnej kategorii, takiej jak adres email lub nazwa użytkownika, narzędzie ukazuje szereg przydatnych zasobów w postaci poddrzewa.

Według Adama Patkowskiego, istnieje duże zapotrzebowanie na teleinformatyczne narzędzia śledcze, których wykorzystanie nie ogranicza się jedynie do pracowni komputerowych czy laboratoriów[41]. OsintFramework jest

[37] P. Maciołek, *Internet a a OSINT…*, dz. cyt., s. 241.
[38] C. Saranaj, V. Murali, Using Data Mining Techniqoues for Detecting Terror – Related Activites on the Web, http://www.ijtrd.com/papers/IJTRD1325.pdf.
[39] M. Bazzell, *Open-Source Intelligence Techniques*, CreateSpace Independent Publishing Platform, nr 6/2018, s. 444.
[40] https://osintframework.com/, dostęp: 16.12.2020 r.
[41] A. Patkowski, *Narzędzia OSINT do działań operacyjnych – wybrane problemy*, [w:] J. Kosiński (red.), *Przestępczość Teleinformatyczna 2018*, Akademia Marynarki Wojennej, Gdynia 2019, s. 109

zbiorem narzędzi służącym głownie do ułatwienia, a także zautomatyzowania wyszukiwania informacji w Internecie.

Na potrzeby przedstawienia możliwości narzędzia, w celu pozyskania szczegółowych informacji o domenie, wybrano przypadek „amw.gdynia.pl". Posiadając jedynie nazwę domeny, rozpoczęto od poszukiwania informacji powiązanych z amw.gdynia.pl. OsintFramework posiada zakładkę Domain Name, która zawiera linki do narzędzi wyszukujących informacje za pomocą nazwy. Rysunek 4 obrazuje informacje pozyskane o amw.gdynia.pl przy użyciu OsintFramework.



Źródło: Opracowanie własne na podstawie narzędzia Shodan.

Rysunek 7.4. Informacje pozyskane o amw.gdynia.pl przy użyciu OsintFramework

Za pomocą narzędzia OsintFramework, o domenie amw.gdynia.pl, uzyskano następujące informacje: adres IP, lokalizację serwera i informacje na temat certyfikatów SSL.

OsintFramework oferuje wiele możliwości pozyskiwania danych podzielonych na poszczególne kategorie. Wykorzystując narzędzie umiejętnie, możliwe jest otrzymanie dużych ilości przydatnych danych. OsintFramework pozwala na szybkie uzyskiwanie danych w sposób półautomatyczny, usprawniając tym samym działania służb.

Maltego

Maltego to wszechstronne narzędzie do graficznej analizy powiązań, stworzone przez firmę Paterva. Program ten oferuje eksplorację danych i gromadzenie informacji w czasie rzeczywistym oraz przedstawia informacje na wykresie opartym na węzłach, dzięki którym połączenia i relacje są łatwe do

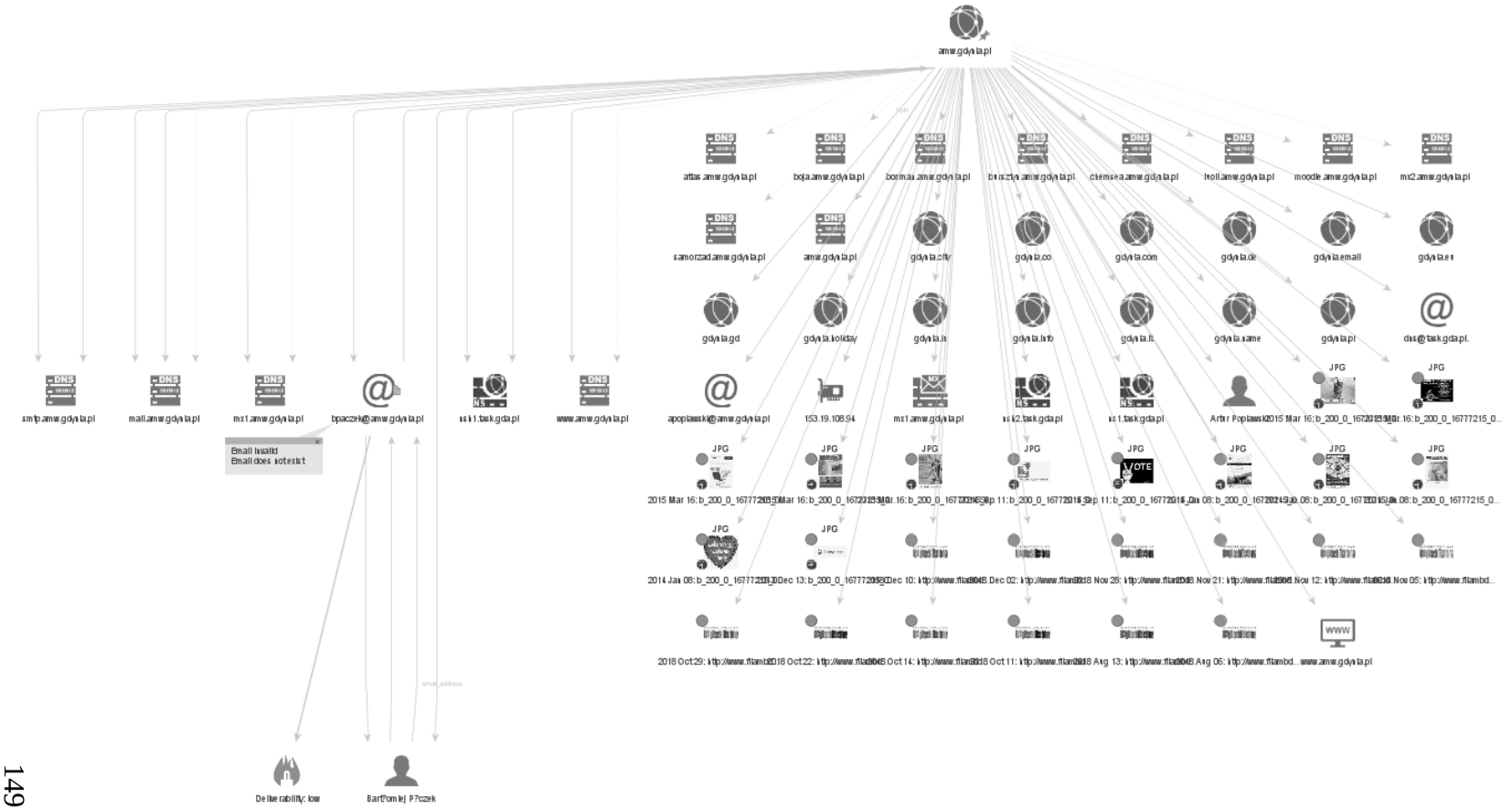
analizowania[42]. Narzędzie to pozwala na łączenie danych i funkcjonalności z różnych źródeł przy pomocy transformacji. Możliwym jest wykorzystywanie danych z firm współpracujących z Maltego oraz z własnych zasobów danych. „Zbieranie wyników za pomocą tego pakietu jest całkowicie legalne, ponieważ program ten wykorzystuje informacje ogólnie dostępne w Internecie"[43].

Maltego jest środowiskiem pozwalającym na wieloetapowe, kumulacyjne, półautomatyczne poszukiwania. Zapytanie zadane przez śledczego, jest sprawdzane przez wiele usług wyszukiwania. Wyniki mogą być ograniczone parametrami wyszukiwania[44].

Na potrzeby przedstawienia możliwości narzędzia, w celu pozyskania szczegółowych informacji o danej domenie, wybrano przypadek „amw.gdynia.pl". Posiadając jedynie nazwę domeny należy w Maltego wybrać opcję domain i wpisać w niej adres pożądanej domeny. Rysunek 7.5 przedstawia informacje uzyskane o amw.gdynia.pl przy użyciu Maltego.

Wykonanie wszelkich możliwych transformacji pozwala na uzyskanie danych takich jak: nazwy serwerów domenowych, serwery pocztowe, adresy IP, adresy email oraz jakie oprogramowanie jest wykorzystywane. Narzędzie przedstawiło również osoby powiązane z wyszukanymi adresami email. Po wykonaniu dalszych transformacji, Maltego przedstawia grafiki zamieszczone na domenie amw.gdynia.pl oraz zrzuty tej strony wykonane przy użyciu usługi The Wayback Machine.

[42] https://docs.maltego.com/support/solutions/articles/15000019166-what-is-maltego-, dostęp: 29.12.2020 r.
[43] D. Chaładyniak, A. Czarnecki, *Analiza wybranych narzędzi do pozyskiwania informacji o zaatakowanym systemie informatycznym,* „Zeszyty Naukowe WWSI", nr 17/2017, s. 84.
[44] A. Patkowski, *Narzędzia OSINT…, dz. cyt.*, s. 117.



Źródło: opracowanie własne na podstawie narzędzia Maltego.

Rysunek 7.5. Informacje uzyskane o amw.gdynia.pl przy użyciu Maltego

Oryon OSINT Browser

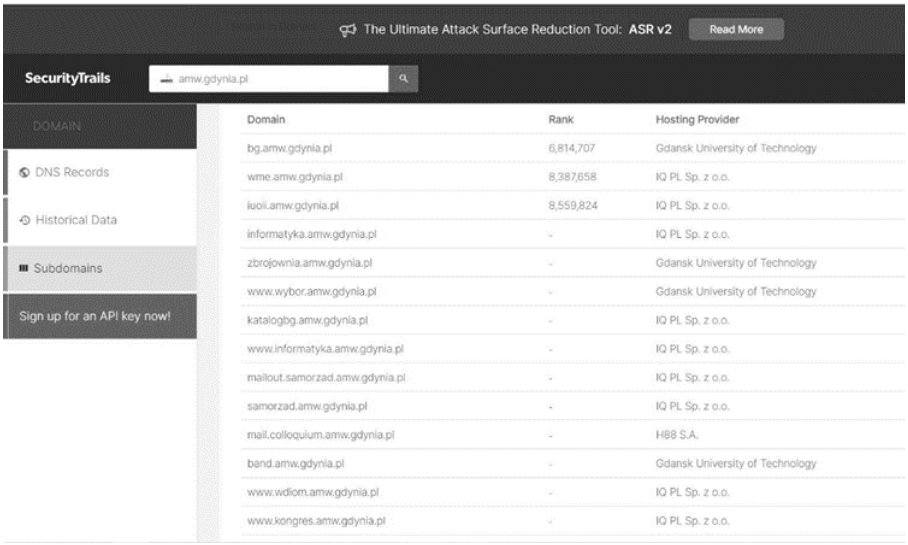
Oryon OSINT Browser to przeglądarka internetowa stworzona w celu wspomagania prowadzenia białego wywiadu przez śledczych, zawierająca dziesiątki wstępnie zainstalowanych narzędzi i zestawy linków skatalogowanych według kategorii[45]. Główną zaletą narzędzia jest możliwość rozszerzania biblioteki narzędzi według indywidualnych potrzeb użytkownika. Przeglądarka Oryon OSINT oparta jest na oprogramowaniu SRWare Iron, które zawiera silnik Chromium oraz inne komponenty zapewniające prywatność i bezpieczeństwo[46]. Dodatkowo, przeglądarka umożliwia przeprowadzanie ukierunkowanych tematycznie sprawdzeń, dotyczących zagadnień takich jak, np.: terroryzm, wyszukiwanie patentów czy wyszukiwanie ludzi.

Oryon OSINT Browser posiada wiele wbudowanych rozszerzeń takich jak: Adblock Plus, HTTPS Everywhere czy Cache Killer, których większość nie jest aktywowana i można je uruchomić na potrzeby śledztwa. Posiada również wiele przydatnych zakładek wspomagających prowadzenie białego wywiadu, na przykład: wyszukiwanie email, artykułów naukowych, informacji o domenach oraz analizowanie zdjęć.

Na potrzeby przedstawienia możliwości narzędzia, w celu pozyskania szczegółowych informacji o domenie, wybrano przypadek „amw.gdynia.pl". Do pozyskania przydatnych informacji wykorzystane zostanie wbudowane narzędzie Querytool. Jest to narzędzie oparte na Arkuszach Google, służące zautomatyzowanemu tworzeniu zapytań w znanych wyszukiwarkach, w celu uzyskania pożądanych rezultatów. Przy użyciu tego narzędzia, możliwym jest przeprowadzenie złożonego wyszukiwania, na przykład: adresów email, słów kluczowych czy osób[47]. Posiadając jedynie nazwę, należy rozpocząć od poszukiwania informacji powiązanych z amw.gdynia.pl. Rysunek 7.6 obrazuje informacje pozyskane o amw.gdynia.pl przy użyciu narzędzia Querytool.
Za pomocą narzędzia Querytool, o domenie amw.gdynia.pl uzyskano spis wszystkich istniejących subdomen oraz nazwy ich dostawców hostingu.

Oryon OSINT Browser to wszechstronne i bardzo przydatne oprogramowanie, które posiada niezbędne narzędzia do prowadzenia śledztwa, przy wykorzystaniu informacji jawnoźródłowych zawartych w globalnej sieci. Przeglądarka ta zapewnia również wiele potrzebnych danych przydatnych dla OSINT-u.

[45] https://sourceforge.net/projects/oryon-osint-browser/, dostęp: 31.12.2020 r.
[46] https://www.softpedia.com/get/Internet/Browsers/Portable-Oryon-C.shtml, dostęp: 03.01.2020 r.
[47] https://docs.google.com/spreadsheets/d/1_x3PXGOahhKT3-ePaWhb3hM1dVxjmBvsVlw6D6lilTQ/edit#gid=1116439221, dostęp: 03.01.2020 r.



Źródło: Opracowanie własne na podstawie narzędzia SecurityTrials.

Rysunek 7.6. Informacje pozyskane o amw.gdynia.pl przy użyciu Querytool

Porównując wyniki uzyskane przy wykorzystaniu przedstawionych narzędzi, należy zauważyć, że każde narzędzie dostarcza zbliżony zakres informacji, lecz występują pewne różnice. Narzędzia pozwalają na otrzymanie podobnych informacji w każdym z przypadków wyszukiwania. Niemniej jednak, każde z narzędzi posiada inny zakres wyszukiwania informacji, co skutkuje różnicami w otrzymanych wynikach. Zespolenie informacji przez wszystkie narzędzia zwiększa ich skuteczność i prawdopodobieństwo otrzymania rzetelnych danych.

Metodologia

Praca została napisana na podstawie dokładnej analizy materiałów zwartych, artykułów naukowych oraz rzetelnych stron internetowych. Praca została napisana na podstawie dokładnej analizy materiałów zwartych, artykułów naukowych oraz rzetelnych stron internetowych. Przedmiotem prowadzonych badań było znalezienie sposobu wykorzystania internetowych źródeł informacji. Celem pracy było przedstawienie problematyki białego wywiadu, zagadnień zarówno teoretycznych, jak i praktycznych z nim związanych opis najistotniejszych i niezbędnych do zrozumienia tematu pracy pojęć oraz dokonanie analizy wykorzystania białego wywiadu na rzeczywistym przykładzie. Ponadto w pracy został przedstawiony biały wywiad w kontekście Internetu. Uzyskane wyniki badania literatury w szczegółowy sposób przedstawiły problematykę białego wywiadu oraz pozwoliły na uzyskanie odpowiedzi na pytania: czym jest biały wywiad, jaki posiada potencjał oraz jak można go wykorzystać.

Przegląd literatury

Autor pracy opierał się głównie na literaturze naukowej, publikacjach naukowych oraz źródłach internetowych. Książka Michaela Bazzella pozwoliła na przedstawienie możliwości wykorzystania białego wywiadu. Analiza publikacji Wojciecha Filipkowskiego i Wiesława Mądrzejowskiego przyczyniła się do rzetelnego omówienia tematyki białego wywiadu, zarówno zagadnień teoretycznych jak i praktycznych. Wykorzystane źródła internetowe umożliwiły przedstawienie funkcjonalności, sposoby wykorzystania i użytkowania narzędzi białego wywiadu: OSINT Framework, Maltego, Oryon OSINT Browser.

Wnioski

Informacje pozyskane przy wykorzystaniu programów potwierdziły, że narzędzia realizują zadania, do których są stworzone, a nierzadko posiadają jeszcze więcej możliwości wykorzystania. Niemniej jednak, korzystanie z tych programów wymaga umiejętnego posługiwania się nimi oraz posiadania odpowiedniej wiedzy z zakresu pozyskiwania informacji i ich analizowania. Podczas prowadzenia białego wywiadu, nie należy ograniczać się do jednego narzędzia. Cytując Cedrica Westphala „Skuteczne śledztwa są pochodną szybkiego i precyzyjnego łączenia danych z wielu źródeł”[48]. Należy wykorzystywać jak największą ilość narzędzi w celu porównania uzyskanych danych z różnych źródeł. Działania takie znacząco wpływają na rzetelność i jakość pozyskanych danych.

Skala potrzeb zautomatyzowania procesu pozyskiwania informacji przez narzędzia wspomagające biały wywiad jest o wiele większa. Udoskonalanie i stopniowy progres możliwości narzędzi pozyskujących informacje, a także wzrost świadomości użytkowników sieci poprzez formalną i nieformalną edukację w tym zakresie, jest kluczowy.

Bibliografia

Opracowania zwarte

1. Minkina M., *Sztuka wywiadu w państwie współczesnym*, Bellona, Warszawa 2014.
2. Minkina M., *Wywiad w państwie współczesnym*, Bellona, Warszawa 2014.
3. Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej*, Uniwersytet Warszawski, Warszawa 2015.

Artykuły

[48] https://datawalk.com/wp-content/uploads/2018/06/DataWalk-Przewodnik-po-narzedziach-OSINT.pdf, dostęp: 03.01.2020 r.

1. Bazzell M., *Open-Source Intelligence Techniques*, CreateSpace Independent Publishing Platform, nr 6/2018.
2. Chaładyniak D., Czarnecki A., *Analiza wybranych narzędzi do pozyskiwania informacji o zaatakowanym systemie informatycznym*, Zeszyty Naukowe WWSI, nr 17/2017.
3. Maciołek P., *Internet a OSINT – Szanse i praktyczne zastosowania*, [w:] W. Filipkowski, W. Mądrzejowski (red.), *Biały wywiad Otwarte źródła informacji – wokół teorii i praktyki*, C. H. Beck, Warszawa 2012.
4. Patkowski A., *Narzędzia OSINT do działań operacyjnych – wybrane problemy*, [w:] J. Kosiński (red.), *Przestępczość Teleinformatyczna 2018*, Akademia Marynarki Wojennej, Gdynia 2019.
5. Stromczyński B., Waszkiewicz P., *Biały wywiad w praktyce organów ścigania na przykładzie wykorzystania NATO Open Source Intelligence Reader serwisów społecznościowych*, „Prokuratura i Prawo", nr 5/2014.
6. Tomanek K., *Analiza sentymentu - metoda analizy danych jakościowych: przykład zastosowania oraz ewaluacja słownika RID i metody klasyfikacji Bayesa w analizie danych jakościowych*, Przegląd Socjologii Jakościowej, nr 10/2 2014.
7. Ziółkowska A., Biały wywiad jako element rozpoznania wojskowego, [w:] S. Topolewski, K. Karwacka, J. Sekuła, T. Sobczyński (red.), Aspekty bezpieczeństwa informacyjnego w obszarze cyberprzestrzeni wymiar teoretyczny i praktyczny, Akademia Marynarki Wojennej, Gdynia 2018.

Źródła internetowe

1. http://www.ijtrd.com/papers/IJTRD1325.pdf, dostęp: 31.12.2020 r.
2. http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf, dostęp: 06.12.2021 r.
3. http://www.robotstxt.org/robotstxt.html, dostęp: 13.12.2020 r.
4. https://datawalk.com/wp-content/uploads/2018/06/DataWalk-Przewodnik-po-narzedziach-OSINT.pdf, dostęp: 03.01.2020 r.
5. https://delante.pl/definicje/crawler/, dostęp: 10.12.2020 r.
6. https://docs.google.com/spreadsheets/d/1_x3PXGOahhKT3-ePaWhb3hM1dVxjmBvsVlw6D6lilTQ/edit#gid=1116439221, dostęp: 03.01.2020 r.
7. https://docs.maltego.com/support/solutions/articles/15000019166-what-is-maltego-, dostęp: 29.12.2020 r.
8. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_pl.html, dostęp: 13.12. 2020 r.
9. https://kursy.operon.pl/Blogi/Co-to-jest-blog, dostęp: 01.12.2020 r.

10. https://mfiles.pl/pl/index.php/Analiza_sentymentu, dostęp: 12.12.2020 r.
11. https://mfiles.pl/pl/index.php/Deep_Web, dostęp: 03.12.2020 r.
12. https://mfiles.pl/pl/index.php/Portal_spo%C5%82eczno%C5%9Bciowy, dostęp: 01.12.2020 r.
13. https://niccs.cisa.gov/training/search/mcafee-institute/certified-open-source-intelligence-cosint, dostęp: 13.12.2020 r.
14. https://osintframework.com/, dostęp: 16.12.2020 r.
15. https://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104, dostęp: 03.12.2020 r.
16. https://slownik.intensys.pl/definicja/chat/, dostęp: 03.12.2020 r.
17. https://sourceforge.net/projects/oryon-osint-browser/, dostęp: 31.12.2020 r.
18. https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/2961,pojecie.html, dostęp: 21.11.2020 r.
19. https://www.app.college.police.uk/app-content/intelligence-management/intelligence-report, dostęp: 07.12. 2020 r.
20. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/Vol49no2/reexamining_the_distinction_3.htm, dostęp: 12.11.2020 r.
21. https://www.cs.cornell.edu/home/kleinber/kdd09-quotes.pdf, dostęp: 31.12.2020 r.
22. https://www.empressia.pl/blog/172-google-trends-jak-korzystac-aby-osiagnac-najlepsze-efekty, dostęp: 12.12.2020 r.
23. https://www.softpedia.com/get/Internet/Browsers/Portable-Oryon-C.shtml, dostęp: 03.01.2020 r.
24. https://www.statista.com/chart/17518/data-created-in-an-internet-minute/, dostęp: 13.12.2020 r.
25. https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie, dostęp: 13.12. 2020 r.
26. https://www.zawszeczujni.pl/2015/09/biay-wywiad-czyli-otwarte-zroda.html, dostęp: 30.10.2020 r.

bsmt pchor. Aleksandra PAWLIKOWSKA

NARZĘDZIA I TECHNIKI DEZINFORMACJI WYKORZYSTYWANE PRZEZ FEDERACJĘ ROSYJSKĄ W CYBERPRZESTRZENI

Streszczenie

Celem niniejszego opracowania jest przedstawienie i omówienie technik oraz narzędzi dezinformacyjnych wykorzystywanych przez Federację Rosyjską w cyberprzestrzeni. Praca skupia się na wyjaśnieniu podstawowych pojęć z zakresu informacji, dezinformacji, metod i technik dezinformacyjnych. Jednocześnie praca wyjaśnia zagadnienie cyberprzestrzeni, a także jej możliwości dezinformacyjnych. Dodatkowo posiada opis czynności i działań, które można wykorzystać w celu przeciwdziałania oraz zwalczania dezinformacji w cyberprzestrzeni. W dalszej części, została opisana działalność dezinformacyjna Federacji Rosyjskiej. Skupiono się w nim na charakterystyce sytuacji na gruncie dezinformacji Federacji Rosyjskiej. Następnie poruszono temat, celów Federacji Rosyjskiej, które nieodzownie związane są z polityką zagraniczną państw na arenie międzynarodowej. Fragment ten skupia się na opisaniu zagrożenia, które przynosi zjawisko dezinformacyjne mocarstwa, jakim jest Rosja. Wskazuje działania, które ukierunkowane są na destabilizację państw na płaszczyźnie gospodarczej, politycznej.

Słowa kluczowe:
dezinformacja, działalność dezinformacyjna, cyberprzestrzeń, propaganda, manipulacja, narzędzia dezinformacyjne.

Abstract

Tools and techniques of disinformation used by the Russian Federation in cyberspace

The aim of the article was to present and discuss disinformation techniques and tools used by the Russian Federation in cyberspace. The work focuses on explaining the basic concepts of information, disinformation, disinformation methods and techniques. At the same time, the article explains the issue of cyberspace, as well as it is disinformation possibilities. Additionally, it has a description of activities and things that can be used to counteract and combat disinformation in cyberspace. The last part of article describes the disinformation activity of the Russian Federation. It focuses on the characteristics of the situation on the grounds of disinformation in the Russian Federation. Then, the subject of the goals of the Russian Federation, which are indispensably related to the foreign policy of states on the international stage, was dis-

cussed. This part focus at describing the threats brought about by the disinformation phenomenon of the power of Russia. It indicates actions that are aimed at destabilizing countries on the economic and political levels.

Keywords:
disinformation, disinformation activity, cyberspace, propaganda, manipulation, disinformation tools.

Wstęp

Rozwój Internetu, technologii cyfrowej, mediów społecznościowych oraz środków komunikacji w sposób znaczący, ułatwiły przepływ informacji. Konieczność, szybkiego oraz nieskrępowanego komunikowania się z każdym użytkownikiem sprawił, iż informacja dominuje w codziennej działalności społeczeństwa. Obecnie posiadanie wiedzy oraz możliwości jej przemyślanego wykorzystania świadczą o władzy. W dzisiejszym świecie informacja traktowana jest jako element kluczowy w procesach decyzyjnych począwszy od sektora publicznego, produkcji, zarządzania i innych. Dokonany progres, w zakresie systemów informatycznych przyczynił się pozytywnie do ciągłego wzrostu gospodarki narodowej. Głównie w wymiarze usług finansowych, transportu, handlu, ale w głównej mierze komunikacji. Świat wykorzystując potężną siłę informacji udowadnia, że jest ona wielokrotnie ważniejsza, niż posiadanie surowców mineralnych, energetycznych bądź innych dóbr materialnych[1]. Tak kluczowa, a zarazem globalna moc informacji, doprowadziła do wywierania wpływu na jej sens oraz znaczenie. Niezależnie od charakteru przekazu wiadomości, przyjmuje ona charakter indywidualny albo zbiorowy. Niestety, wraz z korzystnym wpływem na rozwój, dostrzegane są także negatywne zjawiska. Uzależnienie współczesnego społeczeństwa świata od informacji, znacząco podniosło zagrożenie popularnym zjawiskiem dezinformacji. Powoduje ono zakłócenie funkcjonowania cyberprzestrzeni, a to w konsekwencji prowadzi do zagrożeń bezpieczeństwa narodowego o charakterze sieciowym.

Wielokrotnie celem manipulacji informacją, staje się umyślne i świadome wprowadzanie niepokojów społecznych, które dążą do zaburzenia funkcjonowania państwa, jego struktur, oraz poszczególnych jednostek. Działania te wykorzystują, słabość społeczeństwa informacyjnego, którego prawidłowe funkcjonowanie uzależnione jest od dostępu do wiadomości. W wielu przypadkach operacje te mają charakter zamierzony. Aktywności dezinformacyjne często ukierunkowane są w konkretną partię polityczną, organizację, liderów grup bądź niejednokrotnie w większe ugrupowania ludzi. Dostrzegane są także przedsięwzięcia kampanii dezinformacyjnych, które w widoczny sposób dążą do obciążenia funkcjonowania organizacji pozarządowych. Jednakże, gruntem szerzenia dezinformacji jest cyberprzestrzeń, która jest idealnym środowiskiem. Zaletą tego podłoża jest czas, w jakim można przekazywać informacje oraz skala dotarcia do jednostek zajmujących dowolne miejsce na kuli ziemskiej.

Z dnia na dzień proces dezinformacyjny zyskuje na swojej sile, poprzez wykorzystywanie najnowszych technik oraz narzędzi manipulacyjnych, zawierających

[1] M. J. Wachowicz, *Ujęcie teoretyczne pojęcia dezinformacji*, „Wiedza Obronna", nr 1-2/2019, s. 266-267.

w sobie pewne elementy socjotechniki. Taki typ działań umożliwiają oraz ułatwiają najnowsze technologie. Posługujące się zawansowanymi dziedzinami nauk, takimi jak informatyka, teleinformatyka oraz telekomunikacja. Ich zasięg objął już wszystkie możliwe miejsca na świecie[2].

Szeroko dostępne media bombardują natłokiem informacji. Poruszają kwestie o niskim priorytecie, zamiast skupić się na sprawach arcyważnych. Zdarza się również, że wybrane stacje telewizyjne oraz portale informacyjne celowo zmieniają sens informacji, aby przyczynić się do większego zainteresowania odbiorców.

Istota pojęcia dezinformacji

Dezinformacja nie jest zjawiskiem nowym, jej działanie dostrzegane jest na przestrzeni lat, wpływając na ukierunkowywanie poglądów oraz postaw ludzi. Stanowi podstawę każdego działania. Była i jest skutecznym narzędziem, używanym przez podmioty państwowe, podmioty niepaństwowe, osoby szukające uwagi. Rozumiana jest jako świadome przygotowywanie nieprawdziwych informacji, a następnie ich upowszechnianie. Działanie ukierunkowane jest pod kątem kreowania postaw, zachowań oraz poglądów.

Przykładem takiego działania są kampanie dezinformacyjne, które celowo rozpowszechniają fałszywe informacje, aby wpływać na opinię publiczną oraz ukryć prawdziwe wydarzenia. Niejednokrotnie dezinformacja jest pojmowana jako forma propagandy, do której wykorzystuje popularne metody rozprzestrzeniania informacji, posługując się w tym celu szeroką gamę serwisów społecznościowych oraz aplikacji.

W skrócie dezinformacja nawiązuje do umyślnego, często zorganizowanego działania. Rozumiana jako forma przekazywania nieprawdziwych, niesprecyzowanych, wprowadzających w błąd informacji. Celem postępowania jest chęć wyrządzenia szkody lub uzyskania korzyści o charakterze politycznym, finansowym lub osobistym. Niejednokrotnie proces ten obejmuje szeroki zakres, jeśli chodzi o jego działanie.

Wynikiem rozpatrywanych działań jest celowe oderwanie uwagi od niezwykle niebezpiecznego zjawiska bądź sytuacji, a skupienie jej na sprawach mniej znaczących. Zauważalne jest ono w mediach, radiu, Internecie. Sprawy istotne znikają w natłoku błahych wiadomości[3].

Niestety w dokumentach na temat bezpieczeństwa nie ma jednej precyzyjnej definicji zjawiska dezinformacji. Natomiast, niektórzy specjaliści starają się skupić na stworzeniu pomocnego sformułowania. Poniżej zostały przytoczono niektóre definicje:

[2] I. Oleksiewicz, *Bezpieczeństwo informacyjne w cyberprzestrzeni a stany nadzwyczajne*, „Zarządzanie", nr 33/2019, s. 144-153.

[3] M. Świerczek, „*System matrioszek", czyli dezinformacja doskonała. Wstęp do zagadnienia*, „Przegląd Bezpieczeństwa Wewnętrznego", 10(19)/2018, s. 210.

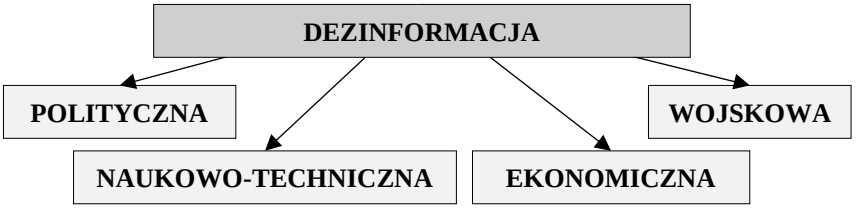
1. Celowo fałszowana informacja, która ma wpływać na określoną grupę ludzi lub całą populację. Jest to jedna z podstawowych metod pracy operacyjnej wywiadu, służąca wpłynięciu na postępowanie przeciwnika, by zachował się korzystnie dla służby wywiadowczej. Przeciwnikiem może być wrogi wywiad lub inna organizacja lub osoba, przeciwko której skierowane są działania służby. Dezinformacje dzieli się na strategiczne, o długoterminowych planach i zamierzeniach oraz dezinformacje operatywne, które tworzy się w zależności od chwilowej sytuacji. Dezinformacja pod względem formy może być językowa, obrazowa lub demonstracyjna (prezentacja obiektów fizycznych)[4].
2. Tworzenie i rozprzestrzenianie mylącej lub fałszywej informacji w celu zniekształcenia obrazu przeciwnika[5].
3. Dezinformacja (…) jest celowym przekazywaniem przeciwnikowi, za pomocą środków i metod pracy operacyjnej, nieprawdziwych informacji w celu wprowadzenia go w błąd i uzyskania zaplanowanych rezultatów[6].
4. Dezinformacja opiera się na prowokacji a nie na kłamstwie. Każde państwo używa swoich źródeł wywiadów do przybliżenia obrazu prowokującego przeciwnika do podejmowania błędnych ocen[7].
5. Dezinformacja stawia sobie za cel realizację konsekwentnego programu zmierzającego do zastąpienia w świadomości, a przede wszystkim podświadomości, mas będących przedmiotem tych działań poglądów uznawanych za niekorzystne dla dezinformatora takimi, które uważa on za korzystne dla siebie[8].
6. Dezinformacja rozumiana jest wprowadzanie w błąd osoby, poprzez podawanie nieprawdziwych informacji[9].
7. Dezinformacja jest to zamierzone opracowywanie oraz rozpowszechnianie bądź bezpośrednie przekazywanie rozpoznaniu przeciwnika mylnych wiadomości dotyczących wojsk, prowadzonych działaniach itp.[10]

Głównym środowiskiem działań dezinformacyjnych jest cyberprzestrzeń, a do jej głównych założeń należą trzy rodzaje zadań. Zaliczają do nich

[4] K. Wojciechowski (tłum.), *Encyklopedia szpiegostwa*, Wydawnictwo Spar, Warszawa 1995, s. 72-73.
[5] N. Polmar, T. B. Allen*, Księga szpiegów. Encyklopedia*, Magnum, Warszawa 2000, s. 151.
[6] H. Lewandowski, *Podstęp, inspiracja i dezinformacja w działalności służb specjalnych*, UOP, Warszawa 2000, s. 81-82.
[7] E. J. Epstein*, Podstęp. Niewidzialna wojna między KGB a CIA*, Scripta Manent, Krosno 1993, s. 31.
[8] V. Volkoff , *Dezinformacja – oręż wojny*, , Wydawnictwo Antyk Marcin Dybowski, Komorów 1991, s. 8.
[9] https://sjp.pwn.pl/sjp/dezinformacja;2554971.html, dostęp: 07.12.2020 r.
[10] P. Dela, *Teoria walki w cyberprzestrzeni*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2020.

między innymi: celowe wprowadzenie w błąd przeciwnika w danej kwestii, wykorzystując w tym zakresie tylko sposoby dezinformowania. Kolejnym przykładem są działania dążące do upewniania przeciwnika, że ma racje, natomiast w rzeczywistości są one mylne. Ostatnim rodzajem zadań są te, które realizowane są z premedytacja i polegają na skupieniu uwagi rozpoznania przeciwnika.

Współcześnie dezinformacja zajmuje każdy, możliwy aspekt funkcjonowania państwa. Od sfery politycznej, naukowo-technicznej, ekonomicznej po wojskową. Poprzez skonkretyzowanie wyróżnia się cztery rodzaje dezinformacji: polityczną, naukowo-techniczną, ekonomiczną oraz wojskową[11]. Rodzaje dezinformacji obrazuje rysunek 8.1.



Źródło: Opracowanie na podstawie: A. Żebrowski, *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Karków 2016, s. 447.

Rysunek 8.0. Rodzaje dezinformacji

Dezinformacja polityczna uwidacznia swoje działanie w strefie wewnętrznej i zewnętrznej państwa (polityka zagraniczna). Prowadzona jest na przez organy decyzyjne oraz kierownicze. Skupiając się na polityce wewnętrznej kraju dotyczy ogółu obywateli. Jej działanie polega na, modelowaniu określonych postaw, zachowań oraz opinii publicznych, poprzez proces ustawodawstwa, kształcenia, wychowania, informowania oraz programy naukowo-badawcze. Natomiast w sferze zewnętrznej państwa dezinformacja, kieruje swoje działania na budowanie jak najbardziej pozytywnego obrazu państwa. Głównym celem dezinformacji politycznej jest ukrycie działań, które mogłyby wywołać krytykę, bądź dezaprobatę innych krajów. Natomiast na ogół priorytetem tego działania jest zdobywanie poparcia przez inne społeczności międzynarodowe[12].

Dezinformacja o charakterze naukowo-technicznym, prowadzi swoje działania w ten sposób, aby przeciwnik nie odkrył prawdziwego celu działania. Chodzi o ukrycie postępów w zakresie odkryć naukowo-technicznych, które

[11] A. Żebrowski, *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2016, s. 447.
[12] Tamże, s. 447.

przyczyniają się podnoszenia zdolności pod kątem obronności, poziomu wyszkolenia wojsk, technik oraz uzbrojenia[13].

Dezinformację ekonomiczną cechuje świadome wprowadzanie przeciwnika w błąd w aspekcie swoich dotychczasowych osiągnięć ekonomicznych. Skupiają się one w szczególności na zatajaniu elementów związanych z obronnością kraju. Tyczy się to obiektów, metod i produkcji[14].

Dezinformacja wojskowa skupia swoja działalność na takich obiektach jak: przeciwnik, wojska własne oraz otoczenie, z którymi związane są kontakty z innymi państwami. Działania owego procesu dezinformacyjnego ukierunkowane są w systemy kierowania oraz dowodzenia, poprzez rozsyłanie fałszywych informacji wykorzystując systemy rozpoznawcze. Działanie te ma na celu wprowadzić w błąd swojego przeciwnika, w taki sposób, aby nie był świadomy i wychodził z przekonania, że zna zamiary państwa a w rzeczywistości ma zupełnie odmienne informacje. Proces ten występuje niezależenie od czasu pokoju, kryzysu czy wojny[15].

Elementy dezinformacji, które wpływają na skuteczność prowadzenia działań, określane są przez następujące zasady, do których należą: 1) zasada celowości; 2) zasada przygotowania; 3) zasada kompleksowości; 4) zasada scentralizowanego kierowania; 5) zasada wiarygodności; 6) zasada dublowania; 7) zasada elastyczności; 8) zasada terminowości; 9) zasada ciągłości; 10) zasada spójności; 11) zasada nieszablonowości; 12) zasada skrytości[16].

Rozpatrując pojęcie dezinformacji należy pamiętać, że przyjmuje ona wielorakie formy. Jedną z nich jest propaganda, która związana jest z historią ludzkości oraz potrzebą wywierania wpływu rządzących na innych ludzi.

Metody oraz techniki dezinformacji

Działania dezinformacyjne prowadzone są z użyciem metod oraz technik, które stosują nowoczesny zasób sił i środków. Z ich pomocą, celowo podaje się mylące i niedokładnie skonstruowane wiadomości, mające za zadanie zmylić odbiorców. Często powiązane są z socjotechnikami, które wywierają wpływ na myśli, uczucia oraz ludzkie zachowania. Natomiast metody wykorzystania dezinformacji uzależnione są od występowania od wielu czynników. Elementami tymi są między innymi: sytuacja polityczna, militarna, ekonomiczna. Związana jest niejednokrotnie z siłami przeciwnika, zainteresowaniem przez służby specjalne oraz rozpoznawcze[17].

Analizując metody, sposoby i użyte środki, można wymienić trzy zasadnicze formy dezinformacji: przekaz, dokument oraz działanie.

[13] Tamże, s. 447.
[14] Tamże, s. 447.
[15] Tamże, s. 447.
[16] T. Grabowski, *Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego (2014-2016)*, Horyzonty Polityki, 7(20)/2016, s. 43.
[17] *Tamże*, s. 454.

Forma przekazu dzieli się na dwie kategorie, a mianowicie ustną i pisemną. Pierwsza z nich mówi o dostarczaniu swojemu przeciwnikowi, informacji niezgodnych z prawdą. W tym celu posługuje się taki elementami jak ludność miejscowa, telewizja, radio, Internet, firmy, wojska i inne. Natomiast druga ma ten sam cel, jedyną różnicą jest to, iż forma przekazu odnosi się do zmanipulowanych dokumentów, zarządzeń, rozkazów[18].

Dokument jest drugą forma przekazu, która uważana i traktowana jest, jako najbardziej adekwatna i efektywna forma. Polega na przekazywaniu przeciwnikowi sfałszowanych dokumentów, zwierających przede wszystkim mapy, decyzje, schematy oraz harmonogramy. Celem wykorzystania tej formy przekazu skuteczne użycie działań pozoracyjnych, w które doprowadzą do sytuacji, w której przeciwnik uznaje działania, jako rzeczywiste[19].

Ostatnia forma przekazu skupia się na działaniu, którego celem jest doręczenie fałszywych widomości, zawierających zmanipulowane informacje. Aby proces był pomyślnie zakończony, koniecznie musi nastąpić użycie sił i środków, które wywrą wpływ na zmylenie przeciwnika[20].
Kluczowym elementem dezinformacji są ludzie, ponieważ to oni utożsamiani są z nośnikiem przekazu informacji. Tworzą ją zaangażowane grupy, które składają się z przedstawicieli takich grup jak pracownicy firm, ambasad, urzędów, telewizji, mediów społecznościowych oraz wiele innych. Dodatkowe elementy stanowią natomiast sprzęt oraz kanały transmisyjne[21].

Kolejnym przykładem dezinformacji jest manipulacja. Słowo manipulacja w szerokim znaczeniu rozumiana jest jako „zmiana czegoś". Natomiast w wąskim znaczeniu oznacza „wpływ", najczęściej „wpływ kogoś" lub „wpływ kogoś przez zmianę czegoś". Termin manipulacja, często mylony jest z propagandą. Manipulacja opisywana jest w znaczeniu „wpływów opinii". Rozumowana jest traktowana jest jako „cel", a innymi słowy, jako „wpływ"[22]. Sposoby manipulowania i ich charakterystyka przedstawiono w tabeli 8.1.

Następny przykład dezinformacji stanowi propaganda, niestety nie posiada ona jednej szczegółowej definicji. Rozpatrując ją według znanego amerykańskiego socjologa Williama Bidelle'a, oznacza: „propaganda używana jest w kontekście politycznym, oznacza złożone formy wpływów". Jednakże w książce Piotra Deli propaganda rozumiana jest jako szerzenie wyjątkowo stronniczych ideałów oraz poglądów. Używając w tym celu najczęściej kłamstw, podstępów oraz wcześniej opisywanej manipulacji[23].

[18] Tamże, s. 454.
[19] Tamże, s. 454.
[20] R. Szpyra, *Militarne operacje informacyjne*, Wydawnictwo AON, Warszawa 2003, s. 137-138.
[21] Tamże, s. 455.
[22] https://www.bpb.de/gesellschaft/medien-und-sport/bilder-in-geschichte-und-politik/73234/manipulation-und-propaganda?p=2, dostęp: 14.12.2020 r.
[23] P. Dela, *Teoria walki w cyberprzestrzeni*, Akademia Sztuki Wojennej, Warszawa 2020, s. 111.

Tabela 8.1

Sposoby manipulowania i ich charakterystyka

SPOSOBY MANIPULOWANIA	CHARAKTERYSTYKA SPOSOBÓW MANIPULOWANIA
Przekazywanie nieprawdziwych danych.	Podanie podmiotowi oddziaływania, danych z gruntu nieprawdziwych, jednak takich, które powinny utkwić w podświadomości, jako możliwe.
Preparowanie i przesyłanie do przedmiotu danych nieważnych lub mało ważnych z pominięciem najważniejszych.	Odnosi się do przekazywania danych skierowanych do stanu osobowego wojsk przeciwnika i jego ludności na zasadzie przedstawienia rzeczywistego obrazu w tzw. krzywym zwierciadle.
Przekazywanie danych o dużym znaczeniu jako marginalnych.	Każda postać danej, nawet bardzo istotna, przekazywana w dalszej kolejności komunikatu informacyjnego staje się mniej ważną, nieznacząca wiadomością, na którą przedmiot nie zwraca uwagi.
Udostępnianie danych preparowanych w celu wywalania określonych interwencji.	Może być spreparowany do wywołania tzw. tematów dyżurnych. Permanentne przekazywania danych może stanowić swoisty impuls do podjęcia działań interwencyjnych, dociekania prawdy, ucieczki z pola walki i innych tego typu zachowań.
Przesyłanie danych wieloznacznych utrudniających zrozumienie.	Może doprowadzić u ich odbiorcy (przedmiot oddziaływań) do wytworzenia mylnego obrazu tego, co ważne z punktu widzenia celu prowadzenia działań.
Generowanie nadmiaru danych, by spowodować tzw. chaos informacyjny.	To przekazanie danych w nadmiarze, które prowadzi do chaosu informacyjnego. Podmioty może zasypać przedmiot oddziaływana tak dużą ilością danych o faktach i zjawiskach pola walki, że spowoduje u niego brak wrażliwości na istotne i ważne wiadomości.

Źródło: Opracowanie na podstawie: J. Janczak, Zakłócenia informacyjne, Wydawnictwo AON, Warszawa 2001.

Obecnie propaganda opisywana jest jako świadomy proces, wykorzystujący wszystkie formy publicznych i masowo wytwarzanych komunikatów. Wiadomości te są tworzone celowo, w bardzo przemyślany sposób. Mają one wywierać wpływ na emocje, umysły wybranych grup odbiorców tak, aby zrealizować z góry założony cel. Składowe propagandy przedstawia tabela 8.2.

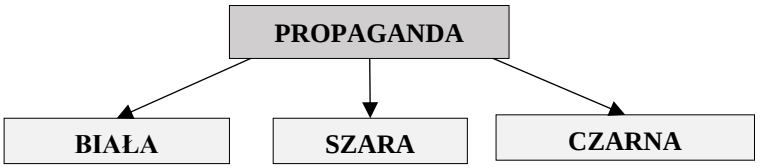
Tabela 8.2

Schemat kampanii dezinformacyjnej

S - Source	Źródło	Kanały informacyjne propagandy
T - Time	Czas	Czas rozpoczęcia i prowadzenia kampanii propagandowej
A - Audience	Publiczność	Odbiorcy propagandy
S - Subject	Temat	Sprawa, której dotyka kampania propagandowa
M - Mission	Misja	Cel kampanii propagandowej powiązany z celem politycznym, itp.

Źródło: Opracowanie na podstawie P. Dela, *Teoria walki w cyberprzestrzeni*, Akademia Sztuki Wojennej, Warszawa 2020.

Pierwsza składowa charakteryzuje źródło informacji, za pomocą których prowadzone są działania propagandowe tzn. kanały informacyjne propagandy. Obecnie zaliczanymi elementami źródła informacji są przede wszystkim: telewizja, prasa, Internet, kanały społecznościowe i inne. Czas odnosi się do momentu rozpoczęcia do chwili zakończenia podejmowanych działań. Jest bardzo istotnym elementem, ponieważ występuje zazwyczaj podczas kryzysu, zbliżających się wyborów. Zależy on także od grupy odbiorców, w jaką jest wycelowana, a także od ich przekonań, idei oraz wykształcenia. Sam temat propagandy jest silnie związany z poglądami oraz oczekiwaniami grup docelowych. Natomiast ostatnim elementem działań kampanii propagandowych jest cel, który został postawiony na początku kampanii. Propaganda, ze względu na swój szczególny charakter została podzielona na trzy grupy. Mianowicie dzieli się ja na propagandę białą, szarą oraz czarną (rys 8.2).



Źródło: Opracowanie na podstawie T. R. Aleksandrowicz, *Podstawy walki informacyjnej*, Editions Spotkania Spółka, Warszawa 2016, s. 85.

Rysunek 8.1. Rodzaje propagandy

Biała propaganda swoje działanie skupia na przekazywaniu informacji w taki sposób, aby ominąć niekorzystne aspekty informacji, które mogą być odebrane negatywnie. Kreuje natomiast wiadomości, które mają charakter pozytywny. Szara propaganda dotyczy, informacji tajnych. Związane są one zazwyczaj z funkcjonowaniem państwa, partii politycznych. Zauważalna jest w mediach, kiedy dziennikarz nie chce ujawnić źródła swoich informacji. Czarna propaganda jest połączeniem propagandy białej i szarej. Jej kluczowym elementem jest kłamstwo i manipulacja. Informacje te nie mają nic wspólnego ze stanem faktycznym albo są przesadzone.

Narzędzia wykorzystywane w procesie rozprzestrzeniania dezinformacji

Współcześnie istnieje wiele narzędzi, które umożliwiają rozprzestrzenianie się dezinformacji. Tabela 8.3 przestawia, wybrane z nich.

Tabela 8.3

Sposoby manipulowania i ich charakterystyka

NARZĘDZIA DEZINFORMACJI	ZAKRES DZIAŁANIA
Farmy trolli	Grupy celowo publikujące duże ilości fałszywych informacji.
Boty	Zautomatyzowane chatboty oraz voiceboty, wykorzystywane w celu rozprzestrzenienia dezinformacji.
Wyszukiwarka TOR	Publikowanie za pomocą wyszukiwarki TOR.
Rekrutacja innych ludzi	Wyłanianie ludzi do wstawiania zmanipulowanych postów.
Portale społecznościowe (Facebook, Twitter, Reddit, itp.)	Publikowanie zmanipulowanych i fałszywych informacji.
Połączenia VPN	Łączenie się z publicznymi adresami IP.
Fake news	Celowe wstawianie fałszywych informacji.
Hotspot	Wysyłanie i wstawianie postów, wykorzystujących dostęp do otwartych hotspotów.
Adres MAC	Zmienianie adresu MAC.
DeepFake	Filmy zawierające zmanipulowaną treść.
Spear Phishing	Rozsyłanie wiadomości wprowadzających w błąd.

Źródło: Opracowanie własne na podstawie źródeł w Internecie.

Jednym z pierwszych narzędzi wykorzystywanym w procesie dezinformacji są tzw. *farmy trolli*. Tworzą je zazwyczaj zespoły rządowe, wojskowe bądź korporacje. Są one zaangażowane w manipulowanie opinią publiczną w mediach społecznościowych, natomiast środki finansowe na ich opłacenie pochodzą zazwyczaj z pieniędzy publicznych. Zatrudniane osoby jako główne zadanie mają rozsiewać niezgodę i buntować ludzi w określonym celu w zależności od ich pobudek. Ich działania polegają przede wszystkim na komentowaniu, poprzez tworzenie własnych komentarzy. Nie posługują się oni gotowymi szablonami. Osoby, które piszą i publikują dane komentarze w łatwy sposób manipulują, użytkowników portali danych platform.

Jako drugie narzędzie stosowane w procesie dezinformacyjnym można zaliczyć zautomatyzowane *boty*. Oprogramowania wykorzystywane są często jako zautomatyzowane narzędzie w celu tworzenia treści w mediach społecznościowych. Jednakże zauważalne są także konta prowadzone przez ludzi, które nie korzystają z automatyzacji. Działanie polega na angażowaniu się w rozmowy przez zamieszczanie komentarzy lub prywatne wysyłanie wia-

domości do osób za pośrednictwem platform społecznościowych. Konta zazwyczaj obsługiwane są przez zatrudnionych w mniej więcej 60 lub 70 krajach. Ich wzmożone działanie zauważalne jest w trakcie trwania np. wyborów prezydenckich. Powodują one generowanie ogromnych ilości postów na platformach oraz portalach. Niejednokrotnie posty są przykładem wsparcia bądź atakowania kandydatów.

Trzecim narzędziem wykorzystywanym w procesie dezinformacji jest przeglądarka *TOR* (*ang. The Onion Router*), która wykorzystuje anonimizację ruchu internetowego, przez sieć *TOR*. Jest ona wolniejsza, natomiast kontrolowanie użytkowników jest niemożliwe. Wykorzystywana jest przez osoby, które nie chcą, aby ich aktywność w sieci była kontrolowana przez rządy bądź służby. Poprzez swoją strukturę, składającą się z trójwarstwowego *proxy*, przeglądarka *TOR* łączy się losowo z jednym z publicznie wymienionych węzłów wejściowych, odbijając ruch przez losowo wybrany środowy przekaźnik, a na koniec kieruje ruch przez trzeci i ostatni węzeł wyjścia. Z tego powodu adres IP na komputerze jest zupełnie inny i wskazuje zazwyczaj dowolne miejsce na świecie. Przeglądarka ta zapewnia anonimowe przeglądanie stron internetowych, a co za tym idzie publikowane w niej treści także ulegają procesom dezinformacyjnym.

Następnym sposobem jest *wyłanianie ludzi*, którzy celowo publikują zmanipulowane treści w celu szerzenia dezinformacji. Niejednokrotnie jest to zamierzone i zaplanowane działanie. Zlecone zazwyczaj przez rządy, partie bądź grupy, które chcą doprowadzić do niepokoju i buntów.

Kolejnym narzędziem są *portale społecznościowe*. Większość osób, funkcjonujących w obecnych czasach posiada przynajmniej jedno bądź więcej kont na tego typu portalach. Tworzą one idealne środowisko do publikowania mylnych lub fałszywych informacji. Często wykorzystywane przez firmy bądź sztaby polityków. Docierają do użytkowników, przez ciasteczka, które wielokrotnie posiadają całą gamę informacji o poszczególnych osobach. Począwszy od ich zainteresowań, miejsca pracy, urodzenia, grona znajomych, czy też poglądów. Cała lista informacji pozwala ukierunkowywać poglądy oraz niejednokrotnie wpływać na decyzję użytkowników.

Następnym elementem wykorzystywanym w bezpiecznym procesie rozprzestrzeniania dezinformacji jest połączenie *VPN*, które zabezpiecza połączenie szyfrowaniem i gwarantuje zachowanie swojej anonimowości przez osoby publikujące informacje.

Fałszywe informacje (ang. *fake news*) stanowią jedno z wielu narządzi dezinformacyjnych. Przede wszystkim są to celowo wykonane, sensacyjne oraz emocjonalnie wzbogacone, wprowadzające w błąd lub całkowicie sfabrykowane informacje. Mają one za zadanie naśladować formę głównego nurtu wiadomości[24]. Pozwalają one szybciej rozprzestrzeniać informacje w sieci. Aczkolwiek musza być spełnione trzy kryteria, aby *fake news* odniósł sukces

[24] https://guides.lib.uw.edu/c.php?g=345925&p=7772376, dostęp: 02.01.2021 r.

na jak najwyższą skalę. Kryteriami tymi są w szczególności narzędzia oraz usługi manipulowania, motywacja oraz miejsce rozpowszechniania w portalach i platformach społecznościowych, które zbierają informacje na temat swoich użytkowników. Do przykładów należą: ankiety, zdjęcia, polubienia stron albo kont. Wszystkie te aspekty pozwalają zebrać bazę danych o osobach i tworzyć fałszywe informacje, w których ofiarami stają się odbiorcy.

Otwarte *hotspoty* są miejscem, najczęściej wykorzystywanym do publikowania treści. Pozwalają one udostępniać informacje, oczyszczając z odpowiedzialności osobę, która opublikowała sfałszowane treści.

Zmiana adresu *MAC* ma na celu utrudnić weryfikację osoby, która publikuje nieodpowiednie bądź zmanipulowane treści na portalach i platformach społecznościowych. W ten sposób osoby publikujące mylące i celowo wprowadzające w błąd informacje dbają o swoją anonimowość.

Deepfakes stanowi jedno z najnowszych dotychczas narzędzi dezinformacyjnych. Skupia się na manipulacji dźwięku, wideo albo obrazu. Najczęściej wykorzystywany w sposób bardzo złośliwy oraz obraźliwy w stosunku do osób publicznych. Jego cechą charakterystyczną jest sposób błyskawicznego rozprzestrzeniania w sieci fałszywych słów i działań. Jeśli w filmie został użyty wizerunek osoby zaangażowanej publicznie, ciężko rozróżnić, czy jest on sfabrykowany bądź autentyczny.

Spear phishing jest także narzędziem dezinformacyjnym, polegającym na rozsyłaniu fałszywych bądź wprowadzających w błąd informacji. Wpływa niejednokrotnie na decyzje odbiorcy lub złe zrozumienie informacji. Natomiast głównymi metodami szerzenia dezinformacji jest:

- selektywna cenzura;
- manipulowanie rankingami wyszukiwania;
- hakowanie i rozpowszechnianie;
- bezpośrednie udostępnianie dezinformacji[25].

Selektywna cenzura, polega na usuwaniu niektórych treści z sieci, a pozostawieniu jedynie treści samych formularzy. Pliki te dokumentują samą aktywność z wykorzystaniem danych. Wyselekcjonowanie usuwania wybranych treści służy uprzywilejowaniu dezinformacji, która nie podlega cenzurowaniu, a jedynie wpływa na jasne jej szerzenie[26].

Kolejna metoda odnosząca się do manipulowania rankingami wyszukiwania, polega na manipulacji algorytmami samego wyszukiwania bądź samymi jej źródłami. Przykładem jest wyszukiwarka Google. Zawieranie słów kluczowych bądź słów bardzo popularnych pomagają reklamować strony internetowe w jej rankingach. Niejednokrotnie wykorzystywane są w tym celu kotwice, których zadaniem jest powiązywać konkretne zapytania z wymaganymi stronami internetowymi. Manipulacja algorytmiczna dostrzegana jest np. w okre-

[25] https://www.hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf, dostęp: 12.01.2021 r.
[26] Tamże.

sie przed wyborami nie tylko na stronach internetowych, ale także na platformach społecznościowych przez powiązanie ich z tzw. *hashtagami* oraz informacją na temat lokalizacji grup odbiorców np. na Facebooku oraz Twitterze. Metoda ta może służyć jako narzędzie do pomiaru kampanii dezinformacyjnych[27].

Trzecia metoda polegająca na hakowaniu i rozprzestrzenianiu informacji polega na hakowaniu informacji wrażliwych bądź szkodliwych, szczególnie z kont pocztowych. Przykładem takich wycieków jest wypłynięcie baz danych na temat kampanii wyborczych kandydatów. Następnie działanie to prowadzi do rozpowszechniania szkodliwych informacji przez farmy trolli oraz boty, które powiązują to z wcześniej wspomnianym wyciekiem informacji z kont pocztowych[28].

Bezpośrednie udostępnianie dezinformacji polega na udostępnianiu portalom społecznościowym już zmanipulowanych bądź sfałszowanych informacji oraz pomaga w ich rozprzestrzenianiu[29].

Cyberprzestrzeń jako nowe środowisko dezinformacji

W wyniku znacznego rozwoju sieci komputerowych, digitalizacji, sztucznej inteligencji oraz Internetu termin cyberprzestrzeń zyskał na znaczeniu. Stanowi on idealne podłoże dla zjawiska dezinformacji. Wykorzystując globalny zasięg, łączy pojedynczych użytkowników a zarazem organizacje międzynarodowe.

Pojęcie cyberprzestrzeni

Termin cyberprzestrzeń jest pojęciem bardzo szerokim i trudnym do zdefiniowania. Odnosi się do świata wirtualnego, innymi słowy do nośnika elektronicznego, który wykorzystywany jest do ułatwienia komunikacji. Cyberprzestrzeń najczęściej obejmuje dużą sieć komputerową składającą się z wielu podsieci komputerowych na całym świecie. Wykorzystują one protokół TCP/IP do komunikacji i wymiany danych. Podstawą funkcjonowania cyberprzestrzeni jest interaktywne i wirtualne środowisko dla szerokiego grona uczestników. Innymi słowy istotą cyberprzestrzeni jest posługiwanie się danymi i informacjami w formie cyfrowej.

Definicja encyklopedyczna ujmuje cyberprzestrzeń jako medium elektroniczne składające się z sieci komputerowych, w których komunikacja odbywa się online[30]. Odnosząc się do innych publikacji cyberprzestrzeń jest opisywana mianem przestrzeni operacyjnej. Jest to grunt, na którym działania wykonywane przez ludzi, mają zrealizować wcześniej założone cele. Natomiast ze swojej strony, powinny przynieść odpowiednie efekty nie tylko w strefie

[27] Tamże.
[28] Tamże.
[29] Tamże.
[30] https://www.ahdictionary.com/word/search.html?q=cyberspace, dostęp: 28.12.2020 r.

cyberprzestrzeni, ale także poza nią. Inaczej ujmując wiadomości bądź inne informacje, powinny wywierać wpływ na użytkowników. Decydować o zmianie jego postępowania albo nastawienia, w danej sprawie. Najważniejszym zaś elementem cyberprzestrzeni jest informacja, która powinna występować w formie zdigitalizowanej[31].

Pojęcie cyberprzestrzeni jest opisywane w wielu dokumentach, natomiast jego treść jest identyczna w większości z nich. Pierwsza kluczowa definicja została ogłoszona 25.09.2002 roku w ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych o zasadach jego podległości konstytucyjnym organom Rzeczpospolitej Polskiej. Według niej cyberprzestrzeń traktowana jest jako przestrzeń przetwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848, 1590), wraz z powiązaniami między nimi oraz relacjami z użytkownikami[32].

Następnym dokumentem jest Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2009-2011 - założenia z roku 2009, w którym cyberprzestrzeń opisywano, jako przestrzeń komunikacyjną tworzoną przez system powiązań internetowych[33].

Kolejna zmodyfikowana definicja występuje w Projekcie Rządowym Programu Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, wersja 1.1. Określa on cyberprzestrzeń, jako cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[34].

Natomiast Doktryna Cyberbezpieczeństwa RP zawiera w sobie bardziej rozwiniętą definicją zawartej w ustawie o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej. Cyberprzestrzeń opisywana jest tam jako zespoły współpracujących urządzeń informatycznych oraz oprogramowania, które zapewniają przetwarzanie, przechowywanie a także wymianę informacji[35].

[31] T. R. Aleksandrowicz, *Podstawy walki informacyjnej*, Editions Spotkania Spółka, Warszawa 2016, s. 176.
[32] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej.
[33] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf, dostęp: 28.12.2020 r.
[34] Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011 – 2016, Departament Ewidencji Państwowych i Teleinformatyki MSWiA, Warszawa 2010.
[35] Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej, BBN, Warszawa 2015.

Dodatkowo, w Strategii Cyberbezpieczeństwa Rzeczypospolitej na lata 2019-2024[36] nazywa się cyberprzestrzenią przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Dokument ten jest kontynuacją przedsięwzięć podejmowanych w przeszłości przez administrację rządową. Ma ona za zadanie podnieść poziom bezpieczeństwa pod kątem cyberprzestrzeni Rzeczypospolitej Polskiej[37].

Cyberprzestrzeń i możliwości dezinformacyjne

Pojawienie się cyberprzestrzeni oraz zaawansowanych technologii zapoczątkowało erę cyfrową. Era ta przyniosła zarówno pozytywne i negatywne konsekwencje dla wszystkich podmiotów wewnątrz i poza domeną wirtualną. Cyberprzestrzeń posiada ogromny potencjał. Poprzez ogromne zaplecze danych, stała się nieodzownie głównym źródłem informacji dla większości użytkowników. Niestety brak filtracji danych oraz ich nadmiar kreuje idealne możliwości dla całego procesu dezinformacyjnego.

Przeciwdziałanie oraz zwalczanie dezinformacji w cyberprzestrzeni

W dzisiejszych czasach coraz to więcej osób, w każdym przedziale wiekowym korzysta z ogólnie dostępnych serwisów informacyjnych oraz portali społecznościowych. Uważając je za interesujące i godne zaufania, aczkolwiek wskutek dominującego natłoku informacji, trudno zweryfikować, czy są zgodne ze stanem faktycznym. Prowadzi to niejednokrotnie do rozprzestrzeniania plotek, fałszywych wiadomości, teorii spiskowych, które są zjawiskiem niezwykle niepokojącym. Świat dążąc do prawdy zostaje zmuszony do wykreowania narzędzi oraz metod pozwalających na przeciwdziałanie procesowi dezinformacji oraz manipulacji informacją. Z powodu ogromnej skali tego zjawiska, wiele organizacji medialnych poświęca więcej czasu na weryfikację danych.

Obecnie istnieje wiele sposobów pozwalających na sprawną weryfikację dostępnych źródeł. Jednym z głównych sposobów radzenia sobie z procesem dezinformacji jest Platforma Hoaxy. Powstała ona w wyniku pracy naukowców z University Network Science Institute oraz School of Informatics and Computing's Center for Complex Network and Systems Research. Jest to stosunkowo nowym narzędziem. Służy ona do automatycznego śledzenia dezinformacji online oraz sprawdzania faktów. Jej działanie polega na odtwarzaniu sieci dyfuzji wywołanych przez wszelkie oszustwa oraz poprawki, gdyż są

[36] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024, Ministerstwo Cyfryzacji, Warszawa 2019.
[37] R. Janczewski, *Konwencja terminologiczna w cyberbezpieczeństwi*e, [w:] S. Topolewski, K. Karwacka, J. Sekuła, T. Sobczyński (red.), *Aspekty bezpieczeństwa informacyjnego w obszarze cyberprzestrzeni wymiar teoretyczny i praktyczn*y, AMW, Gdynia 2018, s. 38.

one udostępniane w sieci, a następnie rozprzestrzeniane od użytkownika do użytkownika[38].

Platforma Hoaxy stanowi ważne narzędzie do badania zjawiska dezinformacji. W wielu artykułach, poprzedzonymi badaniami, zauważalna jest zależność pomiędzy fałszywymi wiadomościami promowanymi przez niewielką liczbę aktywnych kont. Rozpowszechniają fakty, a sprawdzenie następuję kilka godzin później. W przyszłości planowane są badania, których celem będzie badanie aktywności osób rozprzestrzeniających fałszywe wiadomości, aby sprawdzić czy działania tego dokonują boty społecznościowe. Dodatkowym celem tych badań, ma być analiza opóźnienia czasowego między dezinformacją cyfrową a faktami.

Kolejnym sposobem sprawdzania wiarygodności informacji jest narzędzie portalu Facebook. Jego nazwa to CrowdTangle. Pomaga ono śledzić, analizować oraz informować, o tym, co się dzieje w mediach społecznościowych. Z użyciem tego narzędzia można porównywać oraz identyfikować historie, mierzyć wyniki społeczne. CrowdTangle wykorzystywane jest przez dziennikarzy, stacje telewizyjne, media cyfrowe, firmy rozrywkowe oraz inne organizacje w celu weryfikacji informacji każdego dnia. Jej celem jest monitorowanie mediów społecznościowych. Zapewnia wgląd w treści, jakie są udostępniane oraz w jaki sposób są udostępniane na platformach takich jak Facebook. Instagram i Reddit[39].

Następnym narzędziem umożliwiającym sprawdzania informacji jest Graphika, które pozwala na mapowanie krajobrazu mediów społecznościowych i znajdowania połączeń między domenami. Działa w sposób kompleksowy i skutecznie wizualizuje przepływ dezinformacji w formie graficznej Gephi[40].

Przydatnym narzędziem, pomagającym w dochodzeniu i sprawdzaniu dezinformacji oraz przestępstw związanych w finansami są DNSlytics.com oraz Adbet. Pierwsze ułatwia poszukiwania reklam oraz podejrzanych działań komercyjnych, zauważalnych na stronach internetowych. Drugie natomiast skanuje sieć oraz zbiera przydatne informacje dotyczące reklam displayowych[41].

Następnym narzędziem jest Whopostedwhat. Opracowany przez specjalistę do spraw wywiadu internetowego Henka van Ess. Służy do badania spraw wagi publicznej. Łącząc owe narzędzie z narzędziami portalu Facebooka, pozwala weryfikować słowa kluczowe z podziałem na daty. Pomaga to na znalezienie osób odpowiedzialnych za wprowadzanie w obieg błędów w opublikowanych postach.

[38] https://cnets.indiana.edu/blog/2016/12/21/hoaxy/, dostęp: 11.11.2021 r.
[39] https://www.crowdtangle.com/, dostęp: 15.11.2020 r.
[40] https://www.graphika.com/posts/deep-learning-at-graphika-scaling-network-maps-with-heterogeneous-graph-embedding/, dostęp: 17.11.2020 r.
[41] reklama displayowa - pozwala firmom dotrzeć z przekazem do określonych grup użytkowników w wybranych witrynach internetowych.

Ostatnim, ale bardzo skutecznym i znanym narzędziem jest wyszukiwarka Google. Za pomocą wpisywania nawet części zdań możemy znaleźć artykuły, książki, posty, które zawierają dalszą cześć zdania.

Działalność dezinformacyjna federacji rosyjskiej w cyberprzestrzeni

Zjawisko dezinformacji w Rosji nie jest niczym nowym i stanowi największe zagrożenie na arenie geopolitycznej. Jej podstawę stanowi strategia, która ma jeden priorytetowy cel, jakim jest osłabienie państw zachodnich, a wzmocnienie Rosji. Kraj ten posiada zasoby oraz zespoły specjalistów zajmujących się, badaniem ruchu w sieci, a ruch ten jest stale monitorowany pod każdym względem.

Państwo to używa wszelakich narzędzi, które osiągają skuteczność w sposób intensywny. Zauważalna propaganda i dezinformacja odciskają wpływ na opinię publiczną na temat krajów zachodnich. Wiele państw prowadzących rozpoznanie, dostrzegło zależność w rosyjskiej dezinformacji. Skupia się ona w szczególności na rozprzestrzenianiu strachu, nienawiści poprzez publikowanie stworzonych przez nich samych teorii spiskowych w kierunku państw Europy oraz Stanów Zjednoczonych[42]. Kraj ten należy do jednego z czołowych i wykwalifikowanych państw dostarczających największą ilość fałszywych informacji i kłamstw.

Osoby znajdujące się przy władzy, posiadają rozległą sieć trolli internetowych oraz botów, które generują oraz rozprzestrzeniają różnego rodzaju treści w Internecie. Ich działania są wspierane oraz popierane przez dyplomatów, kontrolowane przez media państwowe czego przykładem jest Russia Today. Dodatkowo państwo wspierane jest przez WikiLeaks. Ich współpraca polega na tworzeniu nieprawdziwych historii i dotarciu do jak największej bazy użytkowników.

Dezinformacja jest jednym z głównych i najbardziej atrakcyjnych narzędzi wykorzystywanych przez Federację Rosyjską, ponieważ, posiada kilka atutów, do których należą:

- zasięg – szeroki transgraniczny zasięg;
- koszty - stosunkowo niskie koszty;
- anonimowość – najwyższa technologia oraz nowoczesne metody i techniki pozwalają zagwarantować anonimowość osobom biorącym udział w procesie dezinformacyjnym;
- zadania – pozwalają realizować wyznaczone cele polityki Federacji Rosyjskiej.

Zarys sytuacji na gruncie dezinformacji Federacji Rosyjskiej

[42] https://eufactcheck.eu/blogpost/blog-why-and-how-russian-disinformation-targets-europe-and-the-eu-in-georgia/, dostęp: 05.11.2020 r.

Obecna sytuacja Federacji Rosyjskiej, przedstawia dominującą kontrolę nad tradycyjnymi mediami przez prezydenta Władimira Putina. Całkowita dominacja mediów a przede wszystkim telewizji, radia i gazet, wpływa na relacje pomiędzy władzą w państwie a jego obywatelami. Rząd Federacji Rosyjskiej traktuje cyberprzestrzeń jako bezpieczeństwo informacji i zalicza się ona do integralnych części bezpieczeństwa narodowego państwa. Do przykładowych dokumentów należą w szczególności:

1. Doktryna wojenna Federacji Rosyjskiej z 2014 roku (Военная доктрина Российской Федерации).
2. Strategia Bezpieczeństwa Federacji Rosyjskiej z 2015 roku (Стратегия национальной безопасности Российской Федерации).
3. Doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej z 2016 roku (Доктрина информационной безопасности Российской Федерации).
4. Strategia rozwoju społeczeństwa informacyjnego w Federacji Rosyjskiej na lata 2017-2030 (О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы).

Te cztery podstawowe dokumenty określają priorytety bezpieczeństwa informacji oraz skupiają się na identyfikacji głównych zagrożeń, a także sposobów przeciwdziałania im. Dodatkowym dokumentem jest Konstytucja Federacji Rosyjskiej, która zawiera gwarancje wolności słowa oraz aspekty dotyczące dokładności przekazywania informacji. Są one regulowane przez przepisy federalne, jak Ustawa o mediach masowego przekazu i Ustawa o podstawowych gwarancjach głosu[43]. Wymienione dokumenty opisują ważność środowiska informatycznego, a także podkreślają stosowanie strategii oraz sił i środków w celu zapewnienia bezpieczeństwa. W wysokiej mierze skupiają się na terminologii oraz ważności zagadnienia bezpieczeństwa informatycznego jak i obowiązku podejmowania działań aktywnych w tym obszarze. Wymienione są w nich, zagrożenia, jakie mogą przynieść inne państwa, w zakresie technologii informatycznych oraz komunikacyjnych.

Agresywna taktyka, jaką wykorzystuje rosyjski rząd wpływa na silny wpływ kampanii trolli, które manipulują opinią publiczną, wskutek, czego uciszani są obywatele. Używa się w tym celu trollingu, hakowania oraz innych technik. Federacja Rosyjska publikuje informacje, które są przeznaczone do obywateli kraju oraz reszty państw. Kampanie mają zróżnicowane cele taktyczne w zależności od odbiorców i wykorzystują w tym działaniu różnego rodzaju kanały. Niestety liczba dróg oraz osób ją tworzących jest nieznana, ponieważ część z nich działa w środowisku niepublicznym, bądź wykorzystuje bezpośrednie platformy komunikacyjne oraz kontakty między ludźmi.

[43] https://www.loc.gov/law/help/social-media-disinformation/russia.php, dostęp: 05.11.2020 r.

Cele działań dezinformacyjnych Federacji Rosyjskiej w polityce zagranicznej

Mocarstwo, jakim jest Federacja Rosyjska od zawsze miało oraz ma jasno określone dalekosiężne cele i dąży do ich realizacji. Każde państwo stara się zająć najwyższą pozycję na arenie międzynarodowej, w trakcie wszelkiego rodzaju porozumień czy umów. Rosja nie jest wyjątkiem.

Punktem wyjściowym przy zawieraniu wielu układów, kontraktów jest to jak dane kraje są postrzegane. Jeżeli jakiś kraj jest uważany przez inne kraje, jako taki, który np. łamie prawa człowieka lub też z innych powodów są nałożone na niego sankcje, posiada przegraną pozycję podczas negocjacji. Nawet, jeżeli ma silne argumenty ekonomiczne będą one osłabione. W oczywisty sposób doprowadza to zawierania transakcji na gorszych warunkach niż mogłyby być wynegocjowane w innej sytuacji. Wywołuje to reakcję łańcuchową. Rząd, który doprowadził do sytuacji znaczącego osłabienie swojego państwa na arenie międzynarodowej, przestaje być wiarygodny w oczach wyborców. Bierze się to np. z wyższych cen towarów importowych, wydłużonym czasem oczekiwania na granicy itp.

Każda władza chce utrzymać swoją silną pozycję na arenie międzynarodowej jak najdłużej. Z tego powodu stara się nie dopuszczać do sytuacji, w której mogłaby być osłabiona. Rosja jest w trudnej sytuacji, ponieważ rząd sprawuje jedna partia prowadzona przez tego samego człowieka od wielu lat. Wiele krajów na świecie uważa Rosję jako kraj, w którym demokracja jest „nadwyrężona". Można regularnie przeczytać w wiadomościach, że niektórzy mieszkańcy tego kraju uważają, że wybory są fałszowane. Jednakże zdarzają się wyjątki, które twierdzą, że w Federacji Rosyjskiej panuje ustrój autorytarny i pogwałcane są niektóre prawa człowieka. Te wszystkie oskarżenia i wiele innych są bardzo poważne, a władza nie może sobie pozwolić na takie zachwianie w fundamentach pozycji na arenie międzynarodowej.

Odpowiedzią na tą sytuację ze strony Kremla jest szeroko pojęta akcja dezinformacyjna. W pierwszej kolejności była ona wymierzona w samych obywatelach. Miało to na celu zwiększenie szans na wygranie wyborów i umocnienie pozycji politycznej w państwie. Sposobem na osiągnięcie tego celu, jest wykreowanie społeczeństwa, które nie potrafi odseparować faktów od manipulacji. W wyniku, czego działania rządu są w znaczącym stopniu wyrafinowane. To jednak jest zdecydowanie za mało i nic nie zmienia w kontaktach z innymi państwami. Prezydent Vladimir Putin zauważył, że Internet i media społecznościowe ułatwiają dostęp do światowej publiki. Umożliwia to wpływanie na polityczne poglądy mieszkańców wielu części świata w jednym czasie. W ten sposób Rosja posunęła się dalej, przekraczając tradycyjne sposoby pozyskiwania wpływów. Wielu polityków Unii Europejskiej widzi w tym zagrożenie dla zachodniej demokracji i społecznego porządku[44].

[44] https://rcb.gov.pl/dezinformacja-rosyjska-bron-strategiczna/, dostęp: 05.01.2021 r.

Celem tych ataków jest osłabienie Unii Europejskiej poprzez poróżnienie jej członków. Dzięki tego typu przedsięwzięciom Rosyjski rząd nakierowuje i po części wymusza podejmowania wewnętrznych decyzji w Unii Europejskiej na swoją korzyść. Jednym z takich przykładów jest uniknięcie lub też zmniejszenie do minimum sankcji nałożonych przez kraje członkowskie na Rosję za aneksję Krymu i agresję przeciwko Ukrainie.

W większości przypadków fałszywe informacje, które są wypuszczane przez Rosję na Unię Europejską, Stany Zjednoczone czy inne państwa, są silnym narzędziem podważającym ich integralność. Rosjanie starają się zawsze poruszać najbardziej newralgiczne tematy w danym kraju, regionie, grupie społecznej. Zasianie ziarna niepewności wśród społeczeństwa bardzo często wystarczy, aby wzmocnić pozycję na arenie międzynarodowej. Niejednokrotnie kreowane wiadomości przedstawiają wartości krajów zachodnich jako słabe, złe i zdemoralizowane, niszczące pewne tradycyjne wartości. Powoduje to, że wielu ludzi się zastanawia czy nie potrzeba silnego rządu z jednym silnym przywódcą tak jak w Federacji Rosyjskiej. Wszystkie tego typu działania mają na celu przechylenie szali zwycięstwa. Działania i pojedyncze cele, jakie mają być osiągnięte w danej chwili są bardzo różne, ale każdy prowadzi do jednego - wzmocnienia pozycji Federacji Rosyjskiej na świecie, jako mocarstwa i kreowanie panującego rządu, jako silnego, zdecydowanego bronić interesów i wartości, które uznają obywatele Rosji w taki sposób, aby ich pozycja była pewna i bezpieczna do następnych wyborów.

Zagrożenia związane z dezinformacją Federacji Rosyjskiej na arenie międzynarodowej

Analizując zjawisko dezinformacji prowadzonej przez Federację Rosyjską na arenie międzynarodowej należy podkreślić jej istnienie. Świadomość ta posiadana jest przez wiele państw Unii Europejskiej jak i członków NATO. Wszystkie kraje, borykają się z wpływem dezinformacji, propagandy i szerzenia fałszywych informacji. Działania podejmowane przez Rosję, wypływają na tworzenie wrogich narracji i negatywnych wizerunków państw, a także ich społeczeństw. Wielokrotnie zjawisku temu towarzyszy lęk oraz poczucie zagrożenia. Stale towarzyszące poczucie strachu, może doprowadzić do zaburzenia porządku publicznego i narodowego oraz przynieść ryzyko dla interesów międzynarodowych[45].

Kluczowym zagrożeniem dla państw na arenie międzynarodowej jest znikoma wiedza na temat silnego kraju, jakim jest Rosja. Mała wiedza na temat ich zaplecza technologicznego oraz specjalistów, uniemożliwia zobrazowanie jego przewagi. Federacja Rosyjska wprowadza utrudnienia, które zmniejszają możliwość rozpoznania zagrożenia. Przykładem jest wprowadzenie wiz, które

[45] https://capd.pl/pl/raporty/198-rosyjska-wojna-dezinformacyjna-przeciwko-polsce, dostęp: 14.01.2021 r.

są konieczne, aby przemieścić się na terytorium państwa. Dodatkowo całodobowa kontrola oraz monitorowanie ruchów sieciowych także uniemożliwiają działania rozpoznawcze.

Obecnie sytuacja oraz waga tego problemu zmusiła członków Unii Europejskiej oraz do podjęcia kroków w celu przeciwdziałania i rozpoznawania dezinformacji Federacji Rosyjskiej. Czynnikiem decydującym był fakt, że takie działania mogą mieć fizyczne odzwierciedlenie w wielu aspektach życia. Z punktu widzenia państw są to bardzo poważne zagrożenia, ponieważ mogą doprowadzić do utraty poparcia rządów, pogorszenia stosunków międzynarodowych a nawet przynieść taki efekt, który w fizyczny sposób odczują mieszkańcy. Zagrożenia te związane są między innymi z destabilizacją bezpieczeństwa w wymiarze narodowym jak i społecznym. W ramach zminimalizowania zagrożenia Unia Europejska utworzyła komórkę zajmującą się analizą zjawiska dezinformacji EUvsDisinfo.

Wnioski

Intensywny rozwój społeczeństwa, technologii informacyjnej oraz potencjału sprzętowego znacząco spowodował, że informacja jest nieodzownie istotnym elementem współczesnego społeczeństwa. Odgrywa ważną rolę w funkcjonowaniu poszczególnej jednostki, ale także jest ważna dla podmiotów państwowych. Stanowi element zapewniający bezproblemową komunikację. Tak duże znaczenie posiadania informacji, doprowadziło do rywalizacji pomiędzy krajami na arenie międzynarodowej. Wzmożone i właściwe wykorzystanie treści informacji służy kreowaniu postaw oraz osiąganiu oczekiwanych zachowań. Pomimo pozytywnych aspektów, przyczynia się wielokrotnie do zjawisk niekorzystnych. Takim zjawiskiem jest dezinformacja. Zauważalna niemalże w każdym aspekcie naszego życia. Jej nasilona aktywność obserwowana jest na przestrzeni lat. Towarzyszący jej zakres dostępnych technik oraz narzędzi, umożliwił anonimowe i błyskawiczne rozprzestrzenianie się spreparowanych oraz zmanipulowanych wiadomości. Dezinformacja jest bardzo popularnym narzędziem stosowanym przez podmioty państwowe jak i pozapaństwowe. Dezinformacja jest formą manipulacji, kontrolowania a nawet sterowania jednostkami.

Głównym środowiskiem, rozprzestrzeniania się dezinformacji oraz miejscem, które zapewnia największy wachlarz możliwości wykorzystania narzędzi dezinformacyjnych, jest cyberprzestrzeń. Stanowi ona przestrzeń przetwarzania oraz wymiany informacji tworzonej przez systemy teleinformatyczne.

Głównym celem niniejszego artykułu było opisanie postępującej dezinformacji, prowadzonej przez państwo wiodące prym w tym zakresie, jakim jest Federacja Rosyjska. Doskonałe wyszkolenie specjalistów z zakresu informatyki i cybernetyki oraz dostęp do najnowszych technik czy metod, poważnie wpływa na zaburzenie funkcjonowania reszty podmiotów. Założony Dezinfor-

macja jest elementem kluczowym, w procesie zaburzania porządku w dziedzinie bezpieczeństwa, a także w zakresie polityki czy gospodarki. Posiada ona znaczny potencjał, gdyż ewidentnie potrafi wywierać wpływ na pojedyncze jednostki, a także większe społeczności, budując stan lęku i niepokoju.

Metodologia

Głównym celem niniejszej pracy było opisanie postępującej dezinformacji, prowadzonej przez Federację Rosyjską. Praca została napisana na podstawie analizy i krytyki piśmiennictwa (publikacji zwartych, artykułów naukowych oraz rzetelnych stron internetowych). W czasie badań posłużono się również metodami takimi jak synteza i wnioskowanie.

Przegląd literatury

W artykule wykorzystano szereg ogólnie dostępnych materiałów źródłowych, z których najważniejsze pozycje literatury obejmowały przede wszystkim *Podstawy walki informacyjnej* Tomasza Aleksandrowicza, *Zarządzanie informacją w cyberprzestrzeni* Jacka Unolda, *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego* Andrzeja Żebrowskiego oraz *Rosyjska cyberstrategia* Yannicka Harrela. *Podstawy walki informacyjnej* Tomasza Aleksandrowicza przedstawia znaczenia zmian środowisk bezpieczeństwa, a także informacji jako zasobów strategicznych oraz bezpieczeństwa informacyjnego.

Z*arządzanie informacją w cyberprzestrzeni* Jacka Unolda. Szeroko opisuje problematykę z zakresu informacji w przestrzeni cyfrowej.

Rosyjska cyberstrategia Yannicka Harrela zawiera opis wykorzystywanych przez Federację Rosyjską środków nacisku politycznego oraz militarnego.

W pracy wykorzystano również artykuły dostępne w Internecie, które opisywały zjawisko dezinformacji, technik oraz narzędzi wykorzystywanych w powyższym artykule.

Wnioski

Intensywny rozwój społeczeństwa, technologii informacyjnej oraz potencjału sprzętowego znacząco spowodował, że informacja jest nieodzownie istotnym elementem współczesnego społeczeństwa. Odgrywa ważną rolę w funkcjonowaniu poszczególnej jednostki, ale także jest ważna dla podmiotów państwowych. Stanowi element zapewniający bezproblemową komunikację. Tak duże znaczenie posiadania informacji, doprowadziło do rywalizacji pomiędzy krajami na arenie międzynarodowej. Wzmożone i właściwe wykorzystanie treści informacji służy kreowaniu postaw oraz osiąganiu oczekiwanych zachowań. Pomimo pozytywnych aspektów, przyczynia się wielokrotnie do zjawisk niekorzystnych. Takim zjawiskiem jest dezinformacja. Zauważalna

niemalże w każdym aspekcie naszego życia. Jej nasilona aktywność obserwowana jest na przestrzeni lat. Towarzyszący jej zakres dostępnych technik oraz narzędzi, umożliwił anonimowe i błyskawiczne rozprzestrzenianie się spreparowanych oraz zmanipulowanych wiadomości. Dezinformacja jest bardzo popularnym narzędziem stosowanym przez podmioty państwowe jak i pozapaństwowe. Dezinformacja jest formą manipulacji, kontrolowania a nawet sterowania jednostkami.

Głównym środowiskiem, rozprzestrzeniania się dezinformacji oraz miejscem, które zapewnia największy wachlarz możliwości wykorzystania narzędzi dezinformacyjnych, jest cyberprzestrzeń. Stanowi ona przestrzeń przetwarzania oraz wymiany informacji tworzonej przez systemy teleinformatyczne.

Głównym celem niniejszego artykułu było opisanie postępującej dezinformacji, prowadzonej przez państwo wiodące prym w tym zakresie, jakim jest Federacja Rosyjska. Doskonałe wyszkolenie specjalistów z zakresu informatyki i cybernetyki oraz dostęp do najnowszych technik czy metod, poważnie wpływa na zaburzenie funkcjonowania reszty podmiotów. Założony Dezinformacja jest elementem kluczowym, w procesie zaburzania porządku w dziedzinie bezpieczeństwa, a także w zakresie polityki czy gospodarki. Posiada ona znaczny potencjał, gdyż ewidentnie potrafi wywierać wpływ na pojedyncze jednostki, a także większe społeczności, budując stan lęku i niepokoju.

Bibliografia

Opracowania zwarte

1. Aleksandrowicz T. R., *Podstawy walki informacyjnej*, Editions Spotkania Spółka, Warszawa 2016.
2. Dela P., *Teoria walki w cyberprzestrzeni*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2020.
3. Epstein E. J., *Podstęp. Niewidzialna wojna między KGB a CIA*, Scripta Manent, Krosno 1993.
4. Lewandowski H., *Podstęp, inspiracja i dezinformacja w działalności służb specjalnych*, UOP, Warszawa 2000.
5. Polmar, N. Allen T. B., *Księga szpiegów. Encyklopedia*, Magnum, Warszawa 2000.
6. Volkoff V., *Dezinformacja – oręż wojny*, Wydawnictwo Antyk Marcin Dybowski, Komorów 1991.
7. Wojciechowski K. (tłum.), *Encyklopedia szpiegostwa*, Oficyna Wydawnicza Spar, Warszawa 1995.
8. Żebrowski A., *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2016.

Artykuły

1. T. Grabowski, *Metody walki informacyjnej w mediach elektronicznych na przykładzie konfliktu rosyjsko-ukraińskiego (2014-2016)*, Horyzonty Polityki, 7(20)/2016.
2. Janczewski R., *Konwencja terminologiczna w cyberbezpieczeństwi*e, [w:] S. Topolewski, K. Karwacka, J. Sekuła, T. Sobczyński (red.), *Aspekty bezpieczeństwa informacyjnego w obszarze cyberprzestrzeni wymiar teoretyczny i praktyczn*y, AMW, Gdynia 2018.
3. Świerczek M., *System matrioszek, czyli dezinformacja doskonała. Wstęp do zagadnienia,* „Przegląd Bezpieczeństwa Wewnętrznego", nr 10(19)/2018.
4. Wachowicz M. J., *Ujęcie teoretyczne pojęcia dezinformacji,* „Wiedza Obronna", nr 1-2/2019.
5. Oleksiewicz I., *Bezpieczeństwo informacyjne w cyberprzestrzeni a stany nadzwyczajne*, „Zarządzanie", nr 33/2019.

Dokumenty normatywne

1. *Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej.*
2. *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016 – założenia.*
3. *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011 – 2016*, Departament Ewidencji Państwowych i Teleinformatyki MSWiA, Warszawa 2010.
4. *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019 – 2024*, Ministerstwo Cyfryzacji, Warszawa 2019.
5. *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, BBN, Warszawa 2015.

Źródła internetowe

1. https://capd.pl/pl/raporty/198-rosyjska-wojna-dezinformacyjna-przeciwko-polsce
2. https://eufactcheck.eu/blogpost/blog-why-and-how-russian-disinformation-targets-europe-and-the-eu-in-georgia/
3. https://guides.lib.uw.edu/c.php?g=345925&p=7772376
4. https://mfiles.pl/pl/index.php/Jakość_informacji
5. https://pism.pl/publikacje/Dezinformacja_Chin_i_Rosji_w_trakcie_pandemii_COVID19?fbclid=IwAR3yLwliAZjsELGfS-0oes4dzawacwnUX11TEsWHRz-1P38jEFV6EJjFtPA
6. https://sjp.pwn.pl/sjp/dezinformacja;2554971.html

7. https://www.bankier.pl/wiadomosc/Kreml-probowal-sklocic-Portugalie-i-USA-ws-bazy-wojskowej-7702500.html
8. https://www.bpb.de/gesellschaft/medien-und-sport/bilder-in-geschichte-und-politik/73234/manipulation-und-propaganda?p=2
9. https://www.crowdtangle.com/
10. https://www.cybersecurity-insiders.com/huawei-5g-network-data-espionage-scandal-reignites/
11. https://www.loc.gov/law/help/social-media-disinformation/russia.php
12. https://www.ahdictionary.com/word/search.html?q=cyberspace, dostęp: 28.12.2020 r.
13. https://cnets.indiana.edu/blog/2016/12/21/hoaxy/
14. https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance
15. https://www.brookings.edu/blog/brookings-now/2018/10/03/what-do-russian-disinformation-campaigns-look-like-and-how-can-we-protect-our-elections/
16. https://www.hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf, dostęp: 12.01.2021 r.

bsmt pchor. Kacper PIRCH

SOCJOTECHNIKA JAKO CYBERZAGROŻENIE

Streszczenie

Era informacji oraz gwałtowny techniczny i technologiczny rozwój powoduje kształtowanie się zagrożeń, które występują w całkowicie stworzonej przez człowieka przestrzeni – cyberprzestrzeni. Socjotechnika została zaadaptowana przez cyberprzestępców i jako najczęściej znajduje zastosowania w przestępczej działalności wrogich podmiotów. Cyberprzestrzeń, której charakterystycznymi cechami jest brak fizycznych granic, zdecentralizowana struktura oraz ogólnoświatowy zasięg zapewnia jej użytkownikom anonimowość, która dodatkowo motywuje przestępców do przeprowadzania ataków i wykradania danych wrażliwych głównie w celu osiągnięcia korzyści majątkowych. Wykorzystywana inżynieria społeczna służy atakującym do przełamywania nawet najtrudniejszych zabezpieczeń poprzez podszywanie się pod inne osoby lub instytucje, wskutek czego przekazane im informacje (często bez wiedzy swojej ofiary) doprowadzają do kradzieży danych poufnych.

Słowa kluczowe:
cyberprzestrzeń, cyberzagrożenia, socjotechnika, Internet, cyberbezpieczeństwo.

Abstract

The information age and rapid technical and technological development are shaping threats that occur in a completely man-made space - cyberspace. Social engineering has been adopted by cybercriminals and is most often used in the criminal activities of hostile entities. Cyberspace, whose characteristic features are the lack of physical boundaries, decentralized structure, and global reach, provides its users with anonymity, which additionally motivates criminals to carry out attacks and stealing sensitive data, mainly to gain financial benefits. The social engineering is used by attackers to break even the most difficult security measures by impersonating other people or institutions, because of which the information provided to them (often without the victim's knowledge) leads to the theft of confidential data.

Keywords:
cyberspace, cyber threats, social engineering, Internet, cyber security.

.

Wstęp

Żyjąc w erze informacji i będąc naocznymi świadkami gwałtownego technicznego
i technologicznego rozwoju można zaobserwować, że korzystając z Internetu, poza zwiększeniem komfortu i ułatwienia życia codziennego, można napotkać wiele nowych zagrożeń w nieznanej dotychczas, całkowicie stworzonej przez człowieka przestrzeni – cyberprzestrzeni. Jednym z zagrożeń jest socjotechnika. Została ona bardzo szybko zaadaptowana przez przestępców i znalazła zastosowanie w działalności przestępczej wrogich podmiotów. W procesie twórczym niniejszego artykułu wykorzystano dostępną literaturę, artykuły oraz źródła internetowe w celu szczegółowego przeprowadzenia analizy. Wykorzystane zostały m.in. następujące pozycje literatury:

- „Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru" – Maciej Marczyk;
- „Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw" – Miron Lakomy;
- „Cyberprzestrzeń – część teatru działań hybrydowych" – Robert Janczewski.

Cyberprzestrzeń - charakterystyka

Cyberprzestrzeń jest przestrzenią całkowicie wykreowaną i wprowadzoną do życia przez człowieka, opierająca się na Internecie, który początkowo wykorzystywany miał być wyłącznie przez struktury wojskowe jako sposób przekazywania informacji, który nie wymagał dużego zapotrzebowania zasobów. Głównymi cechami charakterystycznymi cyberprzestrzeni jest brak fizycznych granic, zdecentralizowana struktura oraz globalny zasięg. Dodatkowo rozważając pojęcie cyberprzestrzeni należy ująć anonimowość, którą użytkownicy cyberprzestrzeni mogą względnie zachować[1].

Definicje cyberprzestrzeni

Pierwszy opis cyberprzestrzeni pojawił się w latach 80. XX wieku w literaturze gatunku science-fiction, która miała zobrazować nadchodzącą rewolucję w dziedzinie informatyki. Do rozpowszechnienia i spopularyzowania terminu cyberprzestrzeń przyczynił się William Gibson, który w jednej ze swoich powieści opisał ją jako „konsensualna halucynacja, doświadczana każdego dnia przez miliardy uprawionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych… Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność…"[2].

[1] M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru,* „Przegląd teleinformatyczny" nr 1-2/2018, s. 59.
[2] W. Gibson, *Neuromancer,* Wydawnictwo Kameleon, Radom 1999, s. 43.

Koncepcja cyberprzestrzeni, początkowo nienaukowa i dodatkowo stworzona na potrzeby wykreowania świata literackiego została następnie uznana za przydatną i użytą do zdefiniowania przestrzeni stworzonej przez sieci komputerowe[3].

Według Józefa Bednarka, można określić pięć głównych funkcji cyberprzestrzeni:

- informacyjna;
- rozrywkowo-relaksacyjna (ludyczna);
- stymulująca;
- wzorcotwórcza;
- interpersonalna[4].

Pierwsza z wyżej wymienionych funkcji określa cyberprzestrzeń jako przestrzeń,
w której nieprzerwanie zachodzi proces wymiany informacji. Umożliwia ona użytkownikowi pozyskiwanie dowolnego rodzaju informacji w zależności od personalnych potrzeb. Druga funkcja cyberprzestrzeni określona przez Józefa Bednarka pozwala nam zaobserwować, że stanowi dla człowieka ważny aspekt w codziennym życiu, ponieważ używana jest celach rozrywkowych z innymi użytkownikami cyberprzestrzeni. „Funkcja stymulująca wyraża się w inspiracji odbiorców do aktywnego odbioru treści znajdujących się w cyberprzestrzeni”[5]. Pomaga ona odnaleźć w cyberprzestrzeni różnego rodzaju funkcje edukacyjne, które umożliwić mogą odbiorcy obranie prawidłowej drogi samorealizacji
i kształcenia. Kolejna z funkcji polega na ukazywaniu wzorów postępowania oraz zachowań, a także obrazowanie osobistości, które charakteryzują się osiągnięciami wszelakich dziedzin nauki, techniki i sztuki. Ostatnia z funkcji (interpersonalna), wynikająca z globalizacji oraz powszechnego dostępu do Internetu, pozwala człowiekowi na samookreśleniu się w życiu poprzez możliwość poznania warunków życia i funkcjonowania ludzi z najdalszych zakątków planety.

Definicja cyberprzestrzeni z powodu nieustępliwego technicznego i technologicznego postępu jest bardzo trudna do ustalenia, ponieważ z dnia na dzień cyberprzestrzeń zaliczana jest do coraz to kolejnych płaszczyzn. Cyberprzestrzeń, która wykształciła się razem z powstaniem sieci komputerowych, nie jest tożsama z Internetem. Środowisko to jest bardziej złożone dzięki wyjątkowym cechom technicznym, które determinują rosnące znaczenie dla życia społecznego i politycznego[6].

[3] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015, s. 73.
[4] J. Lizut, *Zagrożenia cyberprzestrzeni kompleksowy program dla pracowników służb społecznych,* Wydawnictwo Wyższej Szkoły Pedagogicznej im. Janusza Korczaka, Warszawa 2014, s.20.
[5] M. Marczyk, *Cyberprzestrzeń…*, dz. cyt., s. 59.
[6] M. Lakomy, *Cyberprzestrzeń…*, dz. cyt., s. 70.

Tomasz Szubrycht w 2005 roku zdefiniował cyberprzestrzeń jako komunikacyjną przestrzeń, która tworzona jest przez system powiązań internetowych obejmujące systemy komunikacji elektronicznej przesyłające dane ze źródeł numerycznych[7].

Według dokumentu Joint Publication 3-12, cyberprzestrzeń to ogólnoświatowa struktura w środowisku informacyjnym składająca się z współzależnych sieci infrastruktur technologii informacyjnej oraz przechowywania danych, w tym Internet, sieci telekomunikacyjne, systemy komputerowe i wbudowane procesory[8] (tłum. autora).

Cyberprzestrzeń stała się także obszarem, w którym przeprowadzane są działania wojskowe. Zatem poza fizycznymi wymiarami poza lądem, morzem, powietrzem i przestrzenią kosmiczną cyberprzestrzeń stała się polem walki, całkowicie stworzonym przez człowieka[9]. W ostatnim czasie zauważalne niezgodność oraz różnice w punktach widzenia autorów, którzy podejmują się opisu cyberprzestrzeni oraz rozpowszechnienie słów, zaczynających się przedrostkiem „cyber-", których definicje nie zostały naukowo potwierdzone. Używanie nieprawidłowych definicji uniemożliwia określenie możliwych do zrealizowania celów oraz stworzenie prawidłowo funkcjonujących systemów[10].

W ustawie z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej przez cyberprzestrzeń „rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[11]".

W Rządowym programie ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia z 2009 roku zdefiniowano cyberprzestrzeń jako przestrzeń komunikacyjna tworzona przez system powiązań internetowych. W 2010 roku w kierowanym do uzgodnień resortowych Projekcie Rządowego programu ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016 cyberprzestrzeń nazwano cyfrową przestrzenią przetwarzania i wymiany informacji

[7] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*. „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 1/2005.
[8] Joint Publication 3-12, *Cyberspace Operations.*
[9] R. Janczewski, G. Pilarski, M. Marczyk, *Terminology as a barrier to NATO's interoperability in cyberspace operations*, "International Conference Knowlegde-Based Organization", nr 25(3)/2019.
[10] K. Liderman, *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, s. 60.
[11] *Dz. U. 2002 Nr 156 Poz. 1301. Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej*.

tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[12]. W Polityce ochrony cyberprzestrzeni Rzeczypospolitej Polskiej z 2013 roku cyberprzestrzeń zdefiniowano jako przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami; zgodnie z art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. Nr 156, poz. 1301, z późn. zm.), art.. 2 ust. 1a ustawy z dnia 21 czerwca 2002 r. o stanie wyjątkowym (Dz. U. Nr 113, poz. 98, z późn. zm.) oraz art. 3 ust. 1 pkt 4 ustawy z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. Nr 62, poz. 558, z późn. zm.)[13].

Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej z 2015 roku określa cyberprzestrzeń jako „przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami[14]".

W aspekcie definicji cyberprzestrzeni kluczowe jest pojęcie Internetu, czyli ogólnoświatowej sieci komputerowej, która zapewnia bezgraniczną swobodę wymiany informacji za pomocą protokołów informacyjnych. Internet złożony jest z połączonych ze sobą systemów teleinformatycznych, które są w stanie przetworzyć informację w formie elektronicznej. Elementami, które charakteryzują Internet są:

- nieograniczony dostęp do danych i informacji;
- komunikacja z innymi użytkownika w czasie rzeczywistym;
- powszechny i łatwy sposób uzyskania dostępu do globalnej sieci, dla społeczeństwa może to być najważniejszy aspekt Internetu, ponieważ stał się nierozłącznym towarzyszem w życiu codziennym znacznej części ludzkości;
- ekonomiczny charakter, który określa Internet jako jeden z najtańszych środków przetwarzania informacji[15].

[12] *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016,* Departament Ewidencji Państwowych i Teleinformatyki MSWiA, Warszawa 2010.
[13] *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej,* Ministerstwo Administracji i Cyfryzacji, Warszawa 2013.
[14] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej,* Warszawa 2015.
[15] M. Marczyk, *Cyberprzestrzeń…*, dz. cyt., s.59.

Według Mirona Lakomego cyberprzestrzeń jest ujmowana jako kategoria zbiorcza opisująca domenę funkcjonującą na podstawie jasno określonych elementów infrastruktury teleinformatycznej. W związku z dynamicznym technicznym i technologicznym rozwojem społeczeństw wykształciła się cyberprzestrzeń – niematerialna (niemożliwa do zmierzenia), aterytorialna (nieograniczona fizyczne granice) i zdecentralizowana sfera działalności człowieka[16]. Cyberprzestrzeń zależna jest od infrastruktury teleinformatycznej, z której jest zbudowana, czyli od sieci komputerowych i innych systemów teleinformatycznych[17].

Struktura cyberprzestrzeni

Struktura cyberprzestrzeni opiera się m.in. o połączone ze sobą sieci, spośród których możemy wyróżnić sieci teleinformatyczne, komputerowe oraz telekomunikacyjne. Sieci teleinformatyczne składają się ze współpracujących urządzeń informatycznych oraz oprogramowania, dzięki którym są w stanie spełniać takie warunki jak:

- wysyłanie i odbieranie danych;
- zapewnienie przechowywania i przetwarzania informacji.

System teleinformatyczny można podzielić na pięć elementów składowych:

- przetwarzana, przechowywana oraz przesyłana informacja;
- urządzenia umożliwiające wyżej wspomniane działanie, do których możemy zaliczyć przede wszystkim komputery oraz wszelkiego rodzaju nośniki i łącza transmisji danych, routery itp.;
- oprogramowanie (systemy operacyjne i inne elementy programowe), aplikacje umożliwiające korzystanie i kontrolowanie;
- szeroko pojęta infrastruktura, do której zaliczyć można budynki, zasilanie, systemy ochrony fizycznej (np. system przepustkowy);
- operatorów korzystających z systemów, administratorów i inny personel[18].

Cyberprzestrzeń oparta jest o rdzeń jakim jest Internet, którego działanie oparte jest o takie urządzenia jak routery, czyli urządzenia trasujące, które odpowiedzialne są za przesyłanie informacji pomiędzy komunikującymi się komputerami. Zadaniem routera jest skierowanie pakietu danych, która umożliwi jego jak najszybsze dostarczenie.

Internet, pomimo swojej różnorodności infrastrukturalnej, jest w stanie funkcjonować jako zgodny system komunikacyjny dzięki protokołom komunikacyjnym jakim jest stos protokołów TCP/IP[19], które umożliwiają połączenie się komputerów za pośrednictwem sieci. Protokoły te przeznaczone są

[16] M. Lakomy, *Cyberprzestrzeń…*, dz. cyt., s. 77.
[17] Tamże, s. 77.
[18] Liderman K., *Bezpieczeństwo…*, dz. cyt., s. 30.
[19] M. Lakomy, *Cyberprzestrzeń…*, dz. cyt., s. 87

m.in. do transferu danych, kontroli poprawności połączeń, zarządzania siecią, zdalnego włączania się do sieci oraz usług aplikacyjnych.

Tabela 9.1

Model TCP/IP

Warstwa aplikacji
Warstwa transportowa
Warstwa internetowa
Warstwa dostępu do sieci

Źródło: https://pasja-informatyki.pl/sieci-komputerowe/model-tcp-ip-iso-osi/, dostęp: 27.11.2020 r.

Model TCP/IP przedstawia tabela 9.1. Wyróżniono w nim warstwę dostępu do sieci, internetową, transportową oraz aplikacji. Warstwa dostępu do sieci kontroluje media transmisyjne oraz urządzenia fizyczne. Media transmisyjne dzielą się na bezprzewodowe i przewodowe. Przewodowymi nazywamy okablowanie miedziane lub włókna światłowodowe, których zadaniem jest przesył sygnału po wcześniej określonym torze. Bezprzewodowe media transmisyjne nie są ograniczone, ponieważ emisja sygnału radiowego występuje we wszystkich kierunkach w przestrzeni[20]. Zadaniem następnej warstwy jest znalezienie najbardziej odpowiedniej trasy pakietów danych. Warstwa transportowa jest odpowiedzialna za komunikację pomiędzy podłączonymi urządzeniami. Ostatnia warstwa jest wykorzystywana bezpośrednio przez użytkownika oraz oprogramowanie, posiada graficzny interfejs ułatwiający obsługę aplikacji[21].

Połączone za pomocą routerów zbiory urządzeń i elementów tworzące globalną infrastrukturę teleinformatyczną nazwano stacjami sieciowymi oraz sieciami komputerowymi. Dane przetwarzane w sieciach teleinformatycznych można podzielić na dane lokalizacyjne oraz dane telekomunikacyjne. Te pierwsze mogą odnosić się do np. do szerokości i długości geograficznej urządzenia, które korzysta z usług telekomunikacyjnych. Dane telekomunikacyjne opisują wykorzystywane usługi sieciowe, do których można zaliczyć m.in. ilość wysyłanych i odbieranych pakietów danych w trakcie sesji[22].

Sieci komputerowe wykorzystywane są jako platformy wymiany informacji pomiędzy operatorami urządzeń informatycznych (komputerów). Głównym zadaniem tych sieci jest jak największe ułatwienie komunikacji i zwiększenie przepływu informacji pomiędzy użytkownikami. Przeznaczone są także do gromadzenia i składowania zasobów oraz zdalnego kontrolowania

[20] D.E. Comer, *Sieci komputerowe i intersieci*, Wydawnictwo Naukowo-Techniczne. Gliwice. 2012, s. 142-143.
[21] http://www.crypto-it.net/pl/teoria/protokoly-tcp-ip.html, dostęp: 27.11.2020 r.
[22] M. Lakomy, *Cyberprzestrzeń…*, dz. cyt., s. 88.

i pracy na innych urządzeniach. W skład sieci komputerowych wchodzą elementy aktywne oraz pasywne sieci[23].

Dane zawarte w tabeli nr 9.2 przedstawiają podział elementów, które wchodzą w skład sieci komputerowych. Podzielone one zostały na elementy aktywne oraz pasywne.

Tabela 9.2

Elementy aktywne i pasywne sieci komputerowych

Elementy aktywne	Elementy pasywne
Routery	Media transmisyjne
Switch – przełącznik łączący segmenty sieci komputerowej	Panele krosowe
Punkty dostępowe	Szafy dystrybucyjne
Serwery	Organizatory kabli

Źródło: https://pasja-informatyki.pl/sieci-komputerowe/elementy-skladowe-sieci/, dostęp: 27.11.2020 r.

Podział sieci komputerowych przyjęty został ze względu na obszar działalności, dlatego wyróżnić możemy sieci lokalne (ang. *Local Area Network*, LAN), sieci miejskie (ang. *Metropolitan Area Network,* MAN) oraz sieci rozległe (ang. *Wide Area Network*, WAN). Sieci lokalne obszarem obejmują zazwyczaj nieznaczny obszar, którym może być dom, kancelaria lub biuro. Sieci miejskie zawierają w sobie lokalne sieci komputerowe, w konsekwencji terytorialnie obejmuje całą aglomerację miejską. Sieć rozległa obejmuje całe państwa oraz kontynenty, a najlepszym przykładem takiej sieci jest Internet[24].

Drugim z kryteriów podziału sieci komputerowych jest funkcja, którą pełni:

- bezprzewodowa sieć lokalna (ang. *Wireless Local Area Network,* WLAN), którą tworzą urządzenia komunikujące się ze sobą metodą bezprzewodową;
- sieć pamięci masowej (ang. *Storage Area Network*, SAN) używana przeważnie w wysoko budżetowych korporacjach, cechuje się zaawansowaną strukturą i znacznymi kosztami utrzymania. Jej zadaniem jest zapewnienie dostępu systemom informatycznym do pamięci masowej, na której przechowywane są dane niezbędne do funkcjonowania tej organizacji;
- szeregowa magistrala komunikacyjna (ang. *Controller Area Network*, CAN) odnalazła zastosowanie m.in. w systemach instalowanych w pojazdach, gdzie zamiast na prędkość przesyłu danych priorytet postawiono na transmisję danych odporną na zakłócenia elektromagnetyczne;

[23] M. Marczyk, *Cyberprzestrzeń…*, dz. cyt. s. 64.
[24] Tamże.

– sieć osobista (ang. *Personal Area Network*, PAN) a także bezprzewodowa sieć osobistah (ang. *Wireless Personal Area Network*, WPAN) wykorzystywana np. w środowisku biurowym lub domowym, sieć o małym zasięgu, może zostać „zbudowana" poprzez połączenie komputera, drukarki lub innych urządzeń zdolnych do wymiany informacji[25].

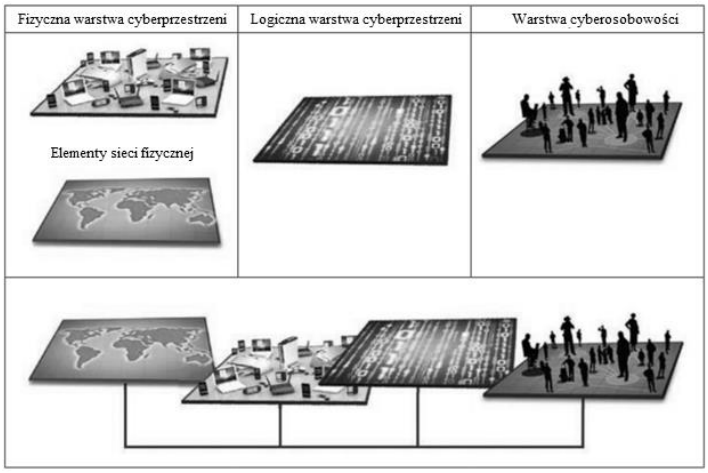
W ustawie „Prawo telekomunikacyjne" sieci telekomunikacyjne zdefiniowane są jako „systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju[26]". Sieci telekomunikacyjne odpowiedzialne są za „wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami[27]"

Cyberprzestrzeń pomimo swej bardzo skomplikowanej niematerialnej postaci (często utożsamianą z wirtualną rzeczywistością[28]) jest ściśle uzależniona od materialnej infrastruktury teleinformatycznej. Każdy użytkownik powinien więc mieć świadomość tego, że poprzez fizyczną interakcję z wykorzystywanym przez siebie urządzeniem, np. uruchomienie aplikacji, korzystanie z portali społecznościowych czy przeglądanie różnego rodzaju stron internetowych, pozostawia na niematerialnym poziomie cyberprzestrzeni ślad w postaci działań arytmetycznych i logicznych.

Na rysunku 9.1 przedstawiono warstwy cyberprzestrzeni. Składa się ona z warstwy fizycznej (ang. *physical network layer*), logicznej (ang. *logical network layer*), cyberosobowości (ang. *cyber-persona layer*).

Warstwa fizyczna tworzona jest przez fizyczne elementy sieci i systemów teleinformatycznych. Składa się z urządzeń oraz infrastruktury zawartej w przestrzeni lądowej, morskiej, powietrznej i kosmicznej, czyli domenach fizycznych. Ich działanie zapewnia przechowywanie, przesyłanie i przetwarzanie danych w cyberprzestrzeni. Wobec wszystkich składników warstwy fizycznej, czyli wszelkiego rodzaju kable, przewody, routery, komputery, itp., należy zastosować fizyczne zabezpieczenia, które mają zapobiec fizycznym uszkodzeniom i nieautoryzowanym fizycznym dostępem.

[25] M. Marczyk, *Cyberprzestrzeń…*, dz. cyt., s. 65.
[26] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2004 r. nr 171, poz. 1800, z późn. zm.).
[27] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej,* Warszawa 2015.
[28] M. Marczyk, *Cyberprzestrzeń…*, dz. cyt., str. 61.



Źródło: Joint Publication 3-12, Cyberspace Operations.

Rysunek 9.1. Warstwy cyberprzestrzeni

Warstwa logiczna zbudowana jest z elementów siei, które powiązane są ze sobą poprzez połączenia logiczne. Za pomocą oprogramowania obsługującego ich kody są w stanie sterować komponentami sieciowymi (modemy, karty sieciowe, routery, przełączniki). Komputery i inne urządzenia sieciowe podłączone do sieci teleinformatycznej są węzłami i posiadają adres IP, czyli logiczny adres interfejsu urządzenia podłączonego do sieci komputerowej. Niezwiązane z pojedynczym węzłem dane, procesy, aplikacje i procesy to rozproszone elementy cyberprzestrzeni. Warstwa cyberosobowości jest stworzona przez wyodrębnione dane z warstwy logicznej z użyciem reguł, które mają zastosowanie w logicznej warstwie sieci w celu opracowania opisu cyfrowych reprezentacji aktora lub podmiotu w cyberprzestrzeni. Warstwa ta składa się z kont użytkowników oraz relacji pomiędzy nimi. Relacje te mogą odnosić się bezpośrednio do rzeczywistej osoby lub podmiotu, z uwzględnieniem niektórych danych osobowych lub organizacyjnych (np. adres e-mail, IP, numer telefonu, dane logowania). Jedna osoba może tworzyć i utrzymywać wiele cyberosobowości poprzez używanie wielu identyfikatorów w cyberprzestrzeni, takich jak osobne służbowe i osobiste adresy e-mail oraz przybrane tożsamości na różnych witrynach internetowych. Sytuacja może również być odwrotna, czyli jedna cyberosobowość może być tworzona i utrzymywana przez wielu użytkowników, np. używanie jednego konta bankowego przez członków rodziny, przez wielu hakerów (osoby znajdujące i wykorzystujące podatności w oprogramowaniu komputerowym dzięki którym uzyskują dostęp do ich zasobów). Cyberosobowość cechuje się znaczną złożonością, co niesie za sobą wzmożony wysiłek rozpoznawczy w celu jej identyfikacji. Podobnie jak w logicznej warstwie sieci, złożone zmiany w cyberosobowości mogą nastąpić bardzo szybko w porównaniu do podobnych zmian w fizycznej warstwie

sieci, co bez szczegółowego śledzenia zmian komplikuje działa w stosunku do rozpoznawanego celu[29].

Cyberzagrożenia – podstawy teoretyczne

Gwałtowny rozwój techniczny oraz technologiczny prowadzi do intensywnego rozwoju cyberprzestrzeni. Wskutek tego cyberzagrożenia stają się dla użytkowników cyberprzestrzeni coraz poważniejszym zagadnieniem. Cyberprzestępcy oraz hackerzy (ang. *hacker*) dostosowują swoje metodologie, narzędzia oraz procesy zależnie od celu ataku[30]. Zagrożenia w cyberprzestrzeni rozumiane są jako niepożądane działanie, którego celem jest wpływ ma funkcjonowanie użytkowników cyberprzestrzeni. W aspekcie przetwarzania informacji można wyróżnić dwie kategorie takich działań:

- Zdarzenia losowe;
- Działania celowe[31].

Oba rodzaje takich działań mogą prowadzić do ujawnienia danych wrażliwych, a także do ich modyfikacji, destrukcji lub kradzieży w celu uzyskania korzyści majątkowych. Aby zapobiegać takim działaniom, podmioty korzystające oraz „poruszające" się po cyberprzestrzeni nieustannie są zmuszeni poszerzać swoją wiedzę na temat sposobów działania osób, które chcą wyrządzić szkodę im lub instytucji, której podlegają[32].

Identyfikacja wszystkich cyberzagrożeń jest zagadnieniem niemożliwym do zrealizowania tak samo jak ich całkowita eliminacja, ponieważ ukształtowana struktura cyberprzestrzeni umożliwia przeprowadzenie skrytych czynności. Wskutek tego, że analiza cyberzagrożeń odbywa się dopiero po wystąpieniu ataku dodatkowo stawia atakującego w znacznie bardziej komfortowej sytuacji niż potencjalnego obrońcę ataku. Taki rodzaj działania, które jest dobrze przygotowane, pomimo tego, że zawiera poznane już elementy, ale użyte jest w oryginalny sposób, sprawia, że różni się od poznanych już metod. Swoboda korzystania z cyberprzestrzeni poprzez zachowanie anonimowości dodatkowo daje atakującemu możliwość działania bez pozostawienia śladów identyfikacyjnych[33].

Działania cyberprzestępców, a także działalność militarna przenoszona jest do cyberprzestrzeni z powodu czynników takich jak:

- Znacznie zredukowany koszt utrzymania wojska oraz sprzętu wojskowego w stosunku do niskich kosztów, jakie niosłoby za sobą

[29] Joint Publication 3-12, *Cyberspace Operations.*
[30] S. Winterfeld, J. Andress, *The basics of cyber warfare*, Syngress Media, U.S., Amsterdam, Boston, Heidelberg, London, New York, Oxford, Paris, San Diego, San Francisco, Singapore, Sydney, Tokyo 2013, s. 1-14.
[31] M. Marczyk, *Cyberprzestrzeń…*, dz. cyt., s. 67.
[32] Tamże.
[33] R. Jaczewski, *Cyberprzestrzeń – część teatru działań hybrydowych*, „Przegląd Sił Zbrojnych", nr 2/2019, s. 37.

utrzymanie zespołu mogącego z powodzeniem zaatakować rozległą infrastrukturę instytucji, armii itp.;
- Oskarżonemu o szkodliwe działanie w cyberprzestrzeni podmiotowi w niewielu przypadkach udaje się udowodnić winę;
- Konsekwencje prawne dotyczące np. wykradania informacji wrażliwych lub pieniędzy w cyberprzestrzeni są mniejsze w stosunku do tych, które dotyczą działań w świecie rzeczywistym;
- Atak w cyberprzestrzeni może zostać przeprowadzony z każdej lokalizacji, co niesie za sobą brak potrzeby zbliżania się do celu w czasie prowadzenia działań[34].

Definicje cyberzagrożeń

Cyberzagrożenie utożsamiane jest z „sytuacją lub stanem, które komuś zagrażają lub w których ktoś czuje się zagrożony[35]" w cyberprzestrzeni. Są to zagrożenia, które wykształciły się w związku z gwałtownym technicznym i technologicznym postępem. Coraz większa popularyzacja Internetu prowadzi do przenoszenia usług i działalności właśnie do Internetu. Działania te ułatwiają cyberprzestępcom oraz tworzą okazje dla nich do przeprowadzenie ataku, a informacje, które są w stanie oni wykorzystać sprzyjają tylko i wyłącznie atakującemu. Dodatkowo im więcej informacji zostanie pozyskane mogą doprowadzić do przeprowadzenia ataku, który ma znaczną szansę powodzenia[36]. Do jednych z najważniejszych cyberzagrożeń można zaliczyć między innymi:

- Ukierunkowany atak wyłudzający informacje (ang. *phishing*), który poprzedzony jest szczegółowym wywiadem środowiskowym w celu uzyskania potrzebnych informacji i zasobów, które mają zapewnić powodzenie w planowanym ataku;
- Boty (skrót od robot), czyli programy komputerowe opierające się na aplikacji lub skrypcie, które automatycznie realizują zaprogramowane działania, wykorzystywane do kradzieży tożsamości swoich ofiar[37].

Cyberprzestrzeń opiera swoje funkcjonowanie na rozwiązaniach firm o ogólnoświatowym zasięgu, takimi jak Microsoft, IBM czy Lenovo. Standaryzacja środowiska cyberprzestrzeni powoduje, że osoby lub instytucje stają się bardziej podatne na ataki. Z powodu rozpoznania struktury oraz kodu atakowanego oprogramowania przełamywanie zabezpieczeń różnego rodzaju baz danych może nie stanowić problemu dla cyberprzestępcy[38]. Wrogo nastawione

[34] M. Marczyk, *Cyberprzestrzeń…*, dz. cyt., s. 70.
[35] https://sjp.pwn.pl/szukaj/zagro%C5%BCenie.html, dostęp: 20.01.2021 r.
[36] https://ostrzegamy.online/cyberzagrozenia-czym-sa-i-jak-sie-przed-nimi-bronic/, dostęp: 20.01.2021 r.
[37] R. Jaczewski., *Cyberprzestrzeń…*, dz. cyt., s. 37.
[38] R. Jaczewski, *Cyberprzestrzeń…*, dz. cyt., s. 38.

podmioty wykorzystują w cyberprzestrzeni także manipulację wartości danych, które pozyskują z urządzeń działających w sieci i systemach teleinformatycznych. Do takich danych należą m.in. długość i szerokość geograficzna, które zmieniane są przez np. zorganizowaną grupę cyberprzestępców w celu zmylenia organów ścigania i zwiększenia własnej swobody w przeprowadzaniu ataków w domenach geograficznych[39].

Według raportu o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 r., najwięcej zarejestrowanych incydentów w Polsce w roku 2019 r. obejmowało struktury ministerstw. Spośród wszystkich incydentów najczęściej występujące zdarzenia to wirusy, czyli fragmenty kodu oprogramowania dołączone do innej aplikacji, które w zależności od określonych zasad działania, mające za zadanie uszkadzać oraz zaburzać integralność zainfekowanego systemu. Oprócz tego, jednym z największych zagrożeń określonych na podstawie raportu Zespołu CSIRT GOV (czyli Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego) są kampanie phishingowe, które polegają ponawiającym się rozsyłaniu fałszywych wiadomości e-mail, najczęściej wykorzystując podszywanie się pod różnego rodzaju instytucje, w celu pozyskiwania danych wrażliwych nieświadomych użytkowników cyberprzestrzeni. Tego rodzaju zorganizowane działanie jest uważane przez Zespół CSIRT GOV jako realne zagrożenie dla bezpieczeństwa systemów teleinformatycznych, poza tym może to być atak poprzedzający następny, który może być dużo bardziej rozległy[40].

Rodzaje cyberzagrożeń

Zagrożenia w cyberprzestrzeni można podzielić na techniczne oraz nietechniczne. Do tych pierwszych zaliczamy złośliwe oprogramowanie, którego celem jest uszkodzenie, zniszczenie lub przejęcie i kontrola systemów komputerowych, teleinformatycznych, do których zaliczają się także na co dzień używane urządzenia przenośne, które można podłączyć do sieci telekomunikacyjnej.

Do nietechnicznych zagrożeń w cyberprzestrzeni należą wszelkiego rodzaju działania, zachowania i zjawiska pośród użytkowników Internetu, których celem są najczęściej kradzież tożsamości oraz zdobycie poufnych informacji i danych, które prowadzą do strat finansowych i wizerunkowych ofiar.

Tabela 9.3 przedstawia podział zagrożeń w cyberprzestrzeni. Zagrożenia te podzielone zostały na techniczne oraz nietechniczne. Jednak ze względu na coraz nowsze oraz bardziej zaawansowane metody prowadzenia cyberataków podziału mogą być dokonywane według różnych kryteriów.

Tabela 9.3

[39] Tamże.

[40] *https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/969,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2019-roku.html, dostęp: 21.01.2021 r.*

Podział zagrożeń w cyberprzestrzeni

Techniczne zagrożenia w cyberprzestrzeni	Nietechniczne zagrożenia w cyberprzestrzeni
Wirusy	Phishing
Robaki	Trolling
Malware	
Konie trojańskie	
DoS/DDoS	

Źródło: https://www.gov.pl/web/baza-wiedzy/cyberbezpieczenstwo/, dostęp: 20.01.2021 r.

Do najpopularniejszych zagrożeń technicznych należą:

- Wirusy;
- Robaki, czyli samodzielny program, który jest w stanie samodzielnie powielać się oraz przesyłać między urządzeniami podpiętymi do sieci komputerowej[41];
- Malware (ang. *malicious software*) – oprogramowanie, którego zadaniem jest wykradanie z zainfekowanego systemu danych wrażliwych właściciela, jednocześnie pozostawiając go nieświadomym jego działania[42].

Natomiast najbardziej rozpowszechnionymi nietechnicznymi zagrożeniami w cyberprzestrzeni są:

- Atak phishing, czyli metoda, w której atakujący podszywa się pod inne instytucje w wiadomościach e-mail, a także specjalnie stworzone strony internetowe, których wygląd, styl i forma przypominać ma pożądany przez użytkownika portal. Oparta na działaniach socjotechnicznych jest najczęstszym nietechnicznym źródłem zagrożenia dla użytkownika cyberprzestrzeni[43];
- Agresywne zachowania najczęściej spotykane na internetowych forach dyskusyjnych, nazywane trollowaniem (ang. *Trolling*). Działanie takie ukierunkowane jest na wpływ na pozostałych użytkowników biorących udział w dyskusji w celu zaburzenia rozmowy nieprawdziwymi informacjami oraz chęci ich ośmieszenia[44].

[41] https://www.pcworld.pl/porada/Czym-jest-robak-i-jak-go-rozpoznac,414776.html, dostęp: 20.01.2021 r.
[42] https://www.avast.com/pl-pl/c-malware, dostęp: 20.01.2021 r.
[43] https://www.pcworld.pl/porada/Phishing-czym-jest-jak-dziala-i-jak-go-unik-nac,415276.html,
dostęp: 20.01.2021 r.
[44] https://www.pcworld.pl/news/Wyciekla-korespondencja-obnazajaca-dzialania-rosyjskich-trolli,397939.html, dostęp: 20.01.2021 r.

Techniczne cyberzagrożenia

Do technicznych cyberzagrożeń zaliczają różnego rodzaju oprogramowania, które przeznaczone są m.in. do przejęcia atakowanego systemu komputerowego. Ponadto ataki złośliwego oprogramowania mogą prowadzić do uszkodzenia zainfekowanego sprzętu. Pierwszą pozycją w tabeli 3 wśród technicznych cyberzagrożeń wskazany został wirus komputerowy. Zbudowany jest on z fragmentu kodu, który ukryty jest w innej aplikacji, która otwarta uruchamia go. Wskutek tego złośliwy kod jest replikowany co powoduje w zainfekowanym systemie takie efekty jak spowolnienie pracy lub usuwanie danych zapisanych na dysku twardym urządzenia[45]. Wirusy komputerowe można podzielić na:

- Wirusy rezydentne, czyli takie, które zainstalowane są w pamięci operacyjnej komputera i wykonujące zaprogramowany szkodliwy kod w momencie otwierania aplikacji;
- Wirusy nierezydentne. Są to wirusy, które charakteryzują się samoczynnym uruchamianiem, egzekwowaniem kodu i infekowanie kolejnych aplikacji. Ponadto, są w stanie zablokować prawidłowy rozruch systemu komputerowego, ponieważ w momencie zainfekowania nośnika rozruchowego uruchamiają się przed zaplanowanymi plikami systemowymi[46].

Następnym technicznym cyberzagrożeniem są robaki (ang. *worms*). Robak to program, który przemieszcza się z jednego komputera na drugi, ale nie dołącza się do systemu operacyjnego komputera, który infekuje. Różni się od wirusa, który jest również programem migracyjnym, ale dołącza się do systemu operacyjnego dowolnego komputera, do którego wchodzi i może zainfekować każdy inny komputer korzystający z plików z zainfekowanego komputera (tłum. autora)[47].

Do technicznych zagrożeń zalicza się również malware (ang. *malicious software*), czyli rodzaj złośliwego oprogramowania, które obejmuje swym działaniem aplikacje i skrypty. Działanie malware określone może być na wiele sposobów. Jego głównym wykorzystaniem jest wydobywanie danych wrażliwych ofiary oraz szpiegowanie bez wiedzy właściciela zainfekowanego urządzenia. Jednym z rodzajów malware jest oprogramowanie szpiegujące (ang. *spyware*). Cyberprzestępcy korzystają z tego rodzaju rozwiązania, aby pozyskać poufne informacje, do których zaliczają się dane logowania do bankowości elektronicznej oraz szczegółowe dane osobowe. Do oprogramowania szpiegującego można zaliczyć także rejestrator używanych klawiszy (ang. *keylogger*). Jego działanie opiera się na rejestrowanie klawiszy, które używane są

[45] https://www.pcworld.pl/porada/Czym-jest-wirus-komputerowy-Piec-oznak-infekcji-wirusem,414611.html, dostęp: 20.01.2021 r.
[46] Tamże.
[47] https://law.justia.com/cases/federal/appellate-courts/F2/928/504/452673/, dostęp: 20.01.2021 r.

przez nieświadomego użytkownika zainfekowanego sprzętu[48]. Następnym rodzajem malware jest spopularyzowane wśród cyberprzestępców złośliwe oprogramowanie wymuszające zapłatę za zakodowane pliki w zaatakowanym systemie (ang. *ransomware*). Ransomware infekuje komputer i wyświetla komunikaty z żądaniem uiszczenia opłaty, aby system znów działał. To program służący do wyłudzania pieniędzy, może zostać zainstalowany za pomocą zwodniczych odnośników w wiadomościach e-mail, komunikacie lub witrynie internetowej. Posiada możliwość zablokowania ekranu komputera lub zaszyfrowania ważnych, z góry określonych plików hasłem, do którego dostęp ma tylko autor ataku[49].
Następną pozycją jest koń trojański (nazwa została zapożyczona z mitologii greckiej – podstęp, zakamuflowane zagrożenie), czyli rodzaj ukrytego wirusa w aplikacji lub załączniku w wiadomości e-mail, których zadaniem jest przekonanie potencjalnego użytkownika, że będzie chciał on z niego skorzystać. Działanie konia trojańskiego umożliwia atakującemu zdobycie kontroli nad urządzeniem, a następnie może niszczyć zgromadzone na nim dane. Poza tym ten szkodliwy fragment kodu (w zależności od zaprogramowanego działania) pozwala także na zdalny dostęp do zainfekowanego komputera lub innego urządzenia[50].

Ostatni technicznym cyberzagrożeniem zawartym w 3 jest atak blokujący usługi poprzez wzmożony ruch użytkowników na wybranych stronach internetowych (ang. *Denial of* Service*, Distributed Denial of Service,* DoS, DDoS). Ataki typu DoS opierają się na generowaniu fałszywego ruchu w obrębie atakowanej strony internetowej. Celem takiego rodzaju ataku jest spowolnienie i „unieruchomienie" danej witryny. Prowadzi to do strat finansowych właściciela. Atak DDoS zazwyczaj wykonywany jest za pomocą sieci komputerów, nad którymi cyberprzestępcy mają kontrolę z powodu wcześniejszego zainfekowania ich złośliwym oprogramowaniem (ang. *botnet*). Następnie właściciele urządzeń stają się nieświadomymi współautorami ataku blokującego usługi[51].

Nietechniczne cyberzagrożenia

Cyberzagrożenia nietechniczne to takie, których działanie opiera się w znacznej mierze na metodzie socjotechnicznej, nazywanej również inżynierią społeczną. Polega ona na stosowaniu manipulacji oraz sztuczek psychologicznych w celu uzyskania u odbiorcy zamierzonego działania. Są to narzędzia, które nie mogą być zatrzymane przez powszechne teraz zabezpieczenia,

[48] https://mfiles.pl/pl/index.php/Z%C5%82o%C5%9Bliwe_oprogramowanie, dostęp: 20.01.2021 r.
[49] https://www.kaspersky.com/resource-center/definitions/what-is-ransomware, dostęp: 20.01.2021 r.
[50] https://mfiles.pl/pl/index.php/Z%C5%82o%C5%9Bliwe_oprogramowanie, dostęp: 20.01.2021 r.
[51] https://mfiles.pl/pl/index.php/Cyberbezpiecze%C5%84stwo, dostęp: 21.01.2021 r.

jakimi są np. programy antywirusowe. Bazujące na niewiedzy oraz ludzkiej podatności na manipulowanie zagrożenia te mogą być znacznie groźniejsze od technicznych cyberzagrożeń. Rozwiązania te wykorzystane są również głównie do kradzieży danych wrażliwych w celu pozyskania korzyści finansowych[52].

W tabeli 9.3 przedstawione zostały poszczególne nietechniczne cyberzagrożenia. Pierwszą pozycją jest niezwykle popularny atak polegający na wyłudzeniu poufnych informacji (ang. *phishing*). Działanie to opiera się próbie podszycia się atakującego pod inną osobę lub instytucję, a następnie w spreparowanej wiadomości e-mail (alternatywą jest fałszywa strona internetowa) nakłania adresata do pożądanego przez siebie działania. W 2015 roku cyberprzestępcy przeprowadzili zorganizowane ataki phishing za pomocą przyjętego przez nich wizerunku firmy kurierskiej DHL. Wiadomości wysyłane przez atakujących wyglądem, treścią, stylem oraz formą przypominały te, która prawdziwa firma wysyła swoim klientom w związku z przesyłkami na nich zaadresowanymi. Kliknięcie odnośnika dołączonego do wiadomości powodowało pobranie, a następnie użytkownik poprzez uruchomienie go powodował nieświadome zainfekowania swojego urządzenia[53].

Poza cyberzagrożeniami, w których korzystający z cyberprzestrzeni może utracić swoje dane wrażliwe istnieją też zagrożenia wynikające z poczucia anonimowości innych użytkowników. Wskutek tego na forach dyskusyjnych, mediach społecznościowych „atakujący" prowokuje pozostałych rozmówców poprzez niepoprawne zachowanie, np. prowokacja, agresja oraz złośliwość w kierunku pozostałych osób. Działanie to nazwane zostało jako trolling (nazwa pochodzi od skandynawskich wierzeń ludowych, w którym troll był stworzeniem podobnym do ludzi, jednak wyróżniał się złośliwością oraz niskim ilorazem inteligencji) lub flaming (ang. *flame war*, wojna na bluzgi)[54].

Socjotechnika jako cyberzagrożenie

„Socjotechnika to wywieranie wpływu na ludzi i stosowanie perswazji w celu oszukania ich tak, aby uwierzyli, że socjotechnik jest osobą o sugerowanej przez siebie, a stworzonej na potrzeby manipulacji, tożsamości. Dzięki temu socjotechnik jest w stanie wykorzystać swoich rozmówców, przy dodatkowym (lub nie) użyciu środków technologicznych, do zdobycia poszukiwanych informacji.[55]" Bazując na doświadczeniu Kevina Mitnicka można zauważyć jak człowiek, korporacje, a nawet rządy państw są podatne na działanie

[52] https://www.computerworld.pl/news/10-sztuczek-inzynierii-spolecznej-na-ktore-trzeba-uwazac,415773.html, dostęp: 21.01.2021 r.
[53] https://sekurak.pl/jak-skutecznie-radzic-sobie-z-phishingiem-studium-przypadku/, dostęp: 21.01.2021 r.
[54] https://slownik.intensys.pl/definicja/trolling/, dostęp: 21.01.2021 r.
[55] K. Mitnick, W. L. Simon, *Sztuka podstępu. Łamałem ludzi, nie hasła*, Wydawnictwo Helion, Gliwice 2010, s. 2.

socjotechniczne. Gwałtowny techniczny i technologiczny rozwój spowodował, że bezpieczeństwo w cyberprzestrzeni opiera się głównie na automatycznych zabezpieczeniach, takich jak programy antywirusowe. Zapomniano jednak o poprawnym i bieżącym informowaniu użytkowników systemów teleinformatycznych o zagrożeniach płynących z ich niewiedzy, ignorancji oraz złudnego poczucia bezpieczeństwa[56]. Cyberprzestępcy korzystający z socjotechniki, która nazywana jest także inżynierią społeczną, bez przerwy kształcą się i udoskonalają swoją technikę, np. poznają procedury, terminologię oraz sposoby komunikacji pracowników danego przedsiębiorstwa. Wskutek tego wymierzone przez nich działania sprawiają wrażenie wiarygodnych, a nieświadomy adresat ataku pada ofiarą kradzieży danych pożądanych przez cyberprzestępcę.

Jedne z groźniejszych złośliwych rodzajów oprogramowania, które spustoszyły zainfekowane urządzenia (np. robak ILOVEYOU, Sircam czy Anna Kournikova) zostały rozpowszechnione właśnie dzięki metodzie socjotechnicznej. Wysłane jako załączniki wiadomości e-mail, które wabiły adresatów m.in. darmowymi filmami pornograficznymi lub informacją, że ich konto bankowe zostało obciążone znaczną sumą[57].

Przygotowując atak opierający się na inżynierii społecznej zaczyna się od pozyskania danych, które są powszechnie dostępne i wbrew przekonaniu przeciętnego użytkownika lub instytucji są one przydatne socjotechnikom. Dane, które są umieszczone na portalach społecznościowych, na stronie internetowej przedsiębiorstwa, doświadczeni socjotechnicy potrafią wykorzystać znajomość godzin otwarcia danej firmy czy nawet informacje na temat sytuacji w życiu prywatnym pracownika[58].

Kevin Mitnick zdefiniował i opisał cykl socjotechniczny. Zawiera on:

- Rozpoznanie – wywiad środowiskowy, w którym analizie podlegają wszystkie informacje, które są ogólnodostępne.
- Budowanie więzi i zaufania – na podstawie zgromadzonych informacji zmiana tożsamości, w trakcie korespondencji z potencjalną ofiarą używa się nazwisk osób, które są znane adresatowi, posłużenie się potrzebą pomocy lub zasugerowanie, że autor ataku posiada wyższy status społeczny.
- Wykorzystanie zaufania, za pomocą którego ofiara sama udostępnia informacje lub prosi o pomoc.
- Wykorzystanie informacji – wszystkie informacje zgromadzone w trakcie trwania cyklu przybliżają atakującego do sukcesu. Jeżeli otrzymane dane nie spełniają oczekiwań atakującego, ale stanowią kolejny etap w zdobyciu cenniejszych informacji, napastnik ponawia cykl socjotechniczny[59].

[56] Tamże, s. 3.
[57] Tamże, s. 108.
[58] K. Mitnick, W. L. Simon, *Sztuka podstępu…*, dz. cyt., s. 26-42.
[59] Tamże, s. 360.

Aby poprawnie zabezpieczyć się przed potencjalnym atakiem socjotechnicznym, instytucje oraz firmy poza implementacją najnowszych aktualizacji oraz użyciem aplikacji zwiększające poziom bezpieczeństwa powinny skupić się na czynniku ludzkim, który nieprawidłowo wyszkolony stanowi poważne źródło zagrożenia na tego rodzaju ataki. Przełamanie zaawansowanych zabezpieczeń uzyskiwane najczęściej jest poprzez działania z użyciem inżynierii społecznej, która „otwiera drzwi" do pozyskania danych wrażliwych[60].

Metodologia

Praca została napisana na podstawie dokładnej analizy materiałów zwartych, artykułów naukowych oraz rzetelnych stron internetowych. Zagadnieniem badawczym powyższej pracy było zbadanie cyberzagrożeń, a także analiza stosowanych technik socjotechnicznych. Podejmowane problemy badawcze pracy zostały postawione w formie szczegółowych pytań badawczych:

1. Jak formułowane są definicje cyberprzestrzeni?
2. Jak kształtuje się struktura cyberprzestrzeni?
3. Jakie są podstawy teoretyczne cyberzagrożeń?
4. Jak definiowane jest pojęcie cyberzagrożeń?
5. Jakie są rodzaje cyberzagrożeń?
6. Co charakteryzuje techniczne cyberzagrożenia?
7. Jak opisywane są cyberzagrożenia o charakterze nietechnicznym?
8. Jak traktowana jest socjotechnika w stosunku do cyberzagrożeń?
9. Jaki jest wpływ socjotechniki jako cyberzagrożenie na użytkowników Internetu?
10. Jak socjotechnika wpływa na użytkowników Internetu?

W pracy zastosowano jako podstawową metodę wykorzystano analizę i krytykę publikacji zwartych, artykułów oraz rzetelnych źródeł internetowych. Zastosowano również metodę badawczą w postaci badania ankietowego. Badanie to polegało na zbadaniu opinii oraz wiedzy respondentów na temat socjotechniki jako cyberzagrożenie dla studentów Akademii Marynarki Wojennej w Gdyni.

Przegląd literatury

Największy wpływ na wyniki pracy miały następujące pozycje:

- „Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru" – M. Marczyk;
- „Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw" – M. Lakomy;
- „Cyberprzestrzeń – część teatru działań hybrydowych" – R. Janczewski;

[60] Tamże, s. 15.

- „Sztuka podstępu. Łamałem ludzi, nie hasła" - K. Mitnick, W. L. Simon;
- "Cyberspace Operations" - Joint Publication 3-12;
- "The basics of cyber warfare", S. Winterfeld, J. Andress;
- Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej;
- „Sieci komputerowe i intersieci", D.E. Comer;
- „Bezpieczeństwo informacyjne", K. Liderman;
- „Neuromancer", W. Gibson.

Wnioski

Wyniki badań pozwalają na sformułowanie wniosku, iż nieustanny rozwój metod przeprowadzania cyberataków, sprawia, że użytkownicy Internetu narażeni są w szczególności na ataki przeprowadzane metodami socjotechnicznymi. W celu ochrony własnych sieci lub systemów teleinformatycznych oprócz implementacji najnowszych aktualizacji systemu oraz ochrony urządzeń programami antywirusowymi należy także zwrócić uwagę na aspekty takie jak:

- Nieustanne pozyskiwanie wiedzy na temat cyberzagrożeń;
- Świadomość użytkowników;
- Zdrowy rozsądek;
- Spostrzegawczość.

Świadomość użytkowników o konieczności przestrzegania podstawowych zasad bezpieczeństwa jest kluczem do udaremnienia potencjalnego ataku socjotechnicznego. Autor ma nadzieję, że zebrane w tej pracy materiały pomogą zauważyć problem oraz skłonić do analizy informacji jakie udostępniane są na portalach społecznościowych oraz innych źródłach internetowych.

Bibliografia

Opracowania zwarte

1. Comer D.E., *Sieci komputerowe i intersieci*, Wydawnictwo Naukowo-Techniczne. Gliwice. 2012.
2. Gibson W., *Neuromancer*, Wydawnictwo Kameleon, Radom 1999.
3. Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015.
4. Liderman K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012.
5. Lizut J., *Zagrożenia cyberprzestrzeni kompleksowy program dla pracowników służb społecznyc*h, Wydawnictwo Wyższej Szkoły Pedagogicznej im. Janusza Korczaka, Warszawa 2014.
6. Mitnick K., Simon W. L., *Sztuka podstępu. Łamałem ludzi, nie hasła*, Wydawnictwo Helion, Gliwice 2010.

7. Winterfeld S., Andress J., *The basics of cyber warfare*, Syngress Media, U.S., Amsterdam, Boston, Heidelberg, London, New York, Oxford, Paris, San Diego, San Francisco, Singapore, Sydney, Tokyo 2013.

Artykuły

1. M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru, „*Przegląd teleinformatyczny", nr 1-2/2018.
2. R. Jaczewski, *Cyberprzestrzeń – część teatru działań hybrydowych*, „Przegląd Sił Zbrojnych", nr 2/2019.
3. R. Janczewski, G. Pilarski, M. Marczyk, *Terminology as a barrier to NATO's interoperability in cyberspace operations*, "International Conference Knowlegde-Based Organization", nr 25(3)/2019.
4. T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*. „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 1/2005.

Dokumenty normatywne

1. Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej, Warszawa 2015.
2. Dz. U. 2002 Nr 156 Poz. 1301. Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej.
3. Joint Publication 3-12, Cyberspace Operations.
4. Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Warszawa 2013.
5. Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, Departament Ewidencji Państwowych i Teleinformatyki MSWiA, Warszawa 2010.
6. Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2004 r. nr 171, poz. 1800, z późn. zm.).

Źródła internetowe

1. http://www.crypto-it.net/pl/teoria/protokoly-tcp-ip.html, dostęp: 27.11.2020 r.
2. https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/969,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2019-roku.html, dostęp: 21.01.2021 r.
3. https://law.justia.com/cases/federal/appellate-courts/F2/928/504/452673/, dostęp: 20.01.2021 r.

4. https://mfiles.pl/pl/index.php/Cyberbezpiecze%C5%84stwo, dostęp: 21.01.2021 r.
5. https://mfiles.pl/pl/index.php/Z%C5%82o%C5%9Bliwe_oprogramowanie, dostęp: 20.01.2021 r.
6. https://mfiles.pl/pl/index.php/Z%C5%82o%C5%9Bliwe_oprogramowanie, dostęp: 20.01.2021 r.
7. https://ostrzegamy.online/cyberzagrozenia-czym-sa-i-jak-sie-przednimi-bronic/, dostęp: 20.01.2021 r.
8. https://sekurak.pl/jak-skutecznie-radzic-sobie-z-phishingiem-studium-przypadku/, dostęp: 21.01.2021 r.
9. https://sjp.pwn.pl/szukaj/zagro%C5%BCenie.html, dostęp: 20.01.2021 r.
10. https://slownik.intensys.pl/definicja/trolling/, dostęp: 21.01.2021 r.
11. https://www.avast.com/pl-pl/c-malware, dostęp: 20.01.2021 r.
12. https://www.computerworld.pl/news/10-sztuczek-inzynierii-spolecznej-na-ktore-trzeba-uwazac,415773.html, dostęp: 21.01.2021 r.
13. https://www.kaspersky.com/resource-center/definitions/what-is-ransomware, dostęp: 20.01.2021 r.
14. https://www.pcworld.pl/news/Wyciekla-korespondencja-obnazajaca-dzialania-rosyjskich-trolli,397939.html, dostęp: 20.01.2021 r.
15. https://www.pcworld.pl/porada/Czym-jest-robak-i-jak-go-rozpoznac,414776.html, dostęp: 20.01.2021 r.
16. https://www.pcworld.pl/porada/Czym-jest-wirus-komputerowy-Pieczoznak-infekcji-wirusem,414611.html, dostęp: 20.01.2021 r.
17. https://www.pcworld.pl/porada/Phishing-czym-jest-jak-dziala-i-jak-go-uniknac,415276.html, dostęp: 20.01.2021 r.

bsmt. pchor. Kuba WOJNICKI

CYBERZAGROŻENIA W ASPEKCIE BEZPIECZEŃSTWA NARODOWEGO

Streszczenie

W pracy podjęto analizie tematykę zjawiska cyberzagrożeń pochodzących z cyberprzestrzeni, które mogą oddziaływać na polskie bezpieczeństwo narodowe. W celu podjęcia tematu, w pierwszej kolejności poddano badaniu materiały naukowe oraz dokumenty kształtujące cyberprzestrzeń w Rzeczpospolitej Polskiej. W pracy przedstawiono wyjaśnienie pojęć, którymi operuje się w odniesieniu do cyberprzestrzeni. Jest to szeroko rozumiane przez organy międzynarodowe oraz państwowe cyberbezpieczeństwo, a także dynamicznie rozwijająca się cyberprzestępczość. Przedstawiono również zagadnienia związane z cyberterroryzmem oraz walką informacyjną wraz z przykładami pochodzącymi z kraju i świata.

Słowa kluczowe:
Cyberzagrożenie, cyberprzestrzeń, cyberbezpieczeństwo, cyberterroryzm, bezpieczeństwo, informacja, obywatel, Rzeczypospolita.

Abstract

Cyber threats in terms of national security

Summary: The work analyses the phenomenon of cyber threats from cyberspace, which may affect Polish national security. In order to address the topic, scientific materials and documents shaping cyberspace in the Republic of Poland were first examined. The work provides an explanation of the terms used in relation to cyberspace. This is widely understood by international bodies and state cybersecurity, as well as dynamically developing cybercrime. It also presents issues related to cyberterrorism and information struggle, along with examples from the country and the world.

Keywords:
cyberthreats, cyberspace, cybersecurity, cyberterrorism, security, information, citizen.

Wstęp

W dzisiejszych czasach rozwój technologii i techniki jest bardzo dynamiczny. Wiele państw rozbudowuje swoje sieci i systemy teleinformatyczne. Ogólnoświatowa cyfryzacja doprowadziła do powstania nowego środowiska, w którym miliony ludzi z całego świata spędzają wiele czasu dziennie. Komputer stał się powszechnie używanym narzędziem do codziennej pracy, wypoczynku czy komunikacji. Wiele osób nie potrafi żyć bez smartfonu. Jego brak sprawia poczucie dyskomfortu i bezradności. W małym urządzeniu znajdują się wszystkie najpotrzebniejsze informacje. Zawiera również wiele danych osobowych. Jego kradzież i dostęp do zawartości pozwalają poznać sekrety właściciela, które łatwo wykorzystać przeciwko niemu. Sieci i systemy teleinformatyczne oraz techniczne i technologiczne rozwiązania łączą w całość złożone struktury państwa. Procesy informacyjne oraz zarządzanie informacjami w dużej mierze odbywają się w cyberprzestrzeni. Powstały internetowe biblioteki, urzędy, instytucje, banki oraz wiele innych podmiotów wykorzystujących i przetwarzających dane osobowe. Bezpieczeństwo funkcjonowania społeczeństwa czy gospodarki w dużym stopniu opiera się o infrastrukturę krytyczną. Wydaje się zatem, że to właśnie szeroko rozumiane bezpieczeństwo powinno być priorytetem państwa. Bez niego techniczny i technologiczny czy społeczny rozwój państwa może stać się utrudniony. W cyberprzestrzeni znajduje się wiele zagrożeń, których nie należy bagatelizować. Celowe jest zatem umacnianie cyberbezpieczeństwa. Na początku lat 90. XX wieku Internet nie był popularny i dostęp do niego posiadała jedynie część światowej populacji, z czego większość stanowili obywatele Stanów Zjednoczonych. W Polsce dostęp do Internetu posiadały głównie instytucje rządowe, samorządowe oraz firmy prywatne. Związane to było ze słabo rozwiniętą infrastrukturą telekomunikacyjną oraz ceną usług internetowych.

W 2020 roku liczba użytkowników Internetu w skali świata to około 4.9 mld[1]. Dynamiczny rozwój techniki i technologii spowodował powstanie nowych dziedzin nauki. Pojawiła się potrzeba zdefiniowania i dodania do słownika pojęć z zakresu cyberbezpieczeństwa oraz stworzenia technicznych i prawnych narzędzi w nowo powstałym Systemie Cyberbezpieczeństwa, gwarantujących bezpieczeństwo użytkowników systemów teleinformatycznych.

Cyberprzestrzeń i pojęcia z nią związane

System teleinformatyczny to podstawowy składnik cyberprzestrzeni. Urządzenia informatyczne i oprogramowania zapewniają przetwarzanie, przechowywanie, wysyłanie i odbieranie danych i informacji za pomocą sieci telekomunikacyjnej i odpowiedniego urządzenia końcowego. Sieć telekomunikacyjna to „*systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają*

[1] https://www.internetworldstats.com/stats.html dane z 30 września 2020 r., dostęp: 30.10.2020 r.

nadawanie, odbiór lub transmisje sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju; wykorzystywane są one głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych"[2]. Cyberprzestrzeń obejmuje wszystkie systemy informatyczne (ang. *Information Technology systems – IT systems*) włączone w ogólnoświatową sieć teleinformatyczną.

Ogólnodostępny słownik terminów i definicji NATO AAP-6 definiuje cyberprzestrzeń jako „*domenę ogólnoświatową obejmującą wszystkie wzajemne połączone systemy komunikacyjne,* informatyczne*, i inne systemy elektroniczne, sieci i ich dane, w tym te, które są oddzielone lub niezależne, które przetwarzają, przechowują lub przesyłają dane*"[3]. Definicja cyberprzestrzeni przedstawiona przez NATO skupia się głównie na systemach i danych znajdujących się w cyberprzestrzeni. Nie precyzuje aspektu prawnego i społecznego.

Powszechnie znana i często przytaczana definicja Departamentu Obrony USA na potrzeby ujednolicenia terminologii wojskowej, określa cyberprzestrzeń jako „*Globalną domenę wewnątrz środowiska informacyjnego składającą się z współzależnych sieci telekomunikacyjnych, infrastruktur informacyjnych technologii i zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe oraz znajdujące się w nich procesory i kontrolery*" (tłum. Janusz Wasilewski)[4]. Definicja ta skupia się również na aspektach technicznych. Wyodrębnia systemy komputerowe wraz z ich podzespołami. Nie odnosi się do aspektów społecznych cyberprzestrzeni.

W Polskim ustawodawstwie cyberprzestrzeń pierwszy raz zdefiniowano

w założeniach do Rządowego Programu Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2009-2011[5]. Dokument określił ją jako „*przestrzeń komunikacyjną tworzoną przez system powiązań internetowych*"[6]. Kolejna wersja Rządowego Programu Ochrony Cyberprzestrzeni RP[7] na lata 2011 – 2016 znacznie rozbudowała poprzednią definicję i zastosowała bardziej techniczne pojęcia. Jej treść brzmi w następująco „*cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*"[8]. W polskiej próbie wyjaśnienia tego terminu pojawia się aspekt społeczny określony jako relacje użytkowników.

[2] Art. 2 ustawy z dnia 14 września 2018 r. w sprawie jednolitego tekstu ustawy – Prawo telekomunikacyjne (Dz. U. z 2018 r. poz. 1954 ze zm.).
[3] https://wcnjik.wp.mil.pl/u/AAP6PL.pdf, dostęp: 01.11.2020 r.
[4] https://fas.org/irp/doddir/dod/jp1_02.pdf, dostęp: 01.11.2020 r.
[5] Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia, Warszawa 2009.
[6] Tamże.
[7] Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016, MSWiA, Warszawa 2010.
[8] Tamże.

Bezpieczeństwo jest ważnym aspektem życia każdego człowieka. Zdaniem amerykańskiego psychologa Abrahama Maslowa istnieje pięć ludzkich potrzeb. Według tego autora są to potrzeby fizjologiczne, bezpieczeństwa, przynależności, miłości, uznania, samorealizacji[9]. Należy zwrócić uwagę, że bezpieczeństwo zostało uznane jako ważny stan psychiczny i fizyczny potrzebny do prowadzenia normalnego życia. To od bezpieczeństwa zależy rozwój państwa i komfort życia jego mieszkańców. Konstytucja Polski w art. 5 określa prawo wszystkich obywateli kraju do bezpieczeństwa, którego strzeże Rzeczypospolita Polska[10]. Zapewnienie bezpieczeństwa w cyberprzestrzeni również należy do obowiązków współczesnego państwa, które chce uchodzić za nowoczesne i dostosowujące się do zmieniającego świata.

Bezpieczeństwo w ujęciu słownika języka polskiego oznacza „*stan, w którym nie jest się w żaden sposób zagrożonym, spokój i pewność*"[11]. Funkcjonowanie człowieka bez zmartwień o swoje przetrwanie. Każdy człowiek inaczej odczuwa potrzebę swojego bezpieczeństwa. Rosnące uzależnienie od funkcjonowania w cyberprzestrzeni powoduje powstanie nowych obaw.

W Doktrynie Cyberbezpieczeństwa Rzeczypospolitej Polskiej cyberbezpieczeństwo RP jest opisane jako „*proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni*"[12]. Natomiast w Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022 cyberbezpieczeństwo oznacza „*odporność systemów teleinformatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, integralność i poufność przechowywanych lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne*[13]".

Reasumując, obydwie definicje różnią się od siebie. Pierwsza traktuje cyberbezpieczeństwo jako ciągły i nieprzerwany proces, który pozwala na funkcjonowanie państwa. Podkreśla znacznie struktur państwa, podmiotów, przedsiębiorców i należących do nich systemów teleinformatycznych i zasobów informacyjnych. Nazywa cyberprzestrzeń globalną. Druga utożsamia bezpieczeństwo z odpornością na działania szkodzące atrybutom bezpieczeństwa informacji (dostępność, integralność, poufność), a także z bezpieczeństwem sieci i usług informatycznych. Różnice tych definicji spowodowane są tym, że ocena bezpieczeństwa oraz stan poglądu podmiotu na otaczające go niebezpieczeństwa są obiektywne. Niemniej jednak wszystkie pojęcia opisują

[9] https://mfiles.pl/pl/index.php/Piramida_Maslowa, dostęp: 01.11.2020 r.
[10] https://www.sejm.gov.pl/prawo/konst/polski/kon1.html, dostęp: 01.11.2020 r.
[11] https://sjp.pwn.pl/slowniki/bezpieczeństwo.html, dostęp: 01.11.2020 r.
[12] https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf, dostęp: 01.11.2020 r.
[13] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Warszawa 2017, s. 28.

konieczność ochrony cyberprzestrzeni przed incydentami, nadużyciami i szkodliwymi działaniami.

Cyberbezpieczeństwo odnosi się do działań w cyberprzestrzeni. Wpływ cyberprzestrzeni na funkcjonowanie człowieka we współczesnym świecie jest niezaprzeczalnie bardzo duży. Ryzyko utraty danych i informacji minimalizowane jest przez wzmacnianie cyberbezpieczeństwa. W 2014 roku w Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej ustanowiony został cel strategiczny odnoszący się do bezpiecznego funkcjonowania państwa w cyberprzestrzeni[14]. Dokumentu stracił moc w 2020 roku na rzecz nowej wersji. Nowa Strategia zakłada, że podmioty zwiększą odporność systemów publicznych, wskazuje na potrzebę zapewnienia cyberbezpieczeństwa w kontekście militarnym, rozwijanie świadomości społecznej w zakresie cyberbezpieczeństwa, rozwój rodzimych rozwiązań i finansowanie prac badawczo-rozwojowych w obszarze nowych technologii[15]. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 wskazuje cyberbezpieczeństwo jako środek do pomyślnego rozwoju kraju. Sprawne działanie systemów informacyjnych oraz komunikacyjnych ma odzwierciedlenie w takich aspektach jak gospodarka państwowa, instytucje państwowe, działalność podmiotów, aktywność społeczna, funkcjonowanie obywatela w codziennym życiu[16]. Zostały ustanowione strategiczne założenia funkcjonowania państwa w cyberprzestrzeni, w celu zapewniania bezpieczeństwa obywateli i podmiotów. Istnieją przesłanki do podjęcia tematu cyberbezpieczeństwa w wymiarze zewnętrznym oraz wewnętrznym. Cyberprzestępczość skierowana bezpośrednio w systemy łączności, zakłócanie usług teleinformatycznych i kradzieże danych przedstawiają wymiar wewnętrzny. Natomiast wymiar zewnętrzny odzwierciedlają działania grup terrorystycznych i przestępczych, cyberkonflikty, cyberkryzysy oraz cyberszpiegostwo[17].

Tradycyjna przestępczość jest zachowaniem społecznym. Cechują ją negatywny odbiór. Przestępstwo w ujęciu słownikowym to „*popełnianie przestępstw; ogół przestępstw popełnionych w pewnym okresie w danym kraju lub środowisku albo przez określoną kategorię przestępców*”[18]. Przestępczość kryminalna, narkotykowa i gospodarcza to najogólniejszy podział czynów karalnych. Współcześni przestępcy wychodzą poza tradycyjne ramy. Swoją pomysłowością i determinacją starają się oszukać system prawny wykorzystując naj-

[14] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2014, s. 12.
[15] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2020.
[16] Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, str. 8.
[17] Z. Husak, *Ochrona bezpieczeństwa państwa przed zagrożeniami cybernetycznymi w Unii Europejskiej*, [w:] W. Lis, *Bezpieczeństwo państwa*. Zagadnienia podstawowe, KUL, Lublin 2014, s. 56.
[18] https://sjp.pwn.pl/slowniki/przestępczość.html, dostęp: 01.11.2020 r.

nowsze techniki. Nowa przestrzeń działalności uniezależnia człowieka od zajmowanego miejsca w przestrzeni fizycznej. Umożliwia mu swobodne poruszanie się w niej. Jedynym wymogiem jest podłączenie się do sieci teleinformatycznej poprzez odpowiedni sprzęt. Użytkownik jest w stanie pozostać anonimowym, jeśli jego umiejętności informatyczne są wystarczająco rozwinięte. Jedynie komputer lub inne urządzenie, z którego korzysta może zostać wykryte. Swoboda ta daje szerokie pole manewru dla negatywnej formy ludzkiej działalności. Anonimowość i brak konieczności bezpośredniego, fizycznego udziału zachęca do popełniania przestępstw klasyfikowanych jako cyberprzestępstwa.

W Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej[19] z 2013 roku definicja cyberprzestępstwa przedstawiona jest krótko jako „czyn zabroniony popełniony w obszarze cyberprzestrzeni"[20].

Cyberprzestępstwa opisywane są również jako przestępstwa komputerowe. Ich definicja to „*przestępstwo popełnione za pomocą lub bezpośrednio dotyczące systemu przetwarzania danych lub sieci komputerowe*"[21].

Wyróżniono i opisano trzy następujące po sobie na przestrzeni lat generacje przestępstw komputerowych. Na samym początku, czyli w pierwszej generacji przestępstwa komputerowe były niezbyt skomplikowane i nie powodowały większych szkód. Polegały na naruszaniu integralności oprogramowania oraz ingerowanie w znajdujące się tam dane komputerowe dla poklasku i aprobaty. Okres ten przypisywany jest na wczesne lata 90. XX wieku. Druga generacja przestępstw komputerowych przypada na początek XXI wieku. Wtedy to wraz ze wzrostem wiedzy informatycznej oraz rozwojem sieci teleinformatycznych pojawiły się ataki hackerskie[22]. Motywy przestępców również uległy zmianie. Zaczęli kierować się chęcią zarobienia łatwych pieniędzy. Systemy wykrywania sprawców nie były tak rozbudowane jak dziś. Większość przestępców nie przejmowała się zabezpieczeniami, nie zacierając swoich działań. Trzecia generacja przestępstw komputerowych to znane współcześnie profesjonalne podejście do ataków[23]. Zdecydowana większość ataków jest celowa, skrupulatnie zaplanowana i przeprowadzona z dbałością o szczegóły. Działania są skryte, szybkie i trudne do wykrycia. Masowo używane botnety i złośliwe oprogramowania są w stanie wyszukiwać samodzielnie podatności i uderzyć w najmniej spodziewanym momencie. Ataki skierowane są nie tylko w indywidualnego użytkownika, ale również bezpieczeństwo narodowe. Wrogo nastawione służby specjalne obcych państw, grupy terrorystyczne lub przestępcze mogą starać się wpłynąć na jakość funkcjonowania kraju

[19] Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013, str. 5.
[20] Tamże.
[21] PN-I-02000 Technika informatyczna – Zabezpieczenia w systemach informatycznych – Terminologia; PN-ISO/IEC 2382-8 Technika informatyczna – Terminologia – Bezpieczeństwo.
[22] Haker to osoba włamująca się do sieci i systemów komputerowych, https://sjp.pwn.pl/slowniki/haker.html, dostęp: 13.01.2021 r.
[23] M. Siwicki, *Cyberprzestępczość*, Monografie Prawnicze, C. H. Beck, Warszawa 2013, s. 1.

i jego systemów informatycznych. Wykrycie i dokładne wskazanie sprawców są trudne.

Rada Europy w swojej konwencji z dnia 23 listopada 2001 roku, która została sporządzona w Budapeszcie[24], podzieliła określone cyberprzestępstwa według ich rodzajów. Do pierwszej grupy zaliczono „*przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów*"[25]. Nielegalny dostęp (art. 2) jest to umyślny, bezprawny dostęp do całości lub części systemu informatycznego, naruszenie zabezpieczeń w celu wykradnięcia danych informatycznych. Nielegalne przechwytywanie danych (art. 3) to umyślne, bezprawne przechwytywanie za pomocą urządzeń technicznych niepublicznych transmisji danych z systemu informatycznego. Naruszenia integralności danych (art. 4) to umyślne, bezprawne niszczenie, wykasowanie, uszkodzenie, dokonanie zmian lub usuwanie danych informatycznych. Naruszenia integralności systemu (art. 5) to umyślne, bezprawne zakłócenie działania systemu informatycznego poprzez wprowadzanie, transmisję, niszczenie, wykasowanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych. Niewłaściwe użycie urządzeń (art. 6) to produkcja, sprzedaż, pozyskanie z zamiarem wykorzystania, importowanie, dystrybucja: urządzenia lub programu komputerowego przeznaczonego do popełnienia czynu karalnego, a także hasła komputerowego, kodu dostępu umożliwiających dostęp do systemu informatycznego. Druga grupa to przestępstwa komputerowe. Rozumiane jako fałszerstwa komputerowe (art. 7) czyli umyślne, bezprawne wprowadzanie, dokonywanie zmian, wykasowanie lub ukrycie danych informatycznych, w wyniku czego powstają dane nieautentyczne, wykorzystywane jako autentyczne. Oszustwa komputerowe (art. 8) rozumiane jako umyślne, bezprawne spowodowanie utraty majątku innej osoby poprzez wprowadzenie, dokonanie zmian, wykasowanie, usunięcie danych informatycznych oraz działanie szkodzące funkcjonalności systemu. Trzecia grupa związana z przestępstwami ze względu na charakter zawartych informacji. Przestępstwa związane z pornografią dziecięcą (art. 9) to umyślne i bezprawne produkowanie materiałów w celu ich rozpowszechnienia, oferowanie lub udostępnianie materiałów, rozpowszechniania lub transmitowania, pozyskiwania materiałów, posiadania materiałów za pomocą systemu informatycznego. Czwarta grupa to cyberprzestępstwa związane z naruszeniem praw autorskich i prac pokrewnych (art. 10) popełnione umyślnie, na skalę komercyjną, za pomocą systemu informatycznego. Piąta i ostatnia to grupa innych odpowiedzialności i sankcji, w którą wliczane jest usiłowanie, pomocnictwo i podżeganie do popełnienia przestępstwa wymienionych we wcześniejszych paragrafach (art. 5)[26].

W Doktrynie Cyberbezpieczeństwa RP z 2015 roku, dokonano podziału zagrożeń na mające wymiar wewnętrzny oraz zewnętrzny. Według tej

[24] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., Dz. U. 2015 poz. 728.
[25] Tamże.
[26] Tamże.

Doktryny tradycyjne zagrożenia wewnętrzne w dzisiejszym, nowoczesnym świecie mogą zostać przeniesione do cyberprzestrzeni. Ich forma pomimo zmiany środowiska jest podobna. Mowa o zjawiskach takich, jak cyberprzestępczość, cyberprzemoc, cyberprotesty o charakterze destrukcyjnym, zakłócające realizację istotnych zadań administracji publicznej oraz sektora prywatnego[27]. Wymiar wewnętrzny zagrożeń sprowadza się do pojęć takich jak cyberkryzys i cyberkonflikt z udziałem podmiotów państwowych i niepaństwowych, w tym także groźbę cyberwojny[28].

Aktualnie dla podmiotów stanowiących ryzyko w cyberprzestrzeni można użyć odpowiedniej kategoryzacji wprowadzonej przez Najwyższą Izbę Kontroli w swoich wynikach w zakresie ochrony cyberprzestrzeni przez podmioty państwowe RP. Jest to podział na cyberchuliganów, czyli indywidualne osoby lub grupy składające się z paru członków. Wykorzystują swoje nabyte umiejętności łamiąc zabezpieczenia systemów dla własnej satysfakcji. Cyberaktywiści to zorganizowane grupy, zrzeszone w celu osiągniecia swoich idei. Cyberprzestępcy wykorzystują systemy informatyczne w celu osiągnięcia korzyści finansowych niezgodnie z prawem. Cyberterroryści to pojedyncze osoby lub dobrze zorganizowane grupy wykorzystujące słabości społeczeństwa do osiągnięcia swoich celów politycznych. Cyberszpiedzy to zorganizowane grupy lub przedsiębiorstwa pracujące na rzecz swojego lub innego państwa. Zbierają dane informacyjne z zakresu technologicznego i gospodarczego. Cyberżołnierze to organizacje o charakterze militarnym. Wyspecjalizowane w kierunku walki w cyberprzestrzeni. Współpracują z siłami zbrojnymi lub we własnym zakresie[29].

Tak jak w każdej dziedzinie życia, tak i w polskim ustawodawstwie karnym dynamiczny postęp techniczny wymusił zmiany. Zupełnie nowe typy przestępstw przyczyniły się do nowelizacji Kodeksu karnego. Było to skutkiem wprowadzenia Decyzji Ramowej Rady Unii Europejskiej o cyberprzestępczości[30]. W obowiązującym polskim prawie nie istnieje osobna kategoria dla cyberprzestępstw. Zostały zdefiniowane i podzielone pomiędzy Kodeks karny, ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, ustawę z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych i ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[31]. Mimo tego, iż ich opisy występują to często stanowią problematyczne sytuacje dla podjęcia decyzji przez sąd. Dla rozstrzygnięcia kwestii spornych powoływany jest biegły sądowy z zakresu informatyki.

[27] https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf, dostęp: 31.10.2020 r.
[28] Tamże.
[29] Informacja o wynikach kontroli. Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP, Najwyższa Izba Kontroli, Warszawa 2015, s. 20.
[30] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., Dz.U. 2015 poz. 728.
[31] S. Wojciechowska-Filipek, Z. Ciekanowski, *Bezpieczeństwo funkcjonowania w cyberprzestrzeni*, Wydanie II, CeDeWu, Warszawa 2019.

Infrastruktura krytyczna wobec cyberterroryzmu.

Polska jako kraj nowoczesny, cały czas rozwijający swoje możliwości i wprowadzający wiele technicznych i technologicznych udogodnień, posiada rozbudowany system infrastruktury krytycznej. Są to głównie systemy oraz sieci teleinformatyczne oraz obiekty fizyczne. Wszystkie są ze sobą powiązane i mają na celu zapewnienie prawidłowego funkcjonowania państwa. Sytuacja, w której następuje negatywny wpływ na poziom bezpieczeństwa w państwie oraz ograniczone lub uniemożliwione działanie organów administracji publicznej i podmiotów usługowych, nazywa się sytuacją kryzysową[32]. Systemy wchodzące w skład infrastruktury krytycznej to: zaopatrzenie w energię, surowce energetyczne i paliwa (kopalnie, elektrownie, podmioty odpowiedzialne za produkcje paliw, sieci importu oraz transportu surowców), system łączności i sieci teleinformatycznych (sieci telekomunikacyjne, teleinformatyczne i poczta), system finansowy (instytucje finansowe i ich systemy informacyjne),system zaopatrzenia w wodę i żywność (podmioty i obiekty odpowiedzialne za wytwarzanie, przechowywanie, pozyskiwanie i transport wody oraz żywności), system ochrony zdrowia (instytucje takie jak szpitale, przychodnie, przedsiębiorstwa farmaceutyczne, a także systemy przetwarzania danych osobowych), system ratowniczy (Straż Pożarna, Ratownictwo Medyczne, Ratownictwo Górnicze, Policja oraz należące do nich obiekty), system transportowy i komunikacyjny (infrastruktura transportowa i komunikacyjna na terenie kraju oraz jej obiekty), system zapewniający ciągłość działania administracji publicznej (urzędy wojewódzkie, starostwa powiatowe, urzędy miast), system produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych (podmioty oraz obiekty zajmujące się czynnościami związanymi z manewrowaniem substancjami, które stanowią zagrożenie dla ludzi i środowiska)[33].

Każdy z nich odpowiedzialny jest prawidłowe funkcjonowanie najważniejszych sektorów w kraju. Są ze sobą ściśle powiązane i wrażliwe na ataki. Uszkodzenie lub przerwa w pracy jednego z nich skutkuje problemami z pozostałymi. Dlatego ich bezpieczeństwo jest niezwykle ważne dla gospodarki państwa. Sposoby ochrony powinny być na bieżąco udoskonalane w celu zapewnienia ciągłości, funkcjonalności i integralności. Zadaniem zabezpieczeń jest jednak tylko minimalizacja ryzyka. Jego całkowite wyeliminowanie z uwagi na wiele czynników jest niemożliwe.

Narodowy Program Ochrony Infrastruktury Krytycznej[34] z 2018 roku wymienia działania mające na celu zwiększenie bezpieczeństwa infrastruktury

[32] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 Nr 89 poz. 590. http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/U/D20070590Lj.pdf, dostęp: 03.11.2020 r.

[33] M. Żuber, *Infrastruktura Krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego*, „Rocznik Bezpieczeństwa Międzynarodowego", nr 8(2)/2014, str. 180.

[34] https://rcb.gov.pl/wp-content/uploads/Dokument-Główny-1.pdf, dostęp: 03.11.2020 r.

krytycznej. Zapewnienie bezpieczeństwa fizycznego (bezpieczeństwo fizyczne mające na celu odparcie ataku, próby dostania się do budynków strategicznych pod względem infrastruktury krytycznej. Takie czynności mogą wykonywać określone służby mundurowe lub ochrona fizyczna. Dodatkowo wprowadzone zabezpieczenia techniczne w postaci stref ochronnych i kontroli dostępu, systemów alarmowych, urządzeń monitorujących,); Zapewnienie bezpieczeństwa technicznego (podmioty odpowiedzialne za stałe monitorowanie
i diagnostykę systemów pod względem prawidłowości funkcjonowania procesów, wsparcie eksploatacyjne, określenie minimalnych wymagań); Zapewnienie bezpieczeństwa osobowego (odpowiednie systemy zabezpieczające, przeprowadzenie ankiety bezpieczeństwa osobowego wśród osób posiadających dostęp do najważniejszych elementów systemu); Zapewnienie bezpieczeństwa teleinformatycznego (zagrożenia pochodzące ze strony cyberprzestępców i cyberterrorystów. Celem tych ataków najczęściej są dane i informacje, które mogą posłużyć do zaburzenia pracy lub uszkodzenia systemów infrastruktury krytycznej. Odpowiednie zabezpieczenia systemów, wdrożenie procedur i mechanizmów odpowiedniego działania minimalizują ryzyko); Zapewnienie bezpieczeństwa prawnego (odpowiednie regulacje prawne w zakresie ponoszenia odpowiedzialności za systemy infrastruktury krytycznej oraz ich bezpieczeństwa. Oznacza to, także ograniczenie i blokowanie nieodpowiednich decyzji zarządów na drodze prawnej); Plany ciągłości działania i odtwarzania (sporządzenie odpowiednich dokumentów, zabezpieczenie środków finansowych, bieżące uzupełnianie planów odbudowy)[35].

Zagrożenia infrastruktury krytycznej dzielą się na zagrożenia naturalne (powodzie, silne wiatry, trzęsienia ziemi, susze), zagrożenia techniczne (uwolnienie niebezpiecznych środków chemicznych, awarie, zawalenia budynków, wypadki i zdarzenia losowe) oraz terroryzm[36]. Spośród wymienionych zagrożeń rząd państwa może zmniejszyć ryzyko występowania zagrożeń technicznych oraz terrorystycznych[37].

Wiele państw uniezależniło się od techniki i technologii, systemów, sieci i usług teleinformatycznych. Umożliwiło to powstanie nowego rodzaju terroryzmu, cyberterroryzmu. Cyberterroryzm, czyli terroryzm wymierzony przeciwko newralgicznym dla państwa systemom, sieciom i usługom teleinformatycznym, stanowi kluczową i stale rosnącą postać ataków terrorystycznych[38].

Federalne Biuro Śledcze (ang. *US Federal Bureau of Investigation*) określa cyberterroryzm jako „*obmyślony, politycznie umotywowany akt prze-*

[35] https://rcb.gov.pl/wp-content/uploads/Standardy-służące-zapewnieniu-sprawnego-funkcjonowania-infrastruktury-krytycznej-–-dobre-praktyki-i-rekomendacje.pdf, dostęp: 01.11.2020 r.
[36] J. Milewski, *Identyfikacja Infrastruktury Krytycznej i jej zagrożeń*, Systemowe Wymogi Bezpieczeństwa, „Zeszyty Naukowe AON" nr 4(105)/2016, str. 101.
[37] Tamże.
[38] Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia, AON, Warszawa 2009, s. 4.

mocy wymierzony przeciwko informacjom, programom, systemom komputerowym lub bazom danych, który mając charakter niemilitarny, przeprowadzony jest przez ponadnarodowe lub narodowe grupy terrorystyczne"[39].

Nowe metody walki takie jak np. wykorzystanie złośliwego oprogramowania czy ataki DDoS[40] pozwalają na przeprowadzanie zamachów, przy użyciu komputera. Celem stają się instytucje państwowe, finansowe, systemy infrastruktury krytycznej między innymi wodociągowe, telekomunikacyjne, energetyczne, ochrony zdrowia, transportowe, zaopatrzenia w wodę i żywność. Przeprowadzenie cyberataku nie wymaga przeznaczenia dużych środków finansowych. Różnica pomiędzy zakupem broni, gotowych materiałów wybuchowych lub środków do ich wytworzenia, a sprzętu komputerowego jest znacząca. Atakujący wykorzystując wiedzę informatyczną oraz dostęp do komputera może pozostać anonimowy. Może być to osoba indywidualna lub zorganizowana grupa. Cyberterroryści używają Internetu do propagandy i dezinformacji. Dzięki możliwości ogólnoświatowej komunikacji stają się medialni. Prowadzą wymianę danych, rekrutują w swoje szeregi, udostępniają filmy z ćwiczeń i egzekucji. Informacje potrzebne do podjęcia działań często pozyskują z portali społecznościowych i witryn internetowych[41].

W Estonii w 2007 roku doszło do aktu cyberterroryzmu. Powodem ataku hakerów był usunięty pomnik żołnierzy radzieckich z centrum Tallina. Napastnicy uderzyli w internetowe strony rządowe oraz systemy bankowe, blokując do nich dostęp. Skoordynowane w czasie ataki DDoS sparaliżowały kraj. Państwo bez możliwości komunikacji oraz transakcji finansowych poniosło straty budżetowe. Podobna sytuacja wydarzyła się w 2008 roku na Litwie. Nowe prawo zabraniające prezentowania symboli Związku Radzieckiego sprowokowało cyberterrorystów do zaatakowania około 300 stron rządowych i partii politycznych. Na stronach umieszczone zostały wizerunki sierpa i młota, flagi ZSSR i ubliżające hasła. Maszyny atakujących znajdowały się poza granicami kraju. Główne podejrzenia padły na rosyjskich crackerów[42]. Zauważalny wzrost cyberataków w Europie Zachodniej nastąpił po ukazaniu karykatury Mahometa w 2014 roku przez francuski tygodnik Charlie Hebdo. W związku z tym islamscy radykaliści udostępnili użytkownikom portali społecznościowych m.in. dane osobowe żołnierzy biorących udział w misjach skierowanych przeciwko Państwu Islamskiemu. Również w Polsce miały

[39] T. Szubrycht, *Współczesne aspekty bezpieczeństwa państwa*, „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 4(167)/2006.
[40] DDoS (ang. *distributed denial of service*) to rozproszony atak na systemy komputerowe lub usługę sieciową uniemożliwiający poprawne działanie poprzez zajęcie wszystkich wolnych zasobów. https://www.nask.pl/pl/aktualnosci/oferta/oferta-telekomunikacyjn/bezpieczenstwo/2662,DDoS-Attack-Protection.html, dostęp: 06.01.2021 r.
[41] https://rcb.gov.pl/terroryzm-wciaz-zagraza-unii-europejskiej/, dostęp: 06.01.2021 r.
[42] Cracker to „Informatyk zajmujący się poszukiwaniem i usuwaniem zabezpieczeń w oprogramowaniu komputerowym." T. Pączkowski, *Słownik cyberbezpieczeństwa*, Szkoła Policji w Katowicach, Katowice 2017, str. 18.

miejsce incydenty związane z cyberterroryzmem. W 2012 roku do opinii publicznej trafiła informacja o planach wprowadzenia ustawy ACTA (ang. *Anti-Counterfeiting Trade Agreement*). Dotyczyła ona walki z naruszeniami praw autorski oraz obrotem podrabianymi towarami. Wiele osób uznało jej warunki za próbę odebrania prawa wolności słowa i wypowiedzi w Internecie. Chcąc wymusić zmianę decyzji rządu zaatakowano między innymi strony Premiera, Sejmu, Biura Ochrony Rządu, Ministerstwa Sprawiedliwości oraz Policji.

Ataki są przeprowadzane na systemach finansowych państwa. Niedostępność sektora bankowego nie pozwala na przeprowadzanie transakcji finansowych. Obywatele, którzy w wyniku działań cyberterrorystów nie mają dostępu do swoich pieniędzy tracą zaufanie do rządu i instytucji. Pojawiają się obawy o następujące po sobie skutki ataku. Cyberterroryści mogą próbować manipulować obywatelami oraz modyfikować dane finansowe. Efektem tych działań jest wywołanie strachu. Podobne skutki niesie za sobą atak na systemy teleinformatyczne państwa. Paraliż komunikacji i działalności instytucji państwowych oraz zablokowanie dostępu do stron rządowych to kompromitacja i podważenie wizerunku państwa na arenie międzynarodowej.

Walka informacyjna w cyberprzestrzeni – aspekt wojskowy

Informacja jest kluczowa dla wielu procesów zachodzących w obszarze działań militarnych. Posiadanie wielu informacji ułatwia podejmowanie odpowiednich decyzji. Proces dowodzenia opiera się na pozyskiwaniu informacji. Uzyskanie przewagi informacyjnej, czyli „*umiejętności i zdolności ciągłego zbierania, niezakłóconego przetwarzania, przechowywania oraz terminowego udostępniania i dostarczania danych lub informacji*”[43] pozwala zyskać przewagę nad przeciwnikiem i zmniejszyć ryzyko podjęcia złych decyzji. W pracy przyjęto definicję informacji przedstawioną przez Roberta Janczewskiego, który określił, że „*informacja to wytwór procesu informacyjnego. Wytwór ten stanowi zarazem niematerialny zasób systemu informacyjnego*”[44].

Wykorzystanie informacji do obrony, a także do ataku na cel przyczyniło się do powstania pojęcia walki informacyjnej[45]. Departament Obrony Stanów Zjednoczonych w swojej dyrektywie z 2012[46] roku opisuje walkę informacyjną jako „*operacje informacyjne zintegrowane do użycia w czasie konfliktu zbrojnego, które mają wpłynąć, przeszkodzić, zniekształcić lub przejąć*

[43] R. Janczewski*, Procesy informacyjne w działaniach militarnych w cyberprzestrzeni*, w: *Systemy i sieci teleinformatyczne Sił Zbrojnych RP – wielorakie aspekty bezpieczeństwa cyberprzestrzeni*, [w:] B. Biernacik, L. Kalman (red.), AON, Warszawa 2016, str. 167.
[44] Tamże, str. 168.
[45] Z. Modrzejewski, *Cyberprzestrzeń środowiskiem walki informacyjnej*, Systemy i sieci teleinformatyczne Sił Zbrojnych Rzeczypospolitej, Akademia Sztuki Wojennej, Warszawa 2016, str. 151.
[46] Information Operation, Joint Publication 3-13, 20 November 2012 Incorporating Change 1, 20 November 2014, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf, dostęp: 19.01.2021 r.

procesy podejmowania decyzji przez przeciwników lub potencjalnych przeciwników przy jednoczesnej ochronie własnych procesów informacyjnych" (tłum. autora)[47]. Celem walki informacyjnej jest uniemożliwienie przeciwnikowi podejmowania odpowiednich decyzji i przeprowadzania działań strategicznych na polu walki, a w tym samym czasie zabezpieczenie przed podobnymi działaniami ze strony przeciwnika własnych wojsk[48].

Do prowadzenia walki informacyjnej mogą zostać wykorzystane media w Internecie. Mają one rolę opiniotwórczą. Media społecznościowe zmieniają światopogląd i wywierają wpływ na użytkowników. Informacje są dowolnie kształtowane, a ogólnoświatowy zasięg utrudnia weryfikacje ich prawdziwości. Media umożliwiają manipulacje i dezinformację. Działania propagandowe mogą mieć za zadanie podłożenie fundamentów pod przeprowadzenie działań zbrojnych skierowanych w inne państwo. Za czasów panowania Saddama Husajna, Irak podejrzewany był o wspieranie organizacji terrorystycznej Al-Kaida. Ameryka po atakach na z 11 września 2001 roku na wieże World Trade Center i Pentagon rozpoczęła walkę ze światowym terroryzmem. Stany Zjednoczone oskarżały Irak o domniemane posiadanie bomby atomowej i łamanie ustanowień ONZ. Zarzuty doprowadziły do wtargnięcia i objęcia większości terytorium kraju przez koalicję państw. W walkach zbrojnych obie strony poniosły ofiary. Próby odnalezienia dowodów na współprace z Al-Kaidą oraz posiadanie broni atomowej zakończyły się niepowodzeniem[49].

Walka informacyjna w cyberprzestrzeni wchodzi w skład złożonego zjawiska jakim jest wojna hybrydowa. Pojęcie to opisuje metodę prowadzenia współczesnych konfliktów zbrojnych we wszystkich pięciu wymiarach: morski, lądowy, powietrzny, kosmiczny i cyberprzestrzeni. Wojna hybrydowa to połączenie tradycyjnych form walki wraz z użyciem cyberprzestrzeni do przeprowadzania cyberataków oraz prowadzenia działań propagandowych i dezinformacyjnych. Działania w wojnie hybrydowej nie mieszczą się w ramach ogólnie przyjętego konfliktu zbrojnego pomiędzy dwoma podmiotami. Wojna nie zostaje oficjalnie wypowiedziana. Starcia nie są prowadzone otwarcie. Działania hybrydowe prowadzone są asymetryczne. Atrybutami walki asymetrycznej jest skrytość działania pozwalająca na niewykrywalność, zmienność sposobów ataku, zaskoczenie przeciwnika, wysoka dynamika działań i globalny zasięg[50]. Słownik terminów i definicji AAP-6 NATO zagrożenie asymetryczne definiuje jako „*wynikające z możliwości zastosowania różnych środków i metod w celu obejścia lub neutralizacji silnych punktów przeciwnika, wykorzystując jednocześnie jego słabości w celu uzyskania niewspółmiernych wyników*"[51].

[47] Tamże, str. 9.
[48] Z. Modrzejewski, *Cyberprzestrzeń…*, dz. cyt, str. 154-155.
[49] Ibidem.
[50] K. Piątkowski, *Wojna nowego typu*, „Polska w Europie", nr 3(1)/2002, s. 23-24.
[51] https://wcnjik.wp.mil.pl/u/AAP6PL.pdf, dostęp: 03.11.2020 r.

Zaatakowanie infrastruktury krytycznej państwa oraz zniszczenie lub sparaliżowanie poszczególnych sektorów stworzy podatność do wykorzystania przez przeciwnika oraz obniży zdolności obronne państwa. Osłabienie zdolności obronnych sił zbrojnych będzie skutkiem uderzenia w wojskowe systemy informatyczne, zakłócenia oraz zerwanie łączności, obezwładnienie stanowisk dowodzenia i wprowadzenie dezinformacji.

Przykładem ukazującym ten rodzaj działań stał się konflikt na Ukrainie. Rosja prowadziła działania propagandowe już przed rozpoczęciem konfliktu. Wpływała na wewnętrzne konflikty, destabilizowała gospodarkę i zawyżała ceny gazu. Na arenie międzynarodowej przedstawiała swoje prawa do półwyspu Krymskiego opierając argumenty o historię tego terenu. Argumenty rosyjskie były motywowane ochroną kultury przed europejską i amerykańską polityką. Rosjanie doprowadzili do fizycznego zniszczenia mediów masowego przekazu na Ukrainie i uniemożliwili nadawanie. Mieszkańcy terenów Krymu i Donbasu odbierali jedynie rosyjski przekaz propagandowy z elementami dezinformacji. Starali się utwierdzić mieszkańców w przekonaniu, że to właśnie oni działają na ich korzyść chcąc bronić kultury i tradycji euroazjatyckiej. Media prorosyjskie kreowały Rosję jako wyzwolicieli starających się negocjować pokój w rozbitej na grupy Ukrainie. Jednocześnie Ukraina umyślnie stawiana była w złym świetle. Prowadzono cyberataki na ukraińskie internetowe strony rządowe i instytucje blokując do nich dostęp. W walkach na terenie kraju brali udział rosyjscy żołnierze, którzy nie nosili oznaczeń i flag przynależności do swojego kraju na mundurach. Rosjanie nie przyznawali się do ingerencji twierdząc, że to prorosyjscy separatyści. Ludność, którą większość stanowiła rosyjskojęzyczna społeczność, z czasem zaczęła ulegać propagandzie i zagłosowała korzystnie w referendum aneksji Krymu przez Rosję. Prowadząc działania w ten sposób ukazali całemu światu, w jakim kierunku będzie się rozwijać współczesna wojna[52].

Rozwój techniki umożliwia prowadzenie walki informacyjnej. Wiele państw wykorzystuje informacje jako narzędzie do osiągania swoich celów. Manipulacja informacjami pozwala na wykorzystanie ich przeciwko innym krajom i oddziaływanie na obywateli.

Popularne formy cyberataków

Cyberatak wykorzystuje podatność systemów i sieci teleinformatycznych. Techniki penetracji systemów informatycznych i wykorzystywane do tego oprogramowania złośliwe tworzone są przez ludzi. Wymaga to biegłej wiedzy z zakresu informatyki. Cyberataki wykorzystywane są do kradzieży, oszustw, zniszczeń oraz jako narzędzie do szantażu. Ofiarą cyberataku jest państwo i obywatele. Cyberataki przeprowadzane są przez cyberprzestępców, cyberterrorystów oraz znajdują zastosowanie w cyberwojnach.

[52] J. Kowalewski, M. Kowalewski, *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2017, str. 136.

Najczęściej wykorzystywane w cyberatakach jest oprogramowanie złośliwe (ang. *Malware*). Jego zadaniem jest wykonanie niepożądanego działania w systemie teleinformatycznym. Oprogramowanie złośliwe może zostać nieumyślnie pobrane z Internetu lub umieszczone fizycznie w systemie teleinformatycznym za pomocą przenośnych nośników danych. W przypadku powodzenia oprogramowanie złośliwe zaczyna wyrządzać szkody. Modyfikuje treści, blokuje dostęp do systemu, wykrada ważne informacje i przejmuje kontrolę. Oprogramowanie złośliwe jest zaraźliwe i szybko rozprzestrzenia się w systemie. Jest trudne do wykrycia i usunięcia przez użytkownika, ponieważ potrafi samodzielnie ukrywać swoją obecność w systemie.

Robak (ang. *worm*) to oprogramowanie komputerowe działające samodzielnie. Potrafi rozpowszechniać się samoistnie i nie potrzebuje pomocy nieświadomego użytkownika, w odróżnieniu od wirusa. Robak rozsyła swoje kopie pomiędzy komputerami podłączonymi do sieci teleinformatycznej. Robak wykorzystuje luki w oprogramowaniu komputerowym i jego zabezpieczeniach. Użytkownik nieświadomie sam pobiera robaka na swój sprzęt komputerowy na przykład otwierając nieznany plik lub załącznik w wiadomości na skrzynce poczty elektronicznej. Przykładem incydentu z udziałem robaka była sytuacja
z 2 listopada 1988 roku. Student Robert Tappan Morris użył zaprogramowanego przez siebie robaka. Błędy na etapie tworzenia programu spowodowały niekontrolowane rozprzestrzenianie. W krótkim czasie robak zainfekował od 2 do 6 tysięcy komputerów. W 1988 roku liczba komputerów zaatakowanych tym robakiem stanowiła od 3 do 10% całego Internetu[53]. Drugim przykładem jest robak o nazwie Stuxnet, którego przeznaczeniem było szpiegowanie i przejmowanie kontroli nad systemami przemysłowymi. W 2010 roku większość komputerów zarażonych robakiem Stuxnet znajdowało się w Iranie, gdzie w wyniku ataku tego programu zostały uszkodzone irańskie reaktory atomowe. Oskarżonymi o utworzenie robaka i wykorzystanie go do ataku zostały Stany Zjednoczone oraz Izrael[54].

Koń trojański to oprogramowanie złośliwe nazywane potocznie trojanem. Trojan nie rozprzestrzenia się samodzielnie tylko podszywa pod inne aplikacje. Po dostaniu się do systemu koń trojański wprowadza zmiany, kradnie informacje i śledzi użytkowników w sieci teleinformatycznej. Wprowadzenie konia trojańskiego ułatwiają narzędzia maskujące szkodliwą działalność w systemie komputera (ang. *rootkit*) Narzędzie nadaje uprawnienia administratora. Infekuje system i ukrywa siebie oraz oprogramowanie złośliwe. Usuwa trojana z listy uruchomionych procesów w tle, chroni go przed programami

[53] Dorothy E. Denning, *Wojna informacyjne i bezpieczeństwo informacji*, Wydawnictwo Naukowo-Techniczne, Warszawa 2002, str. 319.
[54] https://www.cert.pl/wp-content/uploads/2015/11/Raport_CP_2010.pdf, dostęp: 07.01.2021 r.

antywirusowymi i administratorem poprzez ukrywanie jego nazwy w plikach[55].

Exploit to szkodliwy program, który wyszukuje oraz wykorzystuje podatności systemu lub programu. Podatności mogą powstać w trakcie tworzenia aplikacji przez programistów lub podczas wprowadzania aktualizacji. Exploit „zero-day" oznacza exploit, który został stworzony od razu po wykryciu podatności w systemie lub programie. Pozwala to na dokonanie ataku przed wprowadzeniem zabezpieczeń przez autora tego systemu lub programu[56].

Ransomware (ang. *ransomware*, „*ransom*" okup i „*software*" oprogramowanie) to oprogramowanie, którego zadaniem jest zablokowanie dostępu użytkownika do urządzenia. Czasem jedyną formą odblokowania komputera jest wpłacenie sumy pieniędzy w wirtualnej walucie. Najgroźniejsze ransomware, które zaatakowały użytkowników Internetu to Petya i WannaCry. Pierwszy z nich w 2017 roku zainfekował komputery na ogólnoświatową skalę. Pierwsze informacje o ataku pochodziły z Ukrainy[57]. Ransomware Petya zablokował komputery banków, dostawców energii oraz prywatnych przedsiębiorstw. Polska także stała się jedną z ofiar. Ataki na prawie całym świecie poskutkowały olbrzymimi stratami finansowymi. Stany Zjednoczone Ameryki oskarżyły Rosję o przeprowadzenie ataku, ta natomiast nie przyznała się do zarzucanych czynów[58]. Cyberatak z udziałem ransomware WannaCry miał miejsce w 2017 roku. Ransomware blokował dostęp do urządzeń w ponad 100 krajach. Wykonanie wpłaty na konto przestępców było wymogiem do odblokowania urządzenia. WannaCry zainfekował komputery przedsiębiorstw takich jak np. Nissan czy FedEx. Wykorzystywał exploita o nazwie EternalBlue do rozpowszechniania swojej treści[59]. Głównym podejrzanym o przeprowadzenie ataku była Korea Północna[60].

Oprogramowanie szpiegujące (ang. *spyware*) to oprogramowanie, które zostało stworzone do szpiegowania użytkownika i monitorowania tego co robi, jakie treści przegląda, gdzie się loguje. Umożliwia cyberprzestępcy pozyskanie danych osobistych, numerów kart płatniczych czy haseł dostępu. Oprogramowanie to zostaje pobrane razem z plikiem lub zainfekowanym załącznikiem w poczcie elektronicznej. Jednym z rodzajów spyware jest keylogger[61]. Umożliwia monitorowanie i zapisywanie, tego co użytkownik pisał na klawiaturze. Ułatwia to odgadnąć hasła dostępu.

---

[55] J. Kowalewski, M. Kowalewski, *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2017, str. 53-54.
[56] T. Pączkowski, *Słownik Cyberbezpieczeństwa*, Szkoła Policji w Katowicach, Katowice 2017, str. 30-31.
[57] https://niebezpiecznik.pl/post/kolejny-grozny-globalny-atak-tym-razem-ransomware-petya-ofiary-sa-takze-w-polsce/, dostęp: 07.01.2021 r.
[58] https://www.avast.com/pl-pl/c-petya, dostęp: 20.11.2020 r.
[59] https://www.cert.pl/news/single/wannacry-ransomware/, dostęp: 20.11.2020 r.
[60] https://www.bbc.com/news/world-asia-41816958, dostęp: 07.01.2021 r.
[61] Keylogger to rodzaj oprogramowania szpiegującego, które potajemnie rejestruje naciśnięcia klawiszy na klawiaturze, https://www.avast.com/pl-pl/c-keylogger, dostęp: 07.01.2021 r.

Adware (ang. *adware*, „*ad*" reklama i „*software*" oprogramowanie) to oprogramowanie złośliwe powodujące pojawianie się reklam. Urządzenie wyświetla reklamy w masowych ilościach, dodatkowo śledzi przeglądane strony internetowe i dostosowuje treść do indywidualnego odbiorcy.

Popularną metodą oszukiwania użytkowników Internetu ostatnich lat jest phishing (ang. *phishing*, „*phony*" fałszywy i „*fishing*" łowienie ryb). W atakach typu phishing cyberprzestępcy wykorzystują elementy inżynierii społecznej. Za pomocą wiadomości SMS lub poczty elektronicznej podszywają się pod banki, instytucje rządowe czy operatów telekomunikacyjnych. Cyberprzestępcy próbują w ten sposób uzyskać od swoich ofiar niejawne informacje, które zostaną wykorzystane do popełniania kolejnych przestępstw[62]. Pomimo swojej prostoty metoda ta jest bardzo skuteczna. W 2014 roku cyberprzestępcy przy pomocy tej metody podszywali się pod Pocztę Polską. W wiadomościach na skrzynce elektronicznej dotyczącej nieodebranej paczki znajdował się załącznik z wirusem komputerowym. Wiele tysięcy ludzi padło ofiarą manipulacji i zostało zainfekowanych[63]. W 2020 roku cyberprzestępcy wysyłali wiadomości na skrzynki elektroniczne podszywając się pod Światową Organizację Zdrowia (ang. *World Health Organization*, skrót WHO). Prosili o wpłatę pieniędzy na walkę z wirusem COVID-19 lub nakłaniali do otworzenia zainfekowanego wirusem linka[64].

Cyberprzestępca za pomocą szkodliwego oprogramowania (ang. *malware*) może przejąć komputer użytkownika Internetu. W ten sposób powstaje „bot[65]", który wykonuje zadania wskazane przez cyberprzestępcę, bez wiedzy właściciela tego komputera. Cyberprzestępca zdobywając dostęp do następnych komputerów tworzy grupę botnetów, potocznie nazywanych komputerami „zombie". Grupy botnetów[66] mogą składać się z kilku do nawet kilkuset tysięcy komputerów[67]. Cyberprzestępca może wykorzystać botnety do rozsyłania dużych ilość wiadomości na poczcie elektronicznej (ang. *spam*). Z wykorzystaniem botnetów może przeprowadzić atak DDoS, polegający na wysyłaniu dużej ilości zapytań (z komputerów „zombie") do serwera, co spowoduje jego przeciążenie i odmowę dostępu do oferowanej przez niego usługi dla innych użytkowników Internetu. Poza tym botnety używane są do infekowania

[62] https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y, dostęp: 07.01.2021 r.
[63] https://www.benchmark.pl/aktualnosci/cyberprzestepcy-podszywaja-sie-pod-poczte-polska.html, dostęp: 20.11.2020 r.
[64] https://www.who.int/about/communications/cyber-security, dostęp: 07.01.2021 r.
[65] Bot to program wykonujący pewne czynności w zastępstwie człowieka. Czasem jego funkcją jest zautomatyzowane naśladowanie ludzkiego zachowania, https://pl.wikipedia.org/wiki/Bot_(program), dostęp: 03.01.2021 r.
[66] Botnet to to grupa zhakowanych komputerów, które są kontrolowane w sposób zdalny, https://plblog.kaspersky.com/botnet/6302/, dostęp: 13.01.2021 r.
[67] R. Kasprzyk, M. Paź, Z. Tarapata, *Modelowanie i symulacja cyberzagrożeń typu botnet*, Symulacja w Badaniach i Rozwoju", nr 6(2)/2015, str. 89-90.

wirusami komputerowymi innych komputerów oraz kradzieży niejawnych danych i informacji[68].

Kolejny bardzo popularny atak to atak polegający na podsłuchu i modyfikacji wiadomości przesyłanych pomiędzy dwiema stronami bez ich wiedzy. Atak taki został nazwany „człowiek w środku" (ang. *man-in-the-middle,* skrót MITM). Atak ten polega na skrytym wtargnięciu pomiędzy dwie komunikujące się ze sobą strony. Odbiorca oraz nadawca nie wiedzą, że pomiędzy nimi znajduje się ktoś jeszcze. Osoba znajdująca się pośrodku podszywa się pod każdą ze stron oraz modyfikuje informacje. Cyberprzestępca tworzy dwa klucze szyfrujące, pierwszy z nich służy mu do rozpoczęcia i nawiązania komunikacji z jedną ze stron, drugi służy do zaszyfrowania już odebranej informacji
i przesłania jej dalej do przeciwnej strony. Przeprowadzanie odpowiedzi zwrotnej wygląda analogicznie z szyfrowaniem za pomocą kluczy. Pozwala to na zbieranie potrzebnych mu danych takich jak np. hasła dostępu. Najprostszą metodą jest stworzenie fałszywego bezprzewodowego punktu dostępu do sieci internetowej, który posiada nazwę taką jak ogólnodostępny punkt, na przykład w centrum handlowym. Osoba łącząc się z nieautoryzowanym Wi-Fi i logując do bankowości elektronicznej naraża się na kradzież danych. Pomocniczym narzędziem wykorzystywanym do tego typu ataków jest sniffer (ang. *sniffer* - wąchacz). Jego zadaniem jest analizowanie ruchu sieciowego i przepływających pakietów danych[69].

Następną formą ataku jest SQL (ang. *Structured Query Language*) Injection. Język zapytań SQL jest wykorzystywany w bazach danych do tworzenia ich struktur. W ataku z wykorzystaniem tej metody cyberprzestępca wyszukuje błędów w aplikacjach lub stronach internetowych, które korzystają z baz danych SQL. Dzięki temu może ominąć autoryzację i uwierzytelnianie. Niewłaściwe filtrowanie pakietów danych pozwala na wstrzyknięcie złośliwych zapytań SQL do baz danych. Pozwala to na modyfikowanie, dodawanie, usuwanie i dostęp do wszystkich wrażliwych informacji zawartych w bazie danych[70].

Wymienione formy ataków ukazują szeroki i różnorodny wachlarz możliwości, które posiada cyberprzestępca. Każdy atak posiada swoje charakterystyczne cechy, a ich wykorzystanie zależy od jego pomysłowości i stopnia zaawansowania. Obrona przed nimi może być trudna i skomplikowana. Wymaga ciągłego dostosowywania potrzeb do nowych sytuacji. Ważna przede wszystkim jest wiedza na temat nowo powstałych cyberataków, co pozwoli na odpowiednie przygotowanie do obrony.

Metodologia

[68] Tamże.
[69] https://plblog.kaspersky.com/co-to-jest-atak-man-in-the-middle/186/, dostęp: 07.01.2021 r.
[70] https://www.acunetix.com/websitesecurity/sql-injection/, dostęp: 22.11.2020 r.

Praca pod tytułem „Cyberzagrożenia w aspekcie bezpieczeństwa narodowego" została napisana na podstawie dokładnej analizy materiałów zwartych, artykułów naukowych oraz rzetelnych stron internetowych. Wszystkie wykorzystane materiały odnosiły się do tematu pracy. Zdecydowaną większość wykorzystanego materiału stanowiły artykuły naukowe oraz strony internetowe. Wynika to z małej liczby publikacji zwartych opisujących cyberzagrożenia w kontekście bezpieczeństwa narodowego. Informacje ze źródeł internetowych zostały odpowiednio wyselekcjonowane i sprawdzone przez autora. Ponadto w pracy skupiono się na obowiązujących ustawach, doktrynach i strategiach narodowych. Ich dostępność pozwoliła na dokładne opisanie wybranego zagadnienia, jakim są zagrożenia w sieci teleinformatycznej w odniesieniu do bezpieczeństwa narodowego.

Przegląd literatury

Praca opiera się na artykułach naukowych, źródłach internetowych oraz pozycjach zwartych. Przy gromadzeniu materiałów do dogłębnej analizy wybranego zagadnienia wybrano kilka najbardziej przydatnych pozycji z literatury zwartej, które były związane z tematem pracy. Są to między innymi *Cyberbezpieczeństwo – zarys wykładu* Cezarego Banasińskiego, *Wojna informacyjna i bezpieczeństwo informacji* Dorothy E. Denning oraz *Bezpieczeństwo funkcjonowania w cyberprzestrzeni* Sylwii Wojciechowska-Filipek i Zbigniewa Ciekanowskiego.

Książka *Cyberbezpieczeństwo – zarys wykładu* Cezarego Banasińskiego jako podręcznik akademicki zawiera omówienie strategicznych obszarów cyberbezpieczeństwa, co pozwala na trafne odniesienie się do bezpieczeństwa narodowego i jego cyberprzestrzeni.

Książka *Wojna informacyjna i bezpieczeństwo informacji* autorstwa Dorothy E. Denning przedstawia współczesne zagrożenia dla bezpieczeństwa informacji spowodowane dynamicznym rozwojem sieci i systemów teleinformatycznych. Książka zawiera realne przykłady z życia, które pozwalają lepiej zrozumieć problematykę bezpieczeństwa cyberprzestrzeni w praktyce.

Książka *Bezpieczeństwo funkcjonowania w cyberprzestrzeni* Sylwii Wojciechowska-Filipek i Zbigniewa Ciekanowskiego posłużyła do opisywania zjawisk oszustw komputerowych za pomocą technologii informacyjno-komunikacyjnych oraz cyberterroryzmu oddziałujących na państwo i obywateli. W książce znajdują się ryzyka dla bezpieczeństwa informacji i systemów informacyjnych państwa.

Wnioski

Przeprowadzona analiza literatury z wybranego zagadnienia pozwoliła na dokonanie następujących wniosków:

1. Istnieje wiele różnic pomiędzy definicjami związanymi z cyberprzestrzenią. Jest to spowodowane nieprzerwanym rozwojem techniki i technologii. Różnice pojęciowe mogą stanowić problem dla wspólnego działania, które ma na celu budowę bezpiecznych systemów i sieci teleinformatycznych w cyberprzestrzeni. Brak ujednoliconej terminologii może prowadzić do nieporozumień już w początkowych etapach współpracy krajowej lub międzynarodowej.

2. Bezpieczeństwo jest procesem, który trwa przez cały czas. W cyberprzestrzeni znajduje się wiele zagrożeń dla bezpieczeństwa, nie tylko pojedynczych systemów i sieci teleinformatycznych, ale całej struktury współczesnego państwa. Poszerzający się wpływ techniki oraz technologii powoduje cyfryzację wszystkich sfer życia. Rząd wykorzystuje cyberprzestrzeń do zarządzania krajem. W dbałości o swoje interesy powinien skupić się na bezpieczeństwie danych i informacji, które codziennie przetwarza.

3. Cyberzagrożenia są różnorodne. Cyberprzestępcy wykorzystują swoją wiedzę informatyczną do działania na szkodę państwa i jego obywateli Znajomość zagrożeń pozwala na szybką reakcję i daje możliwość odparcia ataku. Wrogo nastawione państwa mogą posłużyć się cyberatakami w celu destabilizacji kraju. Rząd powinien być przygotowany nie tylko na obronę, ale skuteczną odpowiedź w razie ataku.

Bibliografia

Opracowania zwarte

1. Denning Dorothy E., *Wojna informacyjne i bezpieczeństwo informacji*, Wydawnictwo Naukowo-Techniczne, Warszawa 2002.
2. Husak Z., *Ochrona bezpieczeństwa państwa przed zagrożeniami cybernetycznymi w Unii Europejskiej*, [w:] W. Lis, *Bezpieczeństwo państwa*. Zagadnienia podstawowe, KUL, Lublin 2014.
3. Janczewski R., *Procesy informacyjne w działaniach militarnych w cyberprzestrzeni*, [w:] *Systemy i sieci teleinformatyczne Sił Zbrojnych RP – wielorakie aspekty bezpieczeństwa cyberprzestrzeni*, B. Biernacik, L. Kalman (red.), AON, Warszawa 2016.
4. Kowalewski J., Kowalewski M., *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2017.
5. Modrzejewski Z., *Cyberprzestrzeń środowiskiem walki informacyjnej*, Systemy i sieci teleinformatyczne Sił Zbrojnych Rzeczypospolitej, Akademia Sztuki Wojennej, Warszawa 2016.
6. Pączkowski T., *Słownik Cyberbezpieczeństwa*, Szkoła Policji w Katowicach, Katowice 2017.
7. Siwicki M., *Cyberprzestępczość*, Monografie Prawnicze, C. H. Beck, Warszawa 2013.

8. Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni*, Wydanie II, CeDeWu, Warszawa 2019.

Artykuły

1. Kasprzyk R., M. Paź, Z. Tarapata, *Modelowanie i symulacja cyberzagrożeń typu botnet*, „Symulacja w Badaniach i Rozwoju" nr 6(2)/2015.
2. Milewski J. (2016), *Identyfikacja infrastruktury krytycznej i jej zagrożenia*, „Zeszyty naukowe AON", nr 4 (105).
3. Piątkowski K., *Wojna nowego typu*, „Polska w Europie", nr 3(1)/2002.
4. Szubrycht T., *Współczesne aspekty bezpieczeństwa państwa*, Zeszyty Naukowe Akademii Marynarki Wojennej, nr 4(167)/2006.
5. Żuber M., *Infrastruktura Krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego,* Rocznik Bezpieczeństwa Międzynarodowego, nr 8(2)/2014.

Dokumenty normatywne

1. Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.
2. Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 14 września 2018 r. w sprawie ogłoszenia jednolitego tekstu ustawy - Prawo telekomunikacyjne.
3. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej.
4. Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011.
5. Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016.
6. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2014 roku.
7. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z dnia 12 maja 2020 roku.
8. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.
9. Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.
10. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

Źródła internetowe

1. https://fas.org/irp/doddir/dod/jp1_02.pdf, dostęp: 01.11.2020 r.
2. https://mfiles.pl/pl/index.php/Piramida_Maslowa, dostęp: 01.11.2020 r.

3. https://www.sejm.gov.pl/prawo/konst/polski/kon1.html, dostęp: 01.11.2020 r.
4. https://sjp.pwn.pl/slowniki/bezpieczeństwo.html, dostęp: 01.11.2020 r.
5. https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf, dostęp: 01.11.2020 r.
6. https://sjp.pwn.pl/slowniki/przestępczość.html, dostęp: 01.11.2020 r.
7. https://sjp.pwn.pl/slowniki/haker.html, dostęp: 13.01.2021 r.
8. https://rcb.gov.pl/wp-content/uploads/Dokument-Główny-1.pdf, dostęp: 03.11.2020 r.
9. https://rcb.gov.pl/wp-content/uploads/Standardy-służące-zapewnieniu-sprawnego funkcjonowania-infrastruktury-krytycznej-–-dobre-praktyki-i-rekomendacje.pdf, dostęp: 01.11.2020 r.
10. https://www.nask.pl/pl/aktualnosci/oferta/ofertatelekomunikacyjn/bezpieczenstwo/2662,DDoS-Attack-Protection.html, dostęp: 06.01.2021 r.
11. https://rcb.gov.pl/terroryzm-wciaz-zagraza-unii-europejskiej/, dostęp: 06.01.2021 r.
12. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf, dostęp: 19.01.2021 r.
13. https://niebezpiecznik.pl/post/kolejny-grozny-globalny-atak-tym-razem-ransomware-petya-ofiary-sa-takze-w-polsce/, dostęp: 07.01.2021 r.
14. https://www.avast.com/pl-pl/c-petya, dostęp: 20.11.2020 r.
15. https://www.cert.pl/news/single/wannacry-ransomware/, dostęp: dnia 20.11.2020 r.
16. https://www.bbc.com/news/world-asia-41816958, dostęp: dnia 07.01.2021 r.
17. https://www.benchmark.pl/aktualnosci/cyberprzestepcy-podszywaja-sie-pod-poczte-polska.html, dostęp: 20.11.2020 r.
18. https://www.who.int/about/communications/cyber-security, dostęp: 07.01.2021 r.
19. https://plblog.kaspersky.com/co-to-jest-atak-man-in-the-middle/186/, dostęp: 07.01.2021 r.
20. https://www.acunetix.com/websitesecurity/sql-injection/, dostęp: 22.11.2020 r.

bsm. pchor Jakub ZAMBROWSKI

INCYDENTY W CYBERPRZESTRZENI

Streszczenie

Postęp technologiczny oraz rozwój sieci telekomunikacyjnej przyniosły ze sobą wiele zalet i ułatwień, ale również mnóstwo niebezpieczeństw. Nieodzownym elementem podczas użytkowania systemów teleinformatycznych stało się cyberbezpieczeństwo. Wszelkie działania związane z tym pojęciem okazały się niezbędne, aby chronić się i zapobiegać przed cyberprzestępstwami oraz wymierzonymi cyberatakami. Pomimo coraz to bardziej zaawansowanych zabezpieczeń, powstające złośliwe programy oraz techniki szkodliwego działania, potrafią wyrządzić znaczne szkody w strukturze systemu teleinformatycznego. Wiele tego typu działań organizowanych jest przez rządy państw, co określane jest jako wojna informacyjna.

Słowa kluczowe:
cyberbezpieczeństwo, cyberprzestrzeń, cyberprzestępstwo, system teleinformatyczny, cyberatak, cyberincydent, malware, Stuxnet, wojna informacyjna.

Abstract

Technological progress and development of telecommunication network have brought many advantages and facilitations, but also a lot of dangers. Cybersecurity has become an indispensable element in the use of ICT systems. All the activities related to this domain turned out to be necessary to protect form cybercrimes and targeted cyberattacks and prevent them. Despite more and more advanced security measures, all new malicious software and techniques of penetrating ICT systems can cause critical damage to their structure. Some of this kind of activities are performed by governments, which is defined as information warfare.

Keywords:
cybersecurity, cyberspace, cybercrime, ICT system, cyberattack, cyber incident, malware, Stuxnet, information warfare.

Wstęp

Tematyka incydentów w cyberprzestrzeni jest szczególnie warta uwagi, ze względu na wszechobecność technologii informatycznej, która jest podstawą istnienia cyberprzestrzeni w dzisiejszych czasach. Wartym zaznaczenia jest fakt, że w obrębie urządzeń bazujących na tej technologii, coraz częściej przetwarzane są wrażliwe dla nas dane. Pomimo korzyści, jakie niesie ze sobą rozwój technologiczny oraz informatyzacja kolejnych aspektów naszego życia, zauważamy nieznane dotąd zagrożenia, które czyhają na nas w cyberprzestrzeni. Incydenty, które mogą dotknąć systemów teleinformatycznych, zależnie od ich rodzaju, mogą ze sobą nieść fatalne skutki. Z uwagi na ten fakt, coraz bardziej istotnym pojęciem staje się cyberbezpieczeństwo, które jest nieodzownym elementem funkcjonowania społeczeństwa informacyjnego. Ze względu na stały rozwój cyberprzestępczości, poruszenie problematyki incydentów w cyberprzestrzeni, niewątpliwie wskazuje różnorodność zagrożeń występujących w jej obrębie.

Cyberprzestrzeń jako wymiar fizyczny, wirtualny oraz ludzki

Postęp technologiczny i powstawanie coraz to nowszych, wydajniejszych i bardziej zaawansowanych technologii komputerowych sprawiło, że zaczęto wprowadzać je do wielu nowych obszarów życia i tworzyć urządzenia, które stawały się ogniwami systemów teleinformatycznych. Oczywiście rozwój tego typu niósł ze sobą korzyści, ale także nieznane dotąd zagrożenia, bowiem każda nowa technologia posiada zarówno zalety, jak i wady[1]. Powszechność urządzeń elektronicznych, zwłaszcza tych z dostępem do sieci telekomunikacyjnych, zaczęła kształtować społeczeństwo informacyjne. W taki sposób w pewnym momencie zaczęto wyodrębniać cyberprzestrzeń, która choć wiadomo czego dotyczy, to ciężko precyzyjnie zdefiniować i określić jej elementy ze względu na ich mnogość.

Najbardziej aktualny dokument wydany w RP, który dotyczy opisywanego pojęcia to Krajowe Ramy Polityki Cyberbezpieczeństwa ma lata 2017-2022. Zgodnie z nim *cyberprzestrzeń oznacza przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*[2]. Analizując to pojęcie zauważamy, że ujęte są w nim dwa elementy składowe – *systemy teleinformatyczne* oraz (ich) *relacje z użytkownikami.* Jednakże, można jeszcze bardziej sprecyzować i wyodrębnić spośród tych dwóch elementów pomniejsze ich składniki

[1] P. Dela, *Wstęp do teorii walki w cyberprzestrzeni,* [w:] *Rocznik Bezpieczeństwa Morskiego. Przestępczość teleinformatyczna 2019,* red. J. Kosiński, G. Krasnodębski, Gdynia 2020, s. 14.
[2] *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022,* Ministerstwo Cyfryzacji, Warszawa 2017, s. 28,

Systemy teleinformatyczne definiuje Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne[3] oraz Ustawa o świadczeniu usług drogą elektroniczną[4]. W powyższych aktach prawnych definiuje się je jako *zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego*. Widzimy więc, że Systemy teleinformatyczne można rozdzielić na urządzenia, oprogramowanie oraz sieci telekomunikacyjne.

Według Głównego Urzędu Statystycznego poprzez urządzenia informatyczne rozumie się *maszyny przenośne do automatycznego przetwarzania danych o masie do 10 kg*[5]. Jest to niewątpliwie mocno rzeczowy opis. W sposób bardziej zrozumiały urządzenia informatyczne można określić jako sprzęt w obrębie systemu teleinformatycznego w postaci urządzeń tworzących i obsługujących system oraz urządzeń końcowych, które pozwalają korzystać z jego funkcji.

Z kolei *oprogramowanie* można rozumieć i definiować na wiele sposobów, ale w kontekście systemu teleinformatycznego można je określić mianem całości informacji w postaci instrukcji (kodu źródłowego), zaimplementowanych interfejsów i zintegrowanych danych przeznaczonych dla sprzętu do realizacji wyznaczonych celów, które razem mają za zadanie umożliwienie funkcjonowania systemu teleinformatycznego w pożądany sposób.
Definicja sieci telekomunikacyjnej według Ustawy z dnia 16 lipca 2004 r. o Prawie Telekomunikacyjnym brzmi następująco: *systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju*[6]. W skrócie jest to połączenie systemów i urządzeń, umożliwiających przesyłanie danych w dowolny sposób, przewodowy lub bezprzewodowy.
Sama relacja systemu teleinformatycznego z użytkownikami to oczywiście wykorzystanie funkcjonalności tego systemu przez człowieka. Jednakże, gdy mówimy o wymiarze ludzkim cyberprzestrzeni należy tu także pamiętać o dużo bardziej istotnej roli osób zajmujących się tworzeniem i administracją danego systemu.

Po dokładnej analizie i rozłożeniu pojęcia cyberprzestrzeni na czynniki pierwsze okazuje się, że w zasadzie, możemy podzielić cyberprzestrzeń

[3] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. 2005 nr 64 poz. 565).
[4] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. 2002 nr 144 poz. 1204),
[5] *Sprawozdanie o wykorzystaniu technologii informacyjno-telekomunikacyjnych w przedsiębiorstwach*, Główny Urząd Statystyczny, Warszawa 2014, s. 3.
[6] Art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. 2004 nr 171 poz. 1800),

na trzech płaszczyznach: wymiar fizyczny – jako połączenie sprzętu i oprogramowania systemu teleinformatycznego, wymiar wirtualny – jako sieć telekomunikacyjna łącząca poszczególne ogniwa systemu teleinformatycznego, oraz wymiar ludzki – jako komponent niezbędny do powstania i funkcjonowania systemu teleinformatycznego oraz element wykorzystujący jego funkcje i możliwości.

Cyberbezpieczeństwo i jego znaczenie

Wraz z rozwojem technologii komputerowych, który nastąpił na przełomie ostatnich kilkudziesięciu lat, ludzkość stawała się coraz to bardziej uzależniona od rozwiązań teleinformatycznych. Systemy teleinformatyczne zaczęto wdrażać do kolejnych dziedzin życia. Warto tu wskazać przykład banków, które już w 1960 r. zaprezentowały pierwszy bankomat działający na podstawie technologii komputerowej, a już w 1973 r. pojawiła się pierwsza oferta płatności elektronicznych. Było to możliwe głownie dzięki powstaniu rozległej sieci w 1969 r. – ARPANET, dziś dużo bardziej rozwiniętej i globalnej, potocznie nazywanej Internetem. Niewątpliwie, to właśnie dzięki niemu rozwój wcześniej wspomnianych technologii komputerowych stał się tak szybki.

Występowanie systemów teleinformatycznych w szczególnie ważnych obszarach, jak chociażby wyżej przedstawiona bankowość, obligowało ich twórców to zapewnienia im odpowiednich zabezpieczeń, zarówno sprzętowych, programowych jak i tych odnoszących się do pracowników. W ten sposób z czasem wyłoniło się pojęcie cyberbezpieczeństwa. Pomimo, że w dokumentach wydawanych przez instytucje RP pojęcie cyberbezpieczeństwa pojawiło się dopiero w 2009 r. w Rządowym Programie Ochrony Cyberprzestrzeni RP na lata 2009-2011, to w angielskim słowniku i tamtejszej branży IT było znane już w 1989 r.[7].

Współcześnie, gdy niemalże każdy człowiek i każdy system funkcjonują w sferze cyberprzestrzeni, kluczowym elementem funkcjonowania w jej obrębie stało się cyberbezpieczeństwo. Oba te pojęcia stały się obiektem zainteresowań Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji oraz organów odpowiedzialnych za cyberprzestrzeń w Rzeczypospolitej Polskiej. Zarówno ENISA jak i instytucje rządowe stale opracowują dokumenty mające wyznaczać kierunek rozwoju i ustalać kwestie istotne dla cyberbezpieczeństwa, odpowiednio Unii Europejskiej i Polski, zwane zazwyczaj Strategiami Cyberbezpieczeństwa. Najaktualniejszym dokumentem tego typu w przypadku struktur Unii Europejskiej jest *Wspólny Komunikat Parlamentu Europejskiego i Rady – Strategia UE w zakresie cyberbezpieczeństwa na cyfrową*

[7] https://io9.gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487, dostęp: 20.02.2021 r.

dekadę[8], a w przypadku Rzeczypospolitej Polskiej są to *Krajowe Ramy Polityki Cyberbezpieczeństwa RO na lata 2017-2022*[9].

Cyberprzestępstwo jako naruszenie cyberbezpieczeństwa

Rozwój technologii komputerowych i informacyjnych, to nie tylko szansa na lepsze i łatwiejsze życie dla każdego z nas. Niestety, to także okazja dla osób, których zamiary są nie do końca zgodne z prawem.

Pomimo faktu, że ilość cyberprzestępstw z roku na rok wzrasta, to brak jest w polskim prawie definicji tego zjawiska. Niemniej jednak, wyjaśnienie tego pojęcia możemy znaleźć w Rządowym Programie Ochrony Cyberprzestrzeni RP na lata 2011-2016 i brzmi ono następująco: *Cyberprzestępstwo – czyn zabroniony popełniony w obszarze cyberprzestrzeni*[10]. Pomimo, że jest to definicja dosyć krótka, to w odpowiedni sposób obrazuje ona omawianą problematykę.

Jak więc wynika z powyższej definicji, cyberprzestępstwo należy rozumieć jako przestępstwo popełnione w obrębie cyberprzestrzeni, a więc szeroko pojętego obszaru, bowiem można do niej zaliczyć każdy jej element, od zwykłego komputera czy smartfona, do złożonych systemów teleinformatycznych przetwarzających dane o wysokich klauzulach i ludzi je obsługujących. Pokazuje to, jak złożonym i ciężkim do jednoznacznego opisania pojęciem jest cyberprzestępstwo.

Tym samym mówimy raczej o zjawisku niż konkretnym działaniu. Chodzi tu oczywiście o popełnianie przestępstw, a dokładniej ujmując cyberprzestępstw. Pojęcie cyberprzestępczości może być interpretowane na wiele sposobów.

Cyberprzestępczość może być rozumiana w wąskim znaczeniu (przestępczość komputerowa) obejmującym wszelkie nielegalne zachowania prowadzone za pomocą działań elektronicznych mających na celu naruszenie bezpieczeństwa systemów komputerowych i przetwarzanych w nich danych. Cyberprzestępczość może być również rozumiana w szerokim znaczeniu (przestępczość związana z komputerami) – jako każde bezprawne zachowanie popełnione poprzez lub w związku z systemem lub siecią komputerową.

Najlepsza interpretacja pojęcia cyberprzestępczości[11] opiera się jednak na Konwencji Rady Europy z dnia 23 listopada 2001r. o cyberprzestępczości[12].

---

[8] *Wspólny Komunikat Parlamentu Europejskiego i Rady – Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę,* Komisja europejska, Bruksela 2020.
[9] *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022,* Ministerstwo Cyfryzacji, Warszawa 2017.
[10] *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016,* Departament Ewidencji Państwowych i Teleinformatyki MSWiA, Warszawa 2010, s. 6 pkt 3.
[11] J. Kosiński, G. Krasnodębski, *Cybercrime predicting in the light of police statistics*, [w] H. Jahankhani, A. Jamal, S. Lawson, *Cybersecurity, Privacy and Freedom Protection in the Connected World*, Springer, Cham 2021.
[12] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, dostęp: 21.02.2021 r.

Konwencja ta zawiera definicje czterech rodzajów przestępstw komputerowych:

1. przestępstwa przeciwko poufności, integralności i dostępności danych i systemów komputerowych,
2. przestępstwa fałszerstwa i oszustwa komputerowego,
3. przestępstwa związane z pornografią dziecięcą,
4. przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych.

Konwencję uzupełnia także Protokół dodatkowy do Konwencji dotyczący czynów przestępczych o charakterze rasistowskim lub ksenofobicznym popełnianych przy użyciu systemów komputerowych[13].

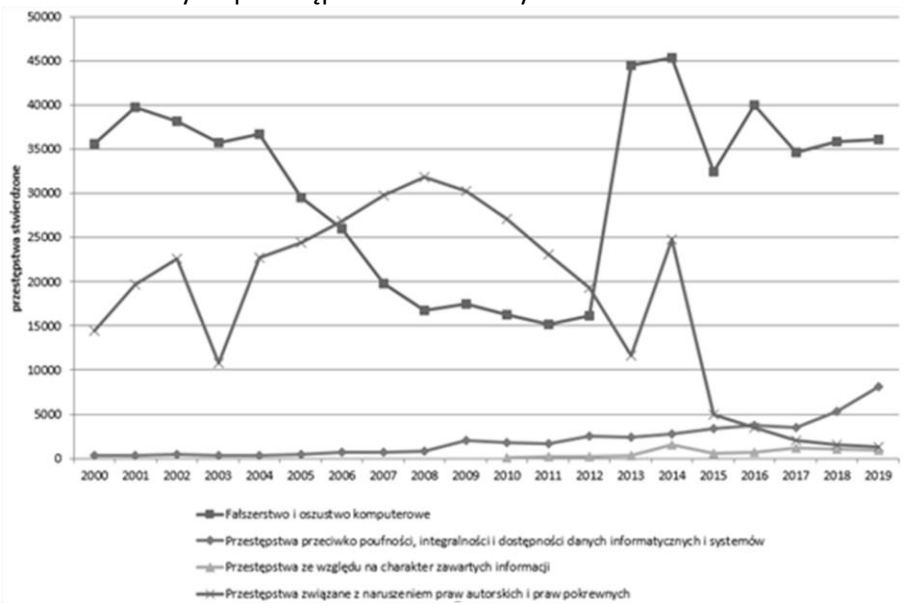
Problem cyberprzestępczości jest dosyć poważny, zwłaszcza ze względu na to, że ilość popełnianych cyberprzestępstw wciąż rośnie. Dowodem na to może być statystyka prowadzona przez CSIRT GOV[14]. W 2019 roku wymieniony zespół reagowania na incydentu odnotował 226 914 zgłoszeń o incydentach teleinformatycznych, co w stosunku do ubiegłego roku, kiedy zanotowano jedynie 31 865 zgłoszeń, świadczy o niemal siedmiokrotnym wzroście. Po weryfikacji liczba ta oczywiście zmalała i wyniosła 12 405 incydentów w 2019 roku, niemniej jest to dwukrotny wzrost w porównaniu do 2018, gdzie naruszeń bezpieczeństwa teleinformatycznego było jedynie 6 236. Niestety, nie jest to statystyka, którą możemy się w pełni sugerować, bowiem jest ona oparta wyłącznie o obserwację incydentów dotyczących systemów teleinformatycznych centralnych organów administracji publicznej i rządowej oraz operatorów infrastruktury krytycznej. Dużo lepiej aktualny stan bezpieczeństwa cyberprzestrzeni pokazują dane statystyczne Policji, które można uzyskać w trybie zapytania o informację publiczną. Na podstawie tak pozyskanych danych można stworzyć zestawienie liczby cyberprzestępstw w kategoriach Konwencji Rady Europy o cyberprzestępczości, które zostały rzeczywiście stwierdzone. Statystyka czterech wybranych rodzajów cyberprzestępstw stwierdzonych w latach 2000-2019 została przedstawiona na wykresie 10.1.

[13] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189, dostęp: 21.02.2021 r.

[14] https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/969,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2019-roku.html, dostęp: 21.02.2021 r.

Wykres 10.1

Liczba cyberprzestępstw stwierdzonych w latach 2000-2019



Źródło: Opracowanie własne na podstawie danych Komendy Głównej Policji[15].

Jak możemy zauważyć na powyższym wykresie, pomimo stosunkowo małego udziału przestępstw przeciwko poufności, integralności i dostępności danych informatycznych i systemów w przedstawionej statystyce, wzrost ich ilości na przestrzeni ostatnich lat jest proporcjonalnie najwyższy.

Incydent jako wykorzystanie podatności systemu teleinformatycznego

Mówiąc o incydencie w cyberprzestrzeni, należałoby przedstawić wyjaśnienie tego pojęcia w aspekcie właśnie tego środowiska. Najprostszą definicją, jaką możemy spotkać w literaturze jest ta, która znajduje się w Ustawie o Krajowym Systemie Cyberbezpieczeństwa i brzmi ona następująco: *incydent to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo*[16]. Wyjaśnienie to jak najbardziej można uznać za poprawne, niestety dosyć ogólne. Niekompletność usprawiedliwiają jednak kolejne definicje, które znajdują się w tym dokumencie. Autorzy opisują *incydent krytyczny, incydent*

[15] Dane pozyskane i udostępnione przez dr hab. Jerzego Kosińskiego.
[16] Art. 2 pkt 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2020 poz. 1560), https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf, dostęp: 23.02.2021 r.

poważny, incydent istotny oraz incydent w podmiocie publicznym[17], a wynika to z potrzeb scharakteryzowania Krajowego Systemu Cyberbezpieczeństwa.

Jeżeli chcielibyśmy bardziej szczegółowo i konkretnie zdefiniować incydent w cyberprzestrzeni, należałoby spojrzeć z perspektywy każdego jej wymiaru – fizycznego, wirtualnego oraz ludzkiego. Oczywiście, większość incydentów, które są omawiane zawiera się w pierwszych dwóch sferach i to na nich należałoby się skupić. Warto by także w pewien sposób rozdzielić ich przyczyny, a w zasadzie wektory ich występowania. Jeżeli chodzi o skutki incydentów, to możemy określić ich rozległość i stopień zaawansowania, a także zwrócić uwagę na naruszanie atrybutów bezpieczeństwa. Podsumowując to wszystko, można stworzyć dosyć kompletną definicję.

Incydent w cyberprzestrzeni jest więc to niepożądane zdarzenie w obrębie wymiaru fizycznego, wirtualnego lub ludzkiego cyberprzestrzeni, zaistniałe w sposób samoistny lub celowy, które narusza lub może naruszyć w mniejszym lub większym stopniu cyberbezpieczeństwo systemu teleinformatycznego, poprzez wyeliminowanie jednego lub kilku jego atrybutów bezpieczeństwa i zakłócając jego działanie.

Mówiąc o atrybutach bezpieczeństwa należałoby przynajmniej wymienić, które z mnich mogą dotyczyć systemów teleinformatycznych. Można tego dokonać na podstawie normy ISO 13335 która rozróżnia sześć podstawowych atrybutów: integralność, poufność, dostępność, autentyczność, rozliczalność oraz niezawodność[18]. Ze względu na to, o jakim systemie jest mowa i co w nim jest kluczowym elementem, możemy wyróżniać inne atrybuty. Chcąc w sposób stosunkowo kompletny je scharakteryzować opisując te najważniejsze należy również wziąć pod uwagę niezaprzeczalność.

Z kolei chcąc scharakteryzować działania, których efektem jest incydent, należy zwrócić uwagę na kilka terminów, które są bezpośrednio z nim powiązane. Mowa tu o pojęciach takich jak zagrożenie, zasoby wykorzystane do jego realizacji, podatność oraz zabezpieczenia. O ile zabezpieczenia nie muszą być brane pod uwagę w procesie jakim jest realizacja wyżej wspomnianego zagrożenia, bo może ich po prostu nie być, to pozostałetrzy elementy są kluczowe. Schemat opisywanego działania przedstawiony został na rysunku 10.1.

[17] Art. 2 pkt 6-9 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2020 poz. 1560).

[18] *Guidelines for the Management of IT Security* (ISO/IEC 13335-1:2004).

Źródło: Opracowanie własne na podstawie K. Liderman, *Bezpieczeństwo Informacyjne. Nowe Wyzwania, Rozdział 1.2.1,* PWN, Warszawa 2017[19].

Rysunek 10.1. Realizacja zagrożenia

Aby więc dane zagrożenie zostało zrealizowane i powstał incydent, potrzebne są trzy czynniki. Tym, bez którego byłoby to niemożliwe jest podatność, która oczywiście może być zabezpieczona, ale nie zawsze tak jest. Dodatkowo wystąpić musi zagrożenie i zasoby, dzięki którym zostanie ono zrealizowane.

Szczególnie ważnym pojęciem w kontekście utrzymania poziomu cyberbezpieczeństwa jest obsługa incydentu. Rozumie się przez to wszystkie czynności, które wykonywane są w stosunku do niego, włącznie z jego wykryciem. Można rozróżnić cztery etapy takich działań, które zostały przedstawione na rysunku 10.2.

Warto tu zwrócić uwagę, że etap pierwszy oraz czwarty są w zasadzie ciągłymi procesami, bowiem zarówno wykrywanie incydentów, jak i zapobieganie im musi mieć miejsce bez względu na to, czy aktualnie występuje jakieś zagrożenie. Mówiąc o obsłudze incydentu, należałoby określić kto się tym zajmuje. Jest to dokładnie opisane w czwartym artykule Ustawa o Krajowym Systemie Cyberbezpieczeństwa[20], gdzie wymienione są jego elementy. Należy tu zwrócić uwagę na fakt, że każda usługa kluczowa powinna posiadać zespół reagowania na niepożądane zdarzenia, w związku z tym w Polsce istnieje kilkaset takich komórek. Głównymi podmiotami zajmującymi się incydentami w cyberprzestrzeni są Zespoły reagowania na incydenty Bezpieczeństwa Komputerowego: CSIRT GOV, CSIRT MON oraz CSIRT NASK.

[19] K. Liderman, *Bezpieczeństwo Informacyjne Nowe Wyzwania*, PWN, Warszawa 2017.
[20] Art. 4. ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2020 poz. 1560), https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf, dostęp: 23.02.2021 r.

Źródło: Opracowanie własne na podstawie K. Liderman, *Bezpieczeństwo Informacyjne. wNowe Wyzwania, Rozdział 1.2.4.1,* PWN, Warszawa 2017[21].

Rysunek 10.2. Etapy obsługi incydentów

Aby móc określić, jak należy postępować w przypadku wystąpienia niepożądanego zdarzenia, zwanego inaczej incydentem lub zabezpieczyć się przed nim, należy najpierw sprecyzować, co nam tak naprawdę zagraża lub ewentualnie może zagrozić. Niezbędna jest więc identyfikacja danego przypadku i przypisanie go do jakiejś grupy lub kategorii. Chcąc przeprowadzić taki podział, konieczne jest posiadanie lub opracowanie jakiegoś wzorca, na podstawie którego będzie to dokonywane. Należy tu wziąć pod uwagę wiele czynników, takich jak wektor ataku, czy umyślność działania, jednakże najważniejsze jest, aby jasno stwierdzić do czego w zasadzie doszło i z jakim incydentem mieliśmy lub możemy mieć do czynienia. Co więcej, świadomość tego, że dany typ incydentu istnieje i może on dotknąć organizacji, systemu teleinformatycznego czy pojedynczej stacji roboczej, której cyberbezpieczeństwo jest dla nas istotne.

Będąc niewielką organizacją lub administratorem jakiegoś systemu teleinformatycznego trudno samodzielnie opracować zestawienie zagrożeń, a wynajęcie zespołu, który zrobi to za nas może być zbyt kosztowne. Z rozwiązaniem przychodzą powszechnie dostępne metody ich podziału, które mogą ułatwić stworzenie takiego zbioru. Należą do nich m. in. Metoda STRIDE, metoda A:F, czy podział wg. MITRE ATT&CK.

Metody działania sprawców cybeincydentów

Aby móc dobrze chronić się przed zagrożeniami, należy poznać nie tylko rodzaje, ale także źródła ataków, a dokładnie motywy ich sprawców. Na wstępie należy zaznaczyć, że do części incydentów nie dochodzi z powodu

[21] K. Liderman, *Bezpieczeństwo Informacyjne Nowe Wyzwania*, PWN, Warszawa 2017.

działania człowieka. Są to na przykład awarie sprzętu, błędy oprogramowania czy katastrofy naturalne. Skupiając się jednak na motywach działania sprawców incydentów, to wyodrębnia się pośród nich dwie grupy. Pierwsza to osoby, które przypadkowo lub z powodu braku odpowiedniej wiedzy i umiejętności spowodowały incydent. Drugą grupą są cyberprzestępcy, których zamierzone działania są często na tyle zaawansowane, że wywołują znaczne szkody w systemach teleinformatycznych.

Ciekawym ich podziałem jest rozdzielenie tej grupy na tzw. białe, czarne oraz szare kapelusze. Na wstępie należy jednak zaznaczyć, że nie chodzi o kolor nakrycia głowy, a przyjęte nazewnictwo, które określa hakerów. Pojęcia te pochodzą ze starych filmów typu western, gdzie źli bohaterowie nosili czarne kapelusze, a dobrzy białe.

Hakerami można nazwać osoby, które znajdują słabe elementy w systemach komputerowych lub sieciach i je wykorzystują, tym samym, zdobywając do nich dostęp. Zazwyczaj są doświadczonymi programistami z zaawansowaną wiedzą na temat bezpieczeństwa komputerowego co ułatwia im operowanie w wirtualnym środowisku[22]. To do której grupy przypiszemy hakera, określają motywacje, którymi się kieruje, a dokładnie czy jego działania łamią prawo.

Jak można się domyśleć, najbardziej szkodliwi i niebezpieczni są hakerzy zwani czarnymi kapeluszami. W jej obrębie znajdziemy osoby o zarówno niskich, jak i wysokich umiejętnościach. To co ich określa to działanie na czyjąś niekorzyść, często wbrew przepisom. Właśnie tej grupie przypisujemy pisanie kodów szkodliwego oprogramowania, które później pozwala uzyskać nieuprawniony dostęp do systemów komputerowych lub wyrządzić w nich inne szkody. Takie osoby zazwyczaj działają, aby osiągnąć korzyść finansową, choć zdarza się, że są zaangażowani w cyberszpiegostwo, propagowanie tzw. fake news, czyli fałszywych wiadomości czy branie udziału z zorganizowanych i zmasowanych atakach hakerskich, niekiedy jedynie dla własnej satysfakcji.

Kompletnie odmienną grupą są hakerzy zwani białymi kapeluszami. Wykorzystują oni swoje umiejętności w dobrym i słusznym celu i to dlatego zwani są również etycznymi hakerami. Tacy ludzie często zatrudniani są przez firmy jako specjaliści od bezpieczeństwa komputerowego, których zadaniem jest testowanie odporności systemów na ataki i szukanie luk w ich zabezpieczeniach. Metody działania białych kapeluszy są bardzo często zbliżone do tych, którymi posługują się szkodliwi hakerzy, jednak istnieje pewien wyjątek. Zanim zaczną działać, uzyskują oni zgodę lub zlecenie właściciela systemu na konkretne czynności, więc są one w stu procentach legalne. Warto tu zaznaczyć, że taki rodzaj hackingu jest pożądany, a co więcej, istnieje wiele szkoleń i kursów z zakresu testów penetracyjnych.

[22] https://www.guru99.com/what-is-hacking-an-introduction.html, dostęp: 24.02.2021 r.

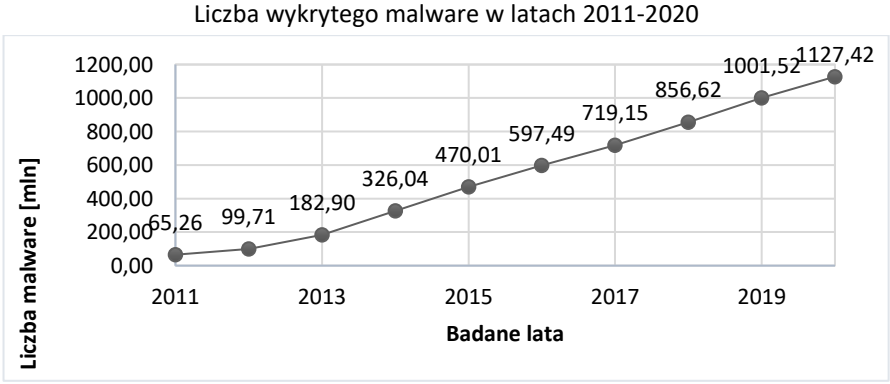
Jak wszędzie, pomiędzy czymś dobrym i złym znajduje się coś pośredniego. Tak jest też w tym przypadku. Szare kapelusze to w zasadzie połączenie dwóch wyżej opisanych typów hakerów. Tak jak czarni, szukają podatności w zabezpieczeniach systemów komputerowych bez pozwolenia ani wiedzy właściciela, jednak, gdy znajdą jakąś lukę informują o niej właściciela. W przypadku braku odpowiedzi z jego strony, taki haker udostępnia wykrytą podatność zwaną exploitem do sieci. Pomimo, że takie działania nie wyrządzają bezpośrednio szkody, to są one również nielegalne, z powodu braku zgody posiadacza systemu na takie działania.

Malware – najbardziej powszechne cyberzagrożenie

Malware (ang. *malicious software*), czyli złośliwe lub szkodliwe oprogramowanie to najbardziej powszechne zagrożenie, jakie może dotknąć nie tylko systemów komputerowych, ale również wszystkich innych urządzeń, które posiadają jakiś system, jak chociażby nowoczesne sprzęty gospodarstwa domowego. Aktualnie istnieje wiele rodzajów malware. Różnią się przeznaczeniem, czyli tym, jaki system lub urządzenie mają zainfekować, sposobem działania, czyli jak kod szkodliwego oprogramowania jest wykonywany i rozprzestrzeniany, a także efektem, czyli co powoduje. Istnieje wiele sposobów ochrony przed tego typu zagrożeniem, od fizycznych, które blokują iniekcję takiego oprogramowania, przez programowe, które próbują wykryć malware w obrębie systemu i go wyeliminować po takie, które polegają na zwykłej ostrożności użytkownika systemu czy urządzenia.

Pomimo, że zagrożenie to znane jest już od lat siedemdziesiątych ubiegłego wieku, to znaczny wzrost ilości zainfekowanych urządzeń nastąpił na przełomie ostatniego dziesięciolecia. Wraz z postępującą informatyzacją, ilość wykrytych przypadków zainfekowania systemów komputerowych wzrosła w okresie lat 2011-2020 niemal dwudziestokrotnie. Zjawisko te przedstawione jest na wykresie 10.2.

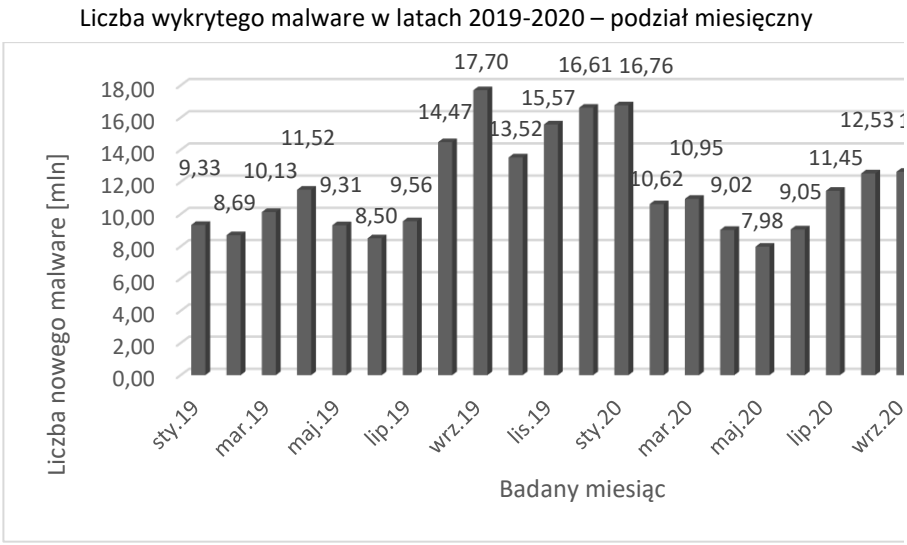
Wykres 10.2.



Źródło: Opracowanie własne na podstawie danych zebranych przez AV-TEST[23].

Pomimo wdrażania coraz nowszych i bardziej skomplikowanych zabezpieczeń oraz większej świadomości użytkowników systemów komputerowych, na przestrzeni ostatnich dwóch lat, tj. 2019-2020, liczba infekcji nie wykazuje tendencji spadkowych, a odnotowywany wzrost jest stały. Obrazuje to wykres 10.3.

Wykres 10.3.



Źródło: Opracowanie własne na podstawie danych zebranych przez AV-TEST.

Można przez to jasno stwierdzić, że stale wzrastający poziom bezpieczeństwa systemów komputerowych oraz wiedzy użytkowników cyberprzestrzeni na temat cyberzagrożeń nie wpływa w zauważalny sposób na obniżenie średniej ilości wykrytych infekcji systemów przez malware, co świadczy o równoległym rozwoju i powstawaniu bardziej skomplikowanych i groźnych wersji szkodliwego oprogramowania. Warto zaznaczyć fakt, że złośliwe programy odgrywają znaczną rolę w większości cyberprzestępstw związanych z naruszeniem bezpieczeństwa danych[24]. Choć nie wszystkie malware są na to ukierunkowane to cześć z nich wykrada nasze dane z zainfekowanych jednostek.

Istnieje wiele źródeł, poprzez które system może zostać zainfekowany szkodliwym oprogramowaniem. Chcąc podzielić je na grupy, można wyodrębnić tu Internet, jako sieć wielu stron www, aplikacje, sieci telekomunikacyjne, oraz fizyczne dostarczenie malware do urządzenia. Przedstawiona kolejność

[23] https://www.av-test.org/en/statistics/malware/, dostęp: 24.02.2021 r.
[24] J. Kosiński, *Paradygmaty cyberprzestępczości,* Difin, Warszawa 2015, s. 94.

nie jest jednak przypadkowa. To właśnie w obrębie stron internetowych, a konkretnie zawartych na nich plików, które mogą zawierać w sobie złośliwe programy, czy odnośników przekierowujących na niebezpieczne adresy, istnieje najwięcej zagrożeń. W obrębie tej kategorii warto wyróżnić tzw. phishing. Są to wiadomości, które podszywają się pod prawdziwe źródła, aby nakłonić odbiorcę do kliknięcia w załączony link, czy wykonania innego działania mającego narazić go na straty. Pod takimi linkami często kryją się różnego rodzaju malware. Również w przypadku aplikacji występuje wiele możliwości infekcji malware. Mogą one zawierać w sobie kody złośliwego oprogramowania lub same w sobie być tzw. riskware. O ile korzystamy z zaufanych i bezpiecznych sieci, to ryzyko wystąpienie zagrożenia i infekcji szkodliwymi programami jest niewielkie. Co innego, gdy korzystamy np. z otwartych hotspotów z dostępem do Internetu. Za ich pomocą sprawca może w łatwy sposób przesłać na nasze urządzenia malware. Jeżeli chodzi o fizyczny dostęp to jest to nic innego jak zainfekowanie urządzenia poprzez podłączenie do niego nośnika danych ze złośliwym oprogramowaniem.

W obliczu jakiegokolwiek zagrożenia, poszukiwane jest rozwiązanie, które pozwoli go uniknąć. Również w wypadku malware istnieją sposoby ochrony i zapobiegania przed infekcją urządzenia szkodliwym oprogramowaniem. Choć opcji jest wiele, nie istnieje rozwiązanie, które pozwoliłoby uniknąć wniknięcia wirusa do systemu. Oczywiście, aby móc zdefiniować metody ochrony przed malware należy znać zarówno jego rodzaje i sposoby ich działania, jak i potencjalne źródła zagrożeń.

Niewątpliwie, najbardziej powszechną i prostą w zastosowaniu metodą jest użycie oprogramowania antywirusowego, nie zapewnia ona jednak pełnej i gwarantowanej ochrony przed malware. Istnieje wiele rozwiązań tego typu, zarówno darmowych jak i takich, które wymagają zakupienia licencji. Tego typu programy opierają się o ciągle aktualizowane bazy danych znanych przypadków malware, które umożliwiają wykrycie złośliwych programów. Obligatoryjnym elementem jest również firewall, czyli zapora sieciowa, która blokuje niechciane połączenia w obrębie sieci zarówno prywatnej, jak i publicznej. W dodatku wiele antywirusów zawiera w sobie tzw. WebAdvisory, czyli funkcje, które ostrzegają użytkownika o niebezpiecznych witrynach, łączach oraz plikach w obrębie Internetu. Część rozwiązań oferuje również filtry spamu i podejrzanych wiadomości dla skrzynek pocztowych email.

Szereg pozostałych rozwiązań można w zasadzie prosto opisać jako dobre praktyki. Są to wzorce zachowań w postaci nawyków i świadomego wybierania i korzystania z dostępnych treści, zwłaszcza w obrębie Internetu. Mogłoby się wydawać, że umiejętność poruszania się w sieci i odpowiedniej obsługi systemu jest drugorzędna, jednak są to kluczowe elementy w trzymaniu bezpieczeństwa i ochrony przed malware. W obrębie tej kategorii możemy wyróżnić wiele praktyk, takich jak stałe aktualizowanie systemu operacyjnego oraz oprogramowania, które użytkujemy, czy korzystanie z konta użytkownika, które ma mniejsze uprawnienie niż profil administratora w systemie. Z

kolei przy korzystaniu z Internetu warto dwa razy sprawdzić link, w który mamy zamiar wejść, aby uniknąć przekierowania na niebezpieczną stronę. Ważne jest, aby podchodzić z dystansem do reklam, jakie mogą się nam wyświetlać w sieci. Ostrożność jest także wskazana przy podejrzanych wiadomościach email. Często mogą się w nich kryć szkodliwe programy[25]. Ze szczególną uwagą należy również dobierać aplikacje i pozostałe oprogramowanie, z którego będziemy korzystać, biorąc również pod uwagę źródło z jakiego pozyskujemy dany program.

Uniknięcie zainfekowania złośliwym oprogramowaniem poprzez fizyczny dostęp jest nieco trudniejsze. Zazwyczaj zwykli użytkownicy nie decydują się na tego typu zabezpieczenia z uwagi na to, że ich urządzenia są pod ich stałym nadzorem i dostęp do nich osób trzecich wymagałby dużego wysiłku. Inaczej sprawa wygląda w przypadku firm, dużych korporacji czy instytucji państwowych. Atakujący system może chcieć zainfekować go przy pomocy urządzenia takiego jak pendrive. Aby chronić się przed tego typu incydentami, organizacja zazwyczaj decyduje się na wyłączenie z użycia wszelkich metod fizycznego dostępu do systemu lub częściowo go ogranicza, umożliwiając użytkowanie jedynie zarejestrowanych nośników danych w postaci pamięci masowych USB czy płyt CD i DVD.

Stuxnet – cyberbroń, która zapoczątkowała wojnę informacyjną

Dosyć ciekawym przykładem złośliwego oprogramowania, jakie powstało, jest Stuxnet. Według raportu UK Border Agency jest to robak komputerowy, który atakuje systemy przemysłowe i mógł być stworzony przez rząd obcego państwa[26]. Choć wykryto je dopiero w czerwcu 2010 r., to gdy eksperci z różnych firm dostarczających oprogramowanie antywirusowe analizowali różne wersje tego robaka, doszli do wniosku, że pierwsza wersja powstała już rok wcześniej – w czerwcu 2009 r. Pomimo, że aktualnie Stuxnet nie stwarza zagrożenia, jeżeli system urządzenia jest aktualny, to w okresie, gdy zostało stworzone i było rozpowszechniane, potrafiło dosłownie paraliżować działanie całych systemów teleinformatycznych opartych o SCADA. Tego typu systemy komputerowe są kluczowym elementem w procesie produkcyjnym w większości zautomatyzowanych fabryk.

Początkowo, gdy w czerwcu 2010 r. Siergiej Ulasen, pracownik firmy zajmującej się oprogramowaniem antywirusowym – VirusBlokAda, wykrył podejrzany malware, który potem nazwano Stuxnet, nie wiedziano kto jest twórcą tego złośliwego zestawu kodów. Dosyć jasne było jednak to, kiedy dochodziło do pierwszych ataków. Zespół techników białoruskiej firmy badający

[25] Ochrona przed malware, https://support.google.com/google-ads/answer/2375413?hl=en, dostęp: 25.02.2021 r.
[26] UK Border Agency. Home office, *Country of origin information report,* 2011, s. 248 https://www.justice.gov/sites/default/files/eoir/legacy/2013/06/12/iran-0611.pdf, dostęp: 25.02.2021 r.

złośliwe pliki, doszedł do wniosku, że napastnicy prowadzili atak w kilku etapach. Pierwsza fala przypuszczalnie miała miejsce już w czerwcu 2009 r., a kolejne w marcu i kwietniu kolejnego roku. Pomiędzy wersjami Stuxneta używanego w poszczególnych fazach, istniały drobne różnice, co wskazywało na sukcesywne wprowadzanie usprawniających zmian w kodzie szkodliwego oprogramowania[27]. Duży wkład w rozpoznanie zagrożenia w pierwszych dniach i tygodniach po wykryciu tego malware, miał wydział reagowania na zagrożenia firmy Symantec, z Liamem O'Murchu na czele.

Dziś z nieoficjalnych źródeł wiadomo, że kod stworzony został przez dużą grupę specjalistów, która pracowała w ramach tajnej operacji o kryptonimie „Olympic Games" na zlecenie służb wywiadowczych Stanów Zjednoczonych i Izraela. Było to działanie, które miało spowolnić rozwój irańskiego programu nuklearnego.

Według wyliczeń firmy produkującej oprogramowanie antywirusowe Kaspersky, stworzenie takiego oprogramowania grupie dziesięciu koderów zajęłoby od dwóch do trzech lat. Tajemnicą nie jest również fakt, że przeznaczeniem Stuxneta była irańska placówka zajmująca się wzbogacaniem uranu w Natanz. Działanie szkodliwego kodu miało uniemożliwić lub przynajmniej spowolnić trwającą tam produkcję. Warto tu również zaznaczyć, że Stuxnet nie miał trafić do powszechnego obiegu. Biorąc pod uwagę kwestię braku dostępu do internetu wewnątrz placówki, najprawdopodobniej ktoś z pracowników zakładu wzbogacającego uran wyniósł na zewnątrz nośnik pamięci zainfekowany złośliwym kodem[28].

Kres działaniu Stuxneta położyła łatka dla systemu Windows o nazwie MS10-092, eliminująca podatność wykorzystywaną przez ten malware. Niestety ta aktualizacja zabezpieczeń miała miejsce dopiero 15 grudnia 2010 r., czyli niemal pół roku po wykryciu zagrożenia[29]. Irański zarząd placówki wzbogacającej uran w Natanz rzekomo wcześniej zabezpieczyli swoje systemy przed Stuxnetem, choć nie wiadomo, jak było w rzeczywistości. Długą prace nad przygotowaniem łatki, która czyniła wirusa nieszkodliwym można wyjaśnić tym, iż zainfekowanych urządzeń było stosunkowo niewiele. Namierzonych zostało jedynie 38 tysięcy takich maszyn na całym świecie, a rzeczywiście zagrożonych było niewiele ponad 100 urządzeń. Procentowy podział zakażeń Stuxnet w obrębie poszczególnych państw przedstawiony został w tabeli nr 10.1.

Odpowiednio, w Iranie wykryto około 22 tysięcy przypadków zainfekowanych maszyn, w Indonezji było to ok. 6700 komputerów, a w Indiach

[27] K. Zetter, *Odliczając do dnia zero: Stuxnet, czyli historia cyfrowej broni,* Helion, Gliwice 2018, s. 23.
[28] https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html, dostęp: 25.02.2021 r.
[29] https://www.welivesecurity.com/2010/12/15/ms10-092-and-stuxnet/, dostęp: 25.02.2021 r.

mniej więcej 3700 stacji. Warto tu również zaznaczyć, że z zarażonych Stuxnetem irańskich urządzeń, jedynie 217 posiadało oprogramowanie, które było niezbędne, aby wirus zaczął działać.

Tabela 10.1

Procentowy podział infekcji Stuxnet w poszczególnych państwach

Państwo	Procentowy podział infekcji
Iran	52,20%
Indonezja	17,40%
Indie	11,30%
Pakistan	3,60%
Uzbekistan	2,60%
Rosja	2,10%
Kazakchstan	1,30%
Białoruś	1,10%
Kirgistan	1,00%
Azerbejdżan	0,70%
Stany Zjednoczone	0,60%
Kuba	0,60%
Tadżykistan	0,50%
Afganistan	0,30%

Źródło: Opracowanie własne na podstawie: https://www.esetnod32.ru/company/viruslab/analytics/doc/Stuxnet_Under_the_Microscope.pdf, dostęp: 25.02.2021 r.

Rozbierając kod źródłowy Stuxneta na czynniki pierwsze, okazuje się, że jest to niezwykle skomplikowany pakiet kodu. Składa się on z czterech głównych plików, których działanie jest ze sobą ściśle powiązane. Elementem, który umożliwiał rozpoczęcie działania Stuxneta, był plik o rozszerzeniu .LNK. Zawartości o takim rozszerzeniu normalnie odpowiadają za wyświetlanie przez system Windows ikon w plikach skrótów. Ten konkretnie spreparowany, wykorzystywał nieznaną dotąd podatność, znaną jako CVE-2010-2568[30]. Problem był w tym, że system automatycznie wczytywał tego typu pliki, a w omawianym przypadku, w kodzie zaszyta była ścieżka do pliku wykonywalnego w formacie .TMP, który rozpoczynał działanie kolejnego. Były to kolejno: WTR4141.tmp oraz WTR4132.tmp. Ten ostatni uruchamiał główną zawartość Stuxneta, czyli trojana[31].

Ciekawy jest fakt, iż trojan zaczynał działać tylko wtedy, gdy odnajdował działające oprogramowanie Siemensa, a konkretnie SIMATIC Step 7 oraz SIMATIC WinCC. Były to programy odpowiedzialne za współpracę ze

[30] https://archive.org/details/Stuxnet, dostęp: 25.02.2021 r.
[31] https://xakep.ru/2010/11/18/53950/, dostęp: 25.02.2021 r.

sterownikami PLC tej samej firmy, w innym wypadku pliki Stuxneta nie były szkodliwe dla systemu. Co do tego, co powoduje kod złośliwego oprogramowania to wykorzystuje on konkretne luki, aby rozprzestrzeniać i wykonywać zadane procedury. Między innymi implementuje Microsoft Remote Procedure Call, umożliwiając systemom, które są nim zarażone, komunikowanie się między sobą. Testuje również aktywne połączenie internetowe, do których urządzenie ma dostęp, w celu komunikacji z zewnętrznymi serwerami. W przypadku SIMATIC WinCC, działa także komponent odpowiedzialny za próbę uzyskania dostępu do bazy danych.

To co czyniło Stuxneta wysoce niebezpiecznym dla systemów, dla których był docelowo stworzony, to to, że wykorzystywał on podatności typu zero-day, czyli takie, które dotychczas nie zostały wykryte lub nie powstały łatki systemowe, które je eliminują. Dodatkowo wykrycie utrudniały certyfikaty szkodliwych plików, należące do firm RealTek oraz JMicron, bowiem twórcom złośliwego kodu udało się w jakiś sposób zdobyć autentyczne ich wersje[32].

Do dziś nie ustalono dokładnego czasu pierwszego zainfekowania systemów obsługujących wirówki do wzbogacania uranu w irańskim ośrodku w Natanz. Znanych jest za to kilka firm, które jako pierwsze padły ofiarą Stuxneta. Pierwsza infekcja wirusem dotknęła firmę Foolad Technique i przypisuje się ją na 23 czerwca 2009 r[33]. Niecały tydzień później, bo 29 czerwca, ofiarą została także firma Behpajooh. Kolejno, 7 lipca, zainfekowana została również firma Neda Industrial Group[34]. Wybór konkretnie tych przedsiębiorstw nie był jednak przypadkowy, bowiem wszystkie były częściowo zaangażowane w wytwarzanie i dostarczanie rozwiązań technicznych, na których bazował system wzbogacania uranu w irańskim ośrodku nuklearnym w Natanz.

Zmiany, które miały usprawnić działanie kodu Stuxneta, dostarczane były do ośrodka, zależnie od wersji, także poprzez inne firmy, które zaopatrywały irański ośrodek nuklearny w sprzęt i oprogramowanie. Modyfikacje kodu były możliwe dzięki opracowywanym przez Międzynarodową Agencję Energii Atomowej raportom, które tworzone były na podstawie kontroli ośrodka w Natanz. Były one ogólnodostępne i każdy mógł mieć do nich dostęp. Raporty były o tyle aktualne, że ów kontrole odbywały się dwa razy w miesiącu.

Wiadome jest także, że od czerwca 2009 r. zaczęła spadać ilość faktycznie pracujących wirówek wzbogacających uran. W czerwcu było to 4920 urządzeń, w sierpniu 4592, a w listopadzie ich liczba spadła do jedynie 3936. Co więcej, pomimo, że taka ilość wirówek pracowała, to było wiele innych, które z niewiadomych dla personelu ośrodka przyczyn, nie spełniały swojego zadania. Dla uzmysłowienia tego zjawiska na początku roku 2010, zainstalo-

[32] K. Zetter, *Odliczając do dnia zero…*, dz. cyt., s. 23.
[33] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/, dostęp: 25.02.2021 r.
[34] K. Zetter, *Odliczając do dnia zero…*, dz. cyt., s. 345-346.

wanych było aż 8692 urządzeń wzbogacających uran, a pracowało z nich jedynie 3772[35]. Tuż po wykryciu zagrożenia tj. w lipcu 2010 r., wirówki pracowały średnio na 45-66% swoich możliwości[36]. Szacuje się, że działanie wirusa spowolniło irański program nuklearny o mniej więcej 18-24 miesiące.

Jako że ataku dopuściły się służby wywiadowcze Stanów Zjednoczonych oraz Izraela wskazuje to na pewnego rodzaju konflikt. Pomimo, że nie użyto czołgów, ani regularnych oddziałów wojska, to niewątpliwie takie zdarzenie można by określić jako naruszenie podmiotu jakim jest państwo wraz z jego własnością. Dziś jasno mówi się, że nieustannie trwa globalna wojna w cyberprzestrzeni, a tego typu ataki są przejawem toczącej się wojny informacyjnej. Warto tu także zaznaczyć, że cyberatak na irański ośrodek nuklearny w Natanz był w zasadzie pierwszym powszechnie znanym przykładem takich działań[37]. Niestety, żadne państwo nie posiada jeszcze jasno sprecyzowanych przepisów prawa ani nie stwierdziło, jakie wrogie działania przeciwnika w obrębie cyberprzestrzeni można uznać za wypowiedzenie wojny.

Metodologia

Celem pracy było przedstawienie pojęć związanych z cyberprzestrzenią w kontekście zagrożenia cyberbezpieczeństwa, takich jak incydenty, cyberprzestępstwa czy cyberataki. Dzięki temu, uwidocznione zostały problemy nie tylko różnorodności zagrożeń występujących w obrębie omawianego środowiska, ale również ich potencjalnych efektów, które mogą stanowić krytyczne zagrożenie dla systemów teleinformatycznych, których one dotyczą.

Praca została napisana na podstawie dokładnej analizy materiałów zwartych, artykułów naukowych, które dotyczą tematyki cyberbezpieczeństwa, aktów prawnych, które tyczą się omawianych pojęć, a także informacji, jakie można znaleźć na rzetelnych stronach internetowych z branży IT i bezpieczeństwa teleinformatycznego.

Przegląd literatury

Źródła wykorzystane w pracy to zarówno polska jak i zagraniczna literatura specjalistyczna z zakresu cyberbezpieczeństwa, przestępstw teleinformatycznych czy bezpieczeństwa informacji. Do sprecyzowania części aspektów bezpieczeństwa cyberprzestrzeni posłużyły również akty normatywne, tj. ustawy, rozporządzenia oraz opracowania rządowe. Dla zróżnicowania źródeł wykorzystane zostały również publikacje europejskich organizacji rządowych, czy też globalne normy ISO/IEC. Przestudiowanie tych wszystkich elementów pozwoliło na rzetelne przygotowanie podstawy teoretycznej, na której oparta

[35] Tamże, s. 347-348.
[36] Tamże, s. 361.
[37] Tamże, s. 315-341.

została pozostała część pracy. Najbardziej bieżące informacje i statystyki dotyczące opisywanej tematyki zaczerpnięte zostały z fachowych stron internetowych odnoszących się do omawianych pojęć.

Wnioski

Cyberprzestrzeń jest wciąż rozwijającym i poszerzającym się środowiskiem, a co za tym idzie, oprócz płynących z tego korzyści, ilość występujących tam zagrożeń, które naruszają cyberbezpieczeństwo również rośnie. Co więcej, każde z nich narusza bezpieczeństwo systemów teleinformatycznych. Pomimo istnienia pewnych sposobów ochrony i przeciwdziałania takim sytuacjom, niektórych cyberincydentów nie da się przewidzieć, ani im zapobiec. Niemniej jednak, istnieją incydenty, których znaczenie jest istotniejsze niż innych, z uwagi na to, że ich skutki mogą być fatalne.

Różnorodność zagrożeń płynących z incydentów w cyberprzestrzeni jest ogromna, a świadczy o tym przede wszystkim występowanie wielu wektorów, z których cyberzagrożenie może nadejść. Wartym zaznaczenia jest również fakt, że cyberincydent może dotknąć trzech różnych wymiarów cyberprzestrzeni, tj. wymiarów fizycznego, wirtualnego oraz ludzkiego. Ponadto, motywy działania sprawców cyberprzestępstw są podzielone i wskazują na różne pobudki w szkodliwym działaniu. Jako, że incydent w cyberprzestrzeni może dotknąć również, a w zasadzie przede wszystkim, samego człowieka, niezbędne jest utrzymanie odpowiedniego poziomu cyberbezpieczeństwa, zarówno w sferze indywidualnej jak i szerszej – firmowej, państwowej itd. Pomijając ogólny poziom podziału incydentów w cyberprzestrzeni, warto wskazać na występowanie ogromnej ilości sposobów działania i typów takich zagrożeń w obrębie każdego wymiaru. Wskazanie cech i atrybutów konkretnego incydentu jest przez to utrudnione, lecz nie niemożliwe, bowiem istnieje wiele sposobów ich taksonomii, a co więcej, w obrębie struktur państwowych i korporacji działają odpowiednie podmioty zajmujące się kwestią wykrywania, opisywania i zwalczania takich incydentów.

Potencjalnie wysokie zagrożenie płynące z faktu występowania incydentów w cyberprzestrzeni wymusza na państwach, które w niej operują utrzymanie odpowiedniego poziomu cyberbezpieczeństwa. W tym celu wiele z nich, w tym również Polska, posiada odpowiednie strategie i regulacje wspomagające utrzymanie odpowiedniego poziomu bezpieczeństwa w ich cyberprzestrzeni. Niemniej jednak, dynamiczny wzrost ilości cyberzagrożeń i ich rodzajów wymaga na rządzących państwami ciągłą obserwację wciąż rozwijającego się środowiska i wprowadzanie zmian i uaktualnień w przepisach prawa
i innych aktach normatywnych.

Pomimo istnienia wyżej opisanych regulacji, trzeba jednak zwrócić uwagę na braki, które w nich występują. Pojęciem szczególnie wartym uwagi, jest wojna informacyjna, która nieustannie toczy się w cyberprzestrzeni. Po-

mimo, że istnieją autorytety naukowe i organizacje, które takie zjawisko definiują i odnajdują je w rzeczywistości, to żadne z państw nie posiada umocowania w prawie, które się do niego odnosi. Od roku 2010, kiedy to wykryto sabotaż w irańskim ośrodku nuklearnym poprzez cyberatak zorganizowany przez inne państwa na tamtejsze systemy teleinformatyczne, mówi się o stale prowadzonej wojnie informacyjnej. Niestety, żadne z państw nie określiło do tej pory, jakie szkodliwe działanie naruszające jego cyberbezpieczeństwo i atakujące elementy cyberprzestrzeni państwa ze strony wrogiego kraju, można by uznać za akt wypowiedzenia wojny, czy chociażby stwierdzenia, że to państwo naruszyło naszą cyberprzestrzeń, za co można by podjąć określone działanie w odwecie. Poza wcześniej wspomnianym uaktualnianiem i ciągłym rozwijaniem strategii cyberbezpieczeństwa państw, niezbędne jest podjęcie kroków w celu określenia zakresu niepożądanych działań w ich cyberprzestrzeni, które będą świadczyły o ataku na ich kraj.

Bibliografia

Opracowania zwarte

1. Dela P., *Wstęp do teorii walki w cyberprzestrzeni,* [w:] J. Kosiński, G. Krasnodębski (red.), *Rocznik Bezpieczeństwa Morskiego. Przestępczość teleinformatyczna 2019,* Gdynia 2020, s. 14.
2. Zetter K., *Odliczając do dnia zero: Stuxnet, czyli historia cyfrowej broni*, Helion, Gliwice 2018.
3. Kosiński J., *Paradygmaty cyberprzestępczości,* Difin, Warszawa 2015.
4. Kosiński J., Krasnodębski G., *Cybercrime predicting in the light of police statistics*, [w] H. Jahankhani, A. Jamal, S. Lawson, *Cybersecurity, Privacy and Freedom Protection in the Connected World,* Springer, Cham 2021.

Dokumenty normatywne

1. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz. U. 2002 nr 144 poz. 1204.
2. Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz. U. 2004 nr 171poz. 1800.
3. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. 2005 nr 64 poz. 565.
4. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. 2018 poz. 1560.
5. Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016, Warszawa 2010.
6. Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-2022, Warszawa 2017.

7. Główny Urząd Statystyczny, Sprawozdanie o wykorzystaniu technologii informacyjno-telekomunikacyjnych w przedsiębiorstwach, Warszawa 2014.
8. Komisja europejska, Wspólny Komunikat Parlamentu Europejskiego i Rady – Strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, Bruksela 2020.

Źródła internetowe

1. https://io9.gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487, dostęp: 20.02.2021 r.
2. https://www.guru99.com/what-is-hacking-an-introduction.html, dostęp: 24.02.2021 r.
3. https://www.av-test.org/en/statistics/malware/, dostęp: 24.02.2021 r.
4. https://www.justice.gov/sites/default/files/eoir/legacy/2013/06/12/iran-0611.pdf, dostęp: 25.02.2021 r.
5. https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html, dostęp: 25.02.2021 r.
6. https://www.welivesecurity.com/2010/12/15/ms10-092-and-stuxnet/, dostęp: 25.02.2021 r.
7. https://archive.org/details/Stuxnet, dostęp: 25.02.2021 r.
8. https://xakep.ru/2010/11/18/53950/, dostęp: 25.02.2021 r.
9. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, dostęp: 21.02.2021 r.
10. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189, dostęp: 21.02.202 r.

Inne

1. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku,* Polska 2019.
2. UK Border Agency. Home office, *Country of origin information report,* 2011.