Nowoczesne Systemy Zarządzania
Zeszyt 16 (2021), nr 1 (styczeń-marzec)
ISSN 1896-9380, s. 97-119
DOI: 10.37055/nsz/134812

Instytut Organizacji i Zarządzania
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

Modern Management Systems
Volume 16 (2021), No. 1 (January-March)
ISSN 1896-9380, pp. 97-119
DOI: 10.37055/nsz/134812

Institute of Organization and Management
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

Człowiek jako najsłabsze ogniwo bezpieczeństwa informacyjnego

Man as the weakest link of the information security

Joanna Skulska
Wojskowa Akademia Techniczna
Wydział Bezpieczeństwa, Logistyki i Zarządzania
joanna.skulska@wat.edu.pl; ORCID: 0000-0001-9875-1774

Weronika Pławińska
P4 Sp. z o.o.,
Departament Bezpieczeństwa i Biuro Ochrony Informacji Niejawnych

Abstrakt. Celem artykułu jest określenie roli i znaczenia człowieka oraz jego słabości w systemie bezpieczeństwa informacyjnego organizacji. Wszyscy ludzie popełniają błędy, które niekiedy mogą wiązać się z poważnymi konsekwencjami. Jak wynika z 2014 Cyber Security Intelligence Index, aż 95% wszystkich incydentów związanych z bezpieczeństwem dotyczy błędów popełnionych przez człowieka. Dla organizacji takie sytuacje są zazwyczaj bardzo kosztowne, ze względu na to, że dotyczą osób, które posiadają dostęp do najbardziej wrażliwych danych. Jak wynika z przytoczonego w artykule badania, świadomość respondentów dotycząca zagrożeń występujących w systemach informacyjnych jest niska. Zmiany zachodzące w dostępie do informacji wiążą się z koniecznością ciągłego doskonalenia jej ochrony. Nie tylko systemowej, lecz także wynikającej z kompetencji człowieka. Dlatego warto na nim skupić uwagę i zastanowić się nad możliwymi metodami poszerzania jego kompetencji oraz ciągłej nauki.
Słowa kluczowe: bezpieczeństwo informacyjne organizacji, zasoby informacyjne, rola człowieka w bezpieczeństwie informacyjnym, zagrożenia bezpieczeństwa informacyjnego

Abstract. The purpose of this article is to define the role and importance of human beings and their weaknesses in the information security system of an organization. All people make mistakes that can sometimes have serious consequences. According to the 2014 Cyber Security Intelligence Index, as much as 95% of all security incidents are related to human errors. For organizations, such situations are usually very costly, as they concern people who have access to the most sensitive data. As the study cited in the article shows,

the awareness of threats in information systems among the respondents is low. The ongoing changes in the availability of information are associated with the need to constantly improvement its protection. Not only systemic, but also protection resulting from human competences. That is why it is worth focusing on him and considering possible methods of expanding his competences and continuous learning..
Keywords: information security of an organization, information resources, human role in information security, threats to information security

Wstęp

Celem artykułu jest określenie roli i znaczenia człowieka oraz jego słabości w systemie bezpieczeństwa informacyjnego. Główną motywacją autorek jest zwrócenie uwagi na fakt, że za każdym systemem informacyjnym stoi człowiek. Z tego powodu istotne jest pokazanie najważniejszych zagadnień bezpieczeństwa informacyjnego w organizacjach oraz odniesienie ich do jednostki ludzkiej. Starano się odpowiedzieć na pytania:

- Czy zagrożenia związane z bezpieczeństwem informacyjnym dotykają bezpośrednio jednostki czy ogółu społeczeństwa?
- Czy człowiek może czuć się zagrożony, jeżeli nie ma dostępu do informacji?
- Czy człowiek jest odpowiedzialny za zagrożenia informacyjne, w jaki sposób?
- Jakie korzyści dla człowieka przynosi ochrona informacji?

Artykuł jest pracą o charakterze opisowo-badawczym. Dobór poszczególnych narzędzi metodologicznych uwarunkowany był treścią zagadnień oraz analizowanych problemów badawczych zawartych w poszczególnych częściach artykułu. Dominującą metodą jest jakościowa analiza treści publikacji kolejno wymienionych w przypisach i bibliografii. Na podstawie analizy treści dokonano opisu, systematyzacji oraz syntezy głównych zagadnień. Dodatkowo w ostatniej części artykułu opisane zostały wyniki ankiety internetowej wykorzystanej jako metoda badania społecznego.

W konstrukcji artykułu została zachowana zasada ciągu wynikania, a także układu hierarchicznego.

Znaczenie informacji we współczesnym świecie

Informacja, jej wykorzystanie i ochrona towarzyszyły człowiekowi od zawsze, jednak od niedawna jej znaczenie wzrosło przez rozwój techniki oraz rewolucję informacyjną, która „(…) wprowadziła świat w erę społeczeństwa informacyjnego, czyli społeczeństwa, w którym informacja stanowi kluczowy produkt, a wiedza niezbędne bogactwo" (Kubiak, Topolewski, 2016, s. 25).

W dzisiejszym społeczeństwie istnieje ogromna i pilna potrzeba dostępu do informacji i jej dostępności. Jak wynika z raportu Mediarecovery, kilka lat temu

podmioty funkcjonujące w sektorach zarówno publicznym, jak i prywatnym nie przywiązywały wielkiej wagi do wartości, jaką są posiadane przez nie informacje. Z tym wiąże się fakt, że bezpieczeństwo informacji nie stanowiło dla polskich firm priorytetu. Co więcej, autorzy tego raportu posuwają się nieco dalej, twierdząc, że „(…) Bezpieczeństwo informacji utożsamiane było w naszym kraju z zamkniętymi drzwiami biura, zamykaną na klucz szafą, alarmem antywłamaniowym oraz gaśnicą. Najważniejsze dokumenty, wtedy jeszcze istniejące przede wszystkim w formie papierowej, przechowywano w szafach, sejfach, chronionych siedzibach, a najbardziej istotne w bankach" (Mediarecovery, 2013, s. 3). Stwierdzenie to identyfikowane jest z tradycyjnymi formami zabezpieczeń, których w większości nie poprzedzano analizą potencjalnych zagrożeń, nastawione były jedynie na zagrożenia fizyczne oraz zewnętrzne.

W wyniku transformacji społeczeństwa w tzw. *społeczeństwo informacyjne* wzrosło znaczenie cyfryzacji – zaczęto cyfryzować dokumenty, a sieć stała się podstawą funkcjonowania nie tylko organizacji, lecz także ludzi. Dziś znaczna część informacji nie jest już przechowywana np. w teczkach, tylko na elektronicznych nośnikach danych – dyskach twardych, serwerach czy w chmurze. Te zmiany spowodowały konieczność adaptacji nowego podejścia do bezpieczeństwa informacji, a ona sama stała się jedną z najwyżej cenionych wartości nie tylko w biznesie, ale i w relacjach między ludźmi (https://panoptykon.org/). Nie wystarczy już tylko dotarcie do informacji, która jest dostępna dla wszystkich, ważna jest umiejętność wyselekcjonowania najistotniejszej, a także posiadanie tej niedostępnej dla innych. To czy zdobyta informacja będzie wartościowa, zależy od tego, jak długo uda się nam utrzymać ją w tajemnicy.

Ze względu na postępującą digitalizację można wnioskować, że całkowite przejście z tradycyjnej formy – papierowej, jaką przybiera informacja, na formę cyfrową jest nieuniknione. Nie należy jednak spodziewać się, że nastąpi to *ad hoc*, będzie to długotrwały proces, ponieważ dziś nawet posiadając wersję papierową dokumentu, robi się często jej cyfrową kopię. Jak podano w raporcie Mediarecovery z 2013 roku: „(…) już tylko 43% informacji nadal funkcjonuje w formie papierowej (…)" (Mediarecovery, 2013, s. 4). Minęło pięć lat od przedstawienia wyników tego badania, więc obecnie mogą być one znacznie niższe.

Dla przeciętnej jednostki otaczająca ją cyfrowa rzeczywistość stanowi możliwość dostępu do informacji praktycznie z każdego miejsca na Ziemi – przykładem jest telefon, który jest wielozadaniowy, daje niemal nieograniczone możliwości (Mediarecovery, 2013, s. 4). Powszechną usługą świadczoną w technologii jest tzw. chmura obliczeniowa – jest to „dostarczanie usług obliczeniowych – w tym serwerów, magazynu, baz danych, sieci, oprogramowania, analizy i inteligencji – za pośrednictwem Internetu w celu zaoferowania szybszych innowacji, elastycznych zasobów i ekonomii skali" (https://azure.microsoft.com/). Dostawcy tego typu usług są podmiotami szczególnie zagrożonymi, jeżeli chodzi o bezpieczeństwo informacji.

Z badania przeprowadzonego w 2013 roku wynika, że ponad 77% organizacji zdaje sobie sprawę z dużej wartości informacji, a jej bezpieczeństwo uważa za jeden z priorytetów. Mimo to bardzo trudno oszacować dokładną wartość informacji. Sprzeciwu nie wzbudza jednak stwierdzenie, że informacja, szczególnie niedostępna dla konkurencji, stanowi wartość dla jej właściciela (Mediarecovery, 2013, s. 10). Na podstawie raportu Mediarecovery oraz książki *Bezpieczeństwo informacyjne XXI w*. M. Kubiak wyciąga wnioski, że potrzeba informacji może wynikać z kilku względów (Kubiak, Topolewski, 2016, s. 56-57):

- informacje są pomocą w podejmowaniu decyzji, tworzeniu polityki potrzebnej dla decydentów, menedżerów itp.;
- informacje będą miały na ludzi wpływ wzmacniający/przekształcający. Bardzo wiele zmian można dostrzec w ludzkich umysłach, postawach dotyczących uzyskiwania informacji, ponieważ zwiększa to zdolność zdobywania wiedzy przez odbiorcę;
- informacje generują nowe informacje. To istniejąca wiedza/informacja pomaga w generowaniu nowych informacji, nowej wiedzy, nowych teorii itp.;
- w rzeczywistości naukowcy i uczeni korzystają z informacji lub wykorzystują informacje do opracowania innego dokumentu, takiego jak raporty z badań, praca naukowa/rozprawa doktorska, książki, artykuły w czasopismach, materiały seminaryjne itp.;
- informacje stymulują proces myślowy użytkowników, zwłaszcza uczonych;
- zdobywanie informacji może służyć jako użyteczne narzędzie sprawowania władzy.

Powyższe uwarunkowania pokazują, że informacja jest jedną z cenniejszych wartości dla człowieka. Mimo to pojawia się pewna nieczytelność, ponieważ z jednej strony informacje próbuje się chronić, natomiast z drugiej występują działania na dużą skalę związane z jej udostępnieniem szerokiemu odbiorcy (Mediarecovery, 2013, s. 8). W październiku 2017 roku na stronie Rządowego Centrum Legislacji pojawił się projekt ustawy o jawności życia publicznego. Ustawa, jeżeli zostałaby przyjęta, narzucała zarówno na podmioty publiczne, jak i przedsiębiorców prywatnych wiele nowych obowiązków. Kwestią kontrowersyjną w projekcie ustawy jest m.in. zmiana zasad dostępu do informacji publicznej, w tym obowiązków składania oświadczeń majątkowych przez kluczowych urzędników oraz inne osoby pełniące np. dyrektorskie stanowiska (https://legislacja.rcl.gov.pl/). Zgłoszono zastrzeżenia odnośnie do projektu ustawy, ponieważ: „(…) celem projektodawcy nie było wzmocnienie transparentności władzy publicznej, lecz dokonanie powszechnej lustracji majątkowej obywateli" (https://www.rpo.gov.pl). Ustawa narzucałaby na zwykłych obywateli obowiązek udostępniania informacji o dochodzie, majątku, nieruchomościach i ruchomościach przez nich posiadanych (oraz ich małżonków), zobowiązaniach, zwolnieniach i ulgach, „(…) danych osobowych w odniesieniu

np. do stron postępowania administracyjnego, czy darczyńców organizacji pozarządowych biorących udział w procesie stanowienia prawa (…)" (www.theguardian.com). Kwestią kontrowersyjną w tym projekcie jest także to, że informacje w większości byłyby udostępniane na szeroką skalę w Internecie, co jest ingerencją i nadużyciem w prawie do prywatności obywateli.

Skalę znaczenia informacji doskonale opisuje wydarzenie, które zostało ujawnione w 2018 roku. Cambridge Analytica to firma zajmująca się analizą danych, która współpracowała z zespołem wyborczym D. Trumpa i zwycięską kampanią za brexitem. Zebrała miliony profili facebookowych amerykańskich wyborców w jednym obszarze. Było to największe z naruszeń danych giganta technologicznego i wykorzystanie ich do zbudowania potężnego programu do przewidywania i wpływania na wybory przy urnie wyborczej (www.theguardian.com). Cambridge Analytica wykorzystała dane osobowe zebrane bez zezwolenia na początku 2014 roku w celu zbudowania systemu, który mógłby profilować indywidualnych wyborców w USA, tak aby kierować do nich spersonalizowane reklamy polityczne. Christopher Wylie, który współpracował z pracownikiem naukowym Uniwersytetu Cambridge w celu uzyskania danych, powiedział: „Wykorzystaliśmy Facebooka, aby zebrać profile milionów ludzi. I zbudowane modele, aby wykorzystać to, co o nich wiedzieliśmy, i atakować ich wewnętrzne demony. Na tej podstawie zbudowano całą firmę" (www.theguardian.com).

Kolejnym przykładem wagi informacji jest to, jak maszyny wykorzystujące *cyfrowe ślady* ludzkiej działalności, np. w mediach społecznościowych, są w stanie ocenić osobowość. „Naszą inteligencję, orientację seksualną – i wiele więcej można obliczyć na podstawie polubień z Facebooka" (https://mfiles.pl).

To wszystko pokazuje, jaką siłę ma jedna z cech informacji ‑ użyteczność. „Informacja użyteczna pozytywnie wpływa na podejmowane decyzje – zwiększając ich efektywność" (https://mfiles.pl).

Wszyscy ludzie popełniają błędy, które niekiedy mogą wiązać się z poważnymi konsekwencjami. Jak wynika z *2014 Cyber Security Intelligence Index*, aż 95 proc. wszystkich incydentów związanych z bezpieczeństwem dotyczy błędów popełnionych przez człowieka (https://securityintelligence.com/). Wiele z nich to ataki przeprowadzane przez osoby z zewnątrz, które wykorzystują ludzką słabość w celu uzyskania dostępu do poufnych informacji. Dla organizacji takie ataki są zazwyczaj bardzo kosztowne, ze względu na to, że dotyczą osób, które posiadają dostęp do najbardziej wrażliwych danych. Na podstawie raportu Vormetic można stwierdzić, że najbardziej udanymi atakami są te, które dotyczą kradzieży własności intelektualnej, poufnych danych, wprowadzenia złośliwego oprogramowania (https://securityintelligence.com/). Co więcej, w raporcie znalazły się również informacje na temat badania, które wykazało, że 59 proc. respondentów zgodziło się z tym, że większość zagrożeń dotyczących bezpieczeństwa technologii informatycznych to wynik niekiedy pozornie niewinnych błędów, a nie złośliwych oprogramowań. Warto zwrócić uwagę na kilka przypadków sytuacji, w których zawinił człowiek.

Na początku maja 2019 roku z Politechniki Warszawskiej wyciekły dane wrażliwe dotyczące studentów. Umieszczone były w pliku SQL, który miał rozmiar 2,8 GB. W pliku znajdowały się takie informacje jak: e-maile, nazwiska, numery indeksów, numery telefonów, hasze haseł, numery PESEL, NIP, numery dowodów osobistych, daty urodzenia, adresy, adresy IP logowań oraz wiele innych. Ponadto można było znaleźć dane kandydatów ubiegających się o przyjęcie na studia oraz informacje na temat pracowników uczelni (https://niebezpiecznik.pl). W wyniku zaistniałej sytuacji uczelnia musiała poinformować o naruszeniu danych osobowych Urząd Ochrony Danych Osobowych i policję. Studenci, których dane wyciekły, zmuszeni byli do zastrzeżenia dowodów osobistych, numeru PESEL, a także wielu innych działań w celu zabezpieczenia swojej tożsamości.

T. Goban-Klas w artykule *Społeczeństwo niedoinformowane* pisze, że „Jeśli zakładamy, że bez materii nie ma nic, a bez energii wszystko jest nieruchome, to bez informacji jest tylko chaos" (Goban-Klas, 1988). To w zupełności wystarcza, aby sądzić, że racją bytu jednostki jest ciągła komunikacja, bez niej przestałoby istnieć społeczeństwo. Teza ta w sposób bardzo dosadny prezentuje znaczenie informacji we współczesnym świecie. Nie tylko w życiu codziennym, lecz także w praktyce gospodarczej.

Należy podkreślić, że tajemnice, z jakimi mierzą się administracja publiczna, rządowa czy przedsiębiorstwa, muszą być chronione i powinny stanowić element bezpieczeństwa w wymiarze państwowym, instytucjonalnym i indywidualnym. Bardzo niepokojące jest to, że na co dzień dochodzi do wycieku tajemnic, które stają się sensacją dla mediów, ale także impulsem wywołującym potyczki polityczne. W obecnej sytuacji ochrona informacji (także tych niejawnych) stanowi nieodłączny element bezpieczeństwa informacyjnego, ale może być też barierą blokującą społeczeństwu dostęp do należnych mu informacji (Fehler, 2015, s. 3).

Istota bezpieczeństwa informacyjnego

Na potrzeby analizy tematu bezpieczeństwa informacyjnego należy omówić wybrane pojęcia, które będą przydatne w rozumieniu dalszych zagadnień poruszanych w pracy:

– społeczeństwo informacyjne – termin określający społeczeństwo, w którym tworzenie, rozpowszechnianie i manipulowanie informacjami stały się najważniejszą działalnością gospodarczą i kulturalną. Społeczeństwo informacyjne można przeciwstawić społeczeństwom, w których podstawa gospodarcza ma charakter przede wszystkim przemysłowy lub rolniczy. Narzędzia społeczeństwa informacyjnego to komputery i telekomunikacja (Burgiewa-Czuma, Gawrol, 2011, s. 32);

- zagrożenia informacyjne – „sytuacja, w której mamy do czynienia z uświadomionymi lub nie ograniczeniami lub nadużyciami w zakresie zgodnego z prawem dostępu oraz swobodnego posługiwania się aktualną, rzetelną, integralną i właściwie ochranianą pod kątem poufności informacją" (Fehler, 2015, s. 82);
- walka informacyjna – „(…) działania kooperacji negatywnej wzajemnej, w których cel destrukcyjnego oddziaływania skoncentrowany jest na systemach informacyjno-sterujących przeciwnych stron. Przedmiotem walki informacyjnej jest system informacyjno-sterujący" (*Słownik terminów z zakresu bezpieczeństwa narodowego*, 2002, s. 153);
- wojna informacyjna – „(…) operacje informacyjne prowadzone podczas kryzysu lub konfliktu w celu osiągnięcia lub poparcia konkretnych celów w odniesieniu do konkretnych przeciwników lub przeciwnika. Operacje informacyjne są to działania podjęte w celu wywarcia wpływu na informacje i systemy informacyjne przeciwnika przy jednoczesnej obronie własnych informacji i systemów informacyjnych" (Denning, 2002, s. 11). D.E. Denning dodaje jednocześnie, że „(…) w wojnie informacyjnej biorą udział nie tylko komputery i sieci komputerowe. Obejmuje ona informacje we wszelkiej postaci i przesyłane wszystkimi środkami, począwszy od ludzi, ich fizycznego środowiska, do druków, telefonów, radia i telewizji, do komputerów i sieci komputerowych. Taka wojna to operacje skierowane przeciw treści informacji i operacje przeciw związanym z nimi systemom, włącznie z oprzyrządowaniem, oprogramowaniem i pracą człowieka" (Denning, 2002, s. 14);
- polityka bezpieczeństwa informacyjnego – „(…) celowa i zorganizowana działalność danego podmiotu (państwa, korporacji, organizacji, instytucji itp.) ukierunkowana na tworzenie i utrzymywanie w optymalnym jakościowo kształcie własnych zasobów informacyjnych i mechanizmów ich użytkowania połączona z efektywną ochroną przed destrukcyjnym oddziaływaniem podmiotów konkurencyjnych, nieprzyjaznych czy wrogich" (Kubiak, Topolewski, 2016, s. 33).

Terminy te podkreślają dynamiczny charakter sfery bezpieczeństwa informacyjnego, która wymaga umiejętności kooperacji, równoważenia interesów oraz zawierania kompromisów.

Podejmując problem określenia istoty bezpieczeństwa informacyjnego, warto mieć na uwadze fakt, że dopóki nie powstanie uniwersalna definicja bezpieczeństwa, trudno znaleźć równie uniwersalne określenie bezpieczeństwa informacyjnego, które jest przedmiotem zainteresowania tej pracy. Aby spróbować zdefiniować pojęcie bezpieczeństwa informacyjnego, należy zacząć od rozbicia tych dwóch członów i określić, czym jest *bezpieczeństwo*. Jako dobro i potrzeba człowieka było ono wyróżniane na każdym etapie rozwoju ludzkości, choć niekoniecznie właściwie i jednoznacznie artykułowane (Szmyd, 2014, s. 10).

Zwracano uwagę na samą potrzebę poczucia braku zagrożenia, jednak formułowanie jej w osobnych traktatach nie było konieczne. Mimo to można odnaleźć ślady pisane, które umożliwiają odtworzenie jego leksykalnych korzeni. Pojęcie to pochodzi z języka łacińskiego – *sine cura* (*securitas*) i przetrwało w niewiele zmienionej formie w języku angielskim – *security* oraz francuskim – *securité* (Jarmoszko, 2016, s. 20). Wychodząc od etymologii w języku polskim, językoznawcy wskazują standardowe sformułowanie – *bez pieczy*, które oznaczało stan bez konieczności starań o opiekę, ochronę nadzór czy też zachowanie kontroli. Pierwotna *piecza* to tyle co *dbałość*, *staranność*, *troskliwość*. Mieć pieczę nad kimś/czymś oznaczało więc opiekę i ochronę (Jarmoszko, 2016, s. 20).

Pojęcie *bezpieczeństwo* jest dość młode w naukach społecznych i funkcjonuje na pograniczu techniki, organizacji oraz prawa (Jarmoszko, 2016, s. 18). Zgłębiając jego temat, pierwsze, co się nasuwa, to fakt, że definiowanie *bezpieczeństwa* zależy od tego, z jakiej z nauk społecznych się czerpie ‑ filozofia, ekonomia, psychologia czy politologia sytuują bezpieczeństwo we właściwym obszarze swojego zakresu tematycznego, tym samym przypisując jego znaczeniu różną wagę teoretyczną i merytoryczną (Jarmoszko, 2016, s. 20). Wielość definicji jest oczywista ze względu na fakt, że przedstawiciele poszczególnych dziedzin postrzegają i opisują bezpieczeństwo w świetle terminologii oraz wiedzy z zakresu swojej dyscypliny. Mimo tego „(…) większość badaczy jest zgodna, że bezpieczeństwo jest kategorią antropocentryczną" (Brzeziński, 2009, s. 30), tzn. że zawsze będzie postrzegane z perspektywy człowieka, mimo że może dotyczyć zjawisk fizycznych i przyrodniczych.

Słownik języka polskiego definiuje pojęcie bezpieczeństwa statycznie ‑ jako *stan niezagrożenia* (https://sjp.pwn.pl/sjp/bezpieczenstwo;2443939.html), tym samym nie uwzględnia innych kluczowych składników, takich jak proces społeczny i dynamiczny, a dodatkowo ‑ to stan, w którym podmioty starają się eliminować zagrożenia i podnosić swoją pewność.

A. Maslow uznał je za drugą w hierarchii potrzebę ludzką. „Bezpieczeństwo (ang. *security*) – stan, który daje poczucie pewności i gwarancję jego zachowania oraz szansę na doskonalenie. Jedna z podstawowych potrzeb człowieka. Jest to sytuacja odznaczająca się brakiem ryzyka utraty czegoś, co człowiek szczególnie ceni, na przykład: zdrowia, pracy, szacunku, uczuć, dóbr materialnych" (*Słownik terminów z zakresu bezpieczeństwa narodowego*, 2002, s. 14).

Według T. Łoś-Nowaka bezpieczeństwo to „(…) nie tylko stan możliwy do określenia jedynie w ustalonym miejscu i czasie, tu i teraz, ale również dynamiczny, zmieniający się w czasie proces" (Łoś-Nowak, 2003, s. 37-38). O ile definicja ta wydaje się spójna, brakuje w niej odwołania do samego człowieka – jakie zajmuje on miejsce? Jakie są jego odczucia? Doskonałym uzupełnieniem tej definicji są słowa R. Zięby: „bezpieczeństwo można określić jako pewność istnienia i przetrwania, posiadania oraz funkcjonowania i rozwoju podmiotu. Pewność jest wynikiem nie

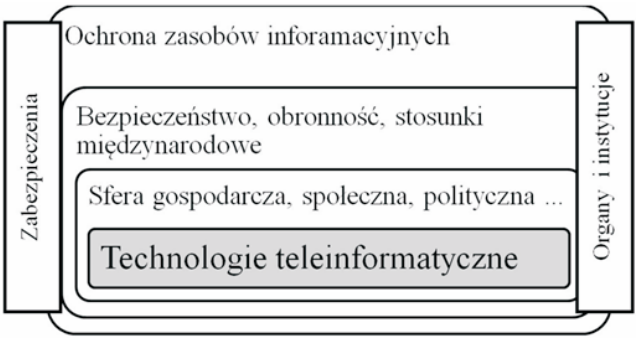
tylko braku zagrożeń (…), ale także powstaje wskutek kreatywnej działalności danego podmiotu i jest zmienna w czasie, czyli ma naturę procesu społecznego" (Zięba, 2008, s. 16). Tutaj należy pamiętać, że mimo starań podmiotów ma ono charakter względny i jest wartością absolutnie nieosiągalną.

Przywołując kilka definicji bezpieczeństwa, powinno się podjąć próbę zdefiniowania *bezpieczeństwa informacyjnego*. Jedna z norm ISO/IEC 17799:2005 definiuje je jako zachowanie trzech cech informacji: poufności (*confidentiality*), spójności (*integrity*) oraz dostępności (*availability*) (Zięba 2008, s. 18). Norma ISO/IEC 17799 została zastąpiona przez rodzinę norm ISO/IEC 27000 (w Polsce opublikowana 4 stycznia 2007 roku jako PN-ISO/IEC 27001:27000). Uwzględniała ona dodatkowe atrybuty bezpieczeństwa informacji: rozliczalność (*accountability*), autentyczność (*authenticity*), niezaprzeczalność (*non-repundation*) i niezawodność (*reliability*). Niezależnie od rodziny norm 17999 funkcjonowały tzw. raporty techniczne (ISO/IEC TR 13335-1 – w Polsce PN-I-13335-1:1999), które definiowały bezpieczeństwo informacji jako właśnie zapewnienie poufności, integralności, dostępności, niezaprzeczalności, rozliczalności, autentyczności i niezawodności. Cechy te należy uznać za trzon budowy bezpieczeństwa informacji. Każda z tych zasad oraz jej znaczenie mogą mieć różną wagę, w zależności od instytucji. Na przykład dla instytucji rządowych, bankowych czy konsultingowych najważniejsza będzie poufność. Reputacja firmy może zostać podważona poprzez wyciek informacji od osób trzecich. Tym samym firma może stać się niewiarygodna dla swoich klientów. Organizacje opracowujące badania statystyczne, raporty nie mogą popełnić pomyłki, gdyż może to bardzo negatywnie wpłynąć na ich wiarygodność. Dla nich najważniejsza będzie integralność w procesie przetwarzania danych (Zięba, 2008, s. 30). Dostępność jest najistotniejszym warunkiem funkcjonowania dla wszystkich organizacji z sektora usług, gdzie krótka przerwa w działaniu biznesu powoduje stratę finansową, np. usługi bankowe, telekomunikacyjne, sklepy internetowe. Jak można przypuszczać, istotne są wzajemne relacje składników bezpieczeństwa.

Podstawowe założenie, które możemy znaleźć w literaturze przedmiotu, jest następujące: „problematyka bezpieczeństwa informacyjnego obejmuje zarówno zabezpieczenia przed niepożądaną ingerencją w informacje wrażliwe i dane osobowe, jak i również formy zabezpieczenia systemów teleinformatycznych przed destrukcyjnymi działaniami zewnętrznych i wewnętrznych obiektów" (Szczepaniuk, 2014).

Zagadnienia związane z bezpieczeństwem informacyjnym można powiązać z tymi dotyczącymi bezpieczeństwa informatycznego lub ograniczyć je do kwestii ochrony informacji niejawnych (Łuszczak, Tyburski, 2009, s. 9). To pierwsze rozumienie pokazuje ochronę informacji jedynie wtedy, kiedy jej postać jest elektroniczna. Jest to o tyle niepełne, że bezpieczeństwo informacyjne to także proces, w którym informacja jest wytwarzana, modyfikowana i przetwarzana (Kubiak, Tobolewski, 2016, s. 36). Natomiast drugie wskazuje kwestie ochrony informacji niejawnych czy

też bezpieczeństwa systemów teleinformatycznych, co potwierdzają słowa K. Liedla: „Bezpieczeństwo informacyjne bardzo często rozumiane jest jako ochrona informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania" (Liedel, 2008, s. 19).



Rys. 1. Model strukturalny bezpieczeństwa informacyjnego
Źródło: Szczepaniuk, 2014

Nawiązując do stwierdzenia T. Gobana-Klasa: „(…) bez informacji jest tylko chaos" (http://rocznikikae.sgh.waw.pl/, s. 12), warto zauważyć, że chaos pojawiłby się również bez odpowiednich wymagań prawnych, które obejmowałyby funkcjonowanie bezpieczeństwa informacji. „Dobrze prosperujące przedsiębiorstwo nie może sobie pozwolić na utratę lub nieautoryzowane ujawnienie poufnych danych, dlatego niezwykle ważnym działaniem podejmowanym przez firmy oraz instytucje publiczne staje się zabezpieczanie środków przechowywania danych lub przetwarzania informacji" (Czekaj, 2012, s. 126). Zabezpieczenie informacji oraz samo bezpieczeństwo informacji nie dotyczą tylko samego przedsiębiorstwa jako „zorganizowanego zespołu składników niematerialnych i materialnych przeznaczonego do prowadzenia działalności gospodarczej" (Dz.U.2019.0.1145, 1964), ale głównie ludzi, którzy na to przedsiębiorstwo się składają. Oczekiwania ludzi wiążą się z zapewnieniem przez władzę poczucia bezpieczeństwa. W drugiej połowie XXI w. Polska notorycznie przekraczała lub była bliska przekroczenia granic nadzoru, który był niezbędny dla bezpieczeństwa, jak i naruszał prawo do prywatności.

„Katalog przestępstw, przy których można stosować inwigilację, liczy około 200 pozycji ukrytych w przepisach karnych różnych ustaw" (Fehler, 2015, s. 88). Co więcej, stosowanie inwigilacji może znajdować swoje prawne *usprawiedliwienie* w umowach i porozumieniach międzynarodowych.

W Polsce bezpieczeństwo obywateli jest gwarancją konstytucyjną, o czym mówi art. 5 Konstytucji RP: „Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz

bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju" (Konstytucja RP, 1997, art. 5). Jest to punkt wyjścia do dalszych rozważań na temat regulacji prawnych dotyczących bezpieczeństwa informacji, jednak jak na razie nie ma jednej zbiorczej ustawy czy rozporządzenia, które kompleksowo mieściłoby: wymagania, wytyczne, techniczne zalecenia czy obowiązkowe zabezpieczenia sprzętowe, programowe i organizacyjne (Łuczak, Tyburski, 2009, s. 29). Dlatego osoby obracające się w tym sektorze bezpieczeństwa, które chcą wdrażać systemy zarządzania nim, muszą przeanalizować akty prawne, na podstawie których funkcjonuje dana organizacja. Dostęp do informacji oraz wolność słowa są standardem obowiązującym w państwach demokratycznych. Taka sytuacja ukształtowała się w momencie uchwalenia Konwencji o ochronie praw człowieka i podstawowych wolności w Rzymie. „Ograniczenie swobodnego dostępu do informacji traktuje się jako atak na podstawowe prawa człowieka" (Dereń, 2001, s. 9).

Psychospołeczne i prakseologiczne aspekty bezpieczeństwa informacyjnego

Jak wynika z przeglądu literatury, informacje stanowią strategiczny zasób organizacji, a od ich ochrony zależy przewaga konkurencyjna przedsiębiorstwa. Ze względu na dynamiczny rozwój technik informatycznych niemal każda firma korzysta z usług świadczonych drogą elektroniczną. Za komputeryzacją idzie informatyzacja, która nasila działania przestępcze. Skala i tempo ewoluujących zagrożeń świadczy o tym, że każda instytucja lub indywidualny użytkownik gromadzący, przetwarzający i przesyłający dane musi liczyć się z ryzykiem związanym z ich kradzieżą. Najczęstszą przyczyną utraty danych nie jest samo „łamanie" zabezpieczeń przez hakerów, ale lekkomyślność i nieświadome użytkowanie sieci przez pracowników czy indywidualnych użytkowników (Grobel-Kijanka, 2015). Można więc uznać, że system bezpieczeństwa danych jest tak silny jak jego najsłabsze ogniwo. Powstaje pytanie, kogo uznać za najsłabsze ogniwo? Opierając się na doświadczeniach hakera K. Mitnicka, to „czynnik ludzki jest piętą achillesową systemów bezpieczeństwa" (Mitnick, Simon, 2003, s. 15). Zatem na pierwszy plan wysuwa się pozatechniczny aspekt bezpieczeństwa informacji – człowiek i jego świadomość dotycząca mechanizmów oraz użytkowania systemów informatycznych, a przede wszystkim po prostu Internetu.

Czynnik ludzki stwarza zagrożenie dla bezpieczeństwa danych, 3,03 mld ludzi, tj. blisko 42 proc. populacji, korzysta obecnie z Internetu (Kemp, 2015, s. 7). Samo przeglądanie przez użytkowników witryn internetowych pozostawia wyraźny ślad, tzw. *ciasteczka* są szybko, bez większego namysłu akceptowane – w przeciwnym razie strona może nam odmówić wyświetlenia treści. Akceptacja tych plików umożliwia

stworzenie *profilu użytkownika* oraz poznanie preferencji konsumenckich, a tym samym dostarczenie treści, które mogą nas zainteresować, mimo że świadomie nie wykazujemy tego zainteresowania. Na podstawie takich przykładów można stwierdzić, że współczesny człowiek nie osiągnął jeszcze na tyle wysokiego rozwoju w zakresie wyszukiwania, przetwarzania i efektywnego wykorzystywania dostępnych mu informacji (Cieślarczyk, 2016, s. 45). Niemal codziennie doświadcza się w sytuacjach życiowych zachowań, które są bezrefleksyjne i impulsywne oraz przeważają nad działaniami adekwatnymi do danej sytuacji. Można to zauważyć w momencie, kiedy większego znaczenia nabiera posiadany przez człowieka system norm, jego filozofia, charakter i w końcu – jego kultura bezpieczeństwa.

Rzeczywistość bezpieczeństwa współczesnego człowieka obejmuje infosferę (infosfera - ang. *infosphere* – dynamiczne środowisko przepływu informacji, w którym żyją ludzie). Jest to sfera ludzkiej działalności związana z gromadzeniem oraz przetwarzaniem informacji w środowisku komputerowym (https://www.lexico.com/definition/infosphere), gdzie można znaleźć przestrzeń do realizacji zadań grupowych i indywidualnych. Poprzez realizację tych zadań ludzie kształtują nowe relacje lub doskonalą stare, ale mogą też je niszczyć i *infekować* chorobami informacyjnymi (Batorowska, 2018c, s. 75-76). S. Jarmoszko umieszcza człowieka w sytuacji bez wyjścia - zagrożeń i ryzyka współczesności, jedno nie jest w stanie istnieć bez drugiego. Zwraca uwagę na to, że wraz z rozwojem społeczeństwa pojawia się zmiana kulturowa w sferze akceptowalności ryzyka, przechodzi się „(…) od kultury niskiej do kultury wysokiej tolerancji ryzyka" (Jarmoszko, 2012, s. 104). Aby poruszać się w infosferze, użytkownik powinien być jej świadomym twórcą, tym samym zmuszony jest do korzystania z technologii informatyczno-komunikacyjnych, a także opanowania różnych strategii informacyjnych niezbędnych w procesie zarządzania informacją. Użytkownicy rzadko są świadomi nakładanych na nich ograniczeń związanych z wpływem technologii informacyjnych. Mogą to być m.in. tendencyjne dobory słów kluczowych w wyszukiwarkach internetowych czy manipulowanie hierarchizacją stron WWW.

Obfitość informacji otaczających człowieka w dzisiejszym świecie zmusza go do ciągłej aktywności związanej z technologią, która ułatwia mu dostęp do informacji, ale jednocześnie zastępuje jego procesy myślowe. Ponadto *rozleniwia* użytkownika, a ten, wyręczany niemal na każdym kroku, nie zadaje sobie trudu weryfikacji źródeł czy też zaprzestaje analizy dostarczanych przez system informacji. Może to wynikać nie tyle z samej niechęci użytkownika, ale i z potopu informacyjnego, który go zalewa. Ciężko jest więc przetworzyć każdą z informacji, ze względu na tempo jej wytwarzania, które jest dużo większe niż możliwości przyswojenia ich przez mózg człowieka. Sytuacja ta pokazuje, w jakim pędzie technologicznym żyjemy, informacje są przez użytkownika jedynie bezrefleksyjnie skanowane. W poszukiwaniu potrzebnych danych opiera się on na powierzchownych kryteriach, na przykład tzw. słowach kluczach - tym samym analizuje wyłącznie fragmenty. Jednostka

żąda natychmiastowej odpowiedzi, podejmuje decyzje niepoparte wcześniejszym procesem analitycznym.

Dzisiejsze społeczeństwo otaczane jest przez ogrom informacji. To uniemożliwia zapanowanie nad ich nadmiarem, co może być przyczyną stresu informacyjnego. W konsekwencji, jeżeli nie posiada się kompetencji informacyjno-komunikacyjnych oraz zdolności analitycznych, może to doprowadzić do poczucia bezsilności (Batorowska, 2018b, s. 94).

Aby zapobiegać ww. niepożądanym zdarzeniom, ważne jest kształtowanie pewnych komponentów kultury bezpieczeństwa w obszarze zarządzania informacją i wiedzą. Należą do nich m.in. dysponowanie kompetencjami w zakresie pozyskiwania wiedzy o zagrożeniach, opowiadanie się za wartościami, na których można budować bezpieczeństwo jednostki i narodu, oraz umiejętność wykorzystywania emocji mobilizujących do przeciwdziałania zagrożeniom. W czasie ciągłych nacisków na zwiększenie bezpieczeństwa w niemal wszystkich obszarach życia nie można marginalizować znaczenia kultury bezpieczeństwa, w której obraca się człowiek. Szczególnie w czasach permanentnej inwigilacji, monitorowania użytkowników i handlu danymi pojawia się problem przetwarzania informacji, które pozwala na nieustanne kontrolowanie, nadzorowanie, ocenianie i sprawdzanie każdego człowieka w rolach, które odgrywa w codziennym życiu.

Pośpiech w codziennym życiu oraz pęd, jaki towarzyszy człowiekowi na co dzień, wymagają od jednostki bycia w ciągłym ruchu. Do tego stopnia, że godzi się ona na wszelkie zmiany zachodzące w jej życiu, bez względu na konsekwencje. Taki styl życia można nazwać konsumpcyjnym. Konsumuje się wszystko, a szczególnie napływające zewsząd informacje (Batorowska, 2018a, s. 71). W dzisiejszych czasach, posiadając informacje, wykorzystuje się je natychmiast, ale równie szybko zapomina. Mózg nie musi już ich zapamiętywać i gromadzić, od tego są nośniki. Najistotniejsze są informacje docierające w czasie rzeczywistym (Batorowska, 2018a, s. 72). Ilość informacji może być wręcz przytłaczająca, jest ich tyle, że jedna wypiera drugą, bez względu na jej wartość. Cenną umiejętnością jest poruszanie się w gąszczu informacji oraz zdolność selekcji. Będąc w nieustannym pośpiechu, informacje uznaje się za zweryfikowane w sposób intuicyjny, np. poprzez to, która najintensywniej przenika do naszej świadomości (Batorowska, 2018a, s. 73). Ogrom informacji zalewa społeczeństwo z każdej strony, dlatego niejednokrotnie świadomie rezygnuje się z weryfikacji ze względu na trudną dostępność danych czy czasochłonny proces ich poszukiwania. Kontrolowanie docierających wiadomości wymaga od człowieka specjalistycznych umiejętności informacyjnych (Batorowska, 2018a, s. 73). Zarządzanie linkami, szybkie poruszanie się w sieci między stronami internetowymi stanowi element pozyskiwania informacji, w tym zdobywania wiedzy. Jednostka skupia się na konsumowaniu dóbr i informacji odpowiadających jej preferencjom. Niekiedy takie zachowanie prowadzi do braku zaangażowania w sprawy społeczne i polityczne. Ignorancja ta może prowadzić do zagrożeń w wymiarze globalnym

(Batorowska, 2018a, s. 73). Wynika to z ignorancji decydentów oraz niewiedzy na temat ryzyka, przez co człowiek staje się ofiarą. Im bardziej kraj jest rozwinięty, tym bardziej narażony jest na ryzyko, które bywa niemożliwe do oszacowania. Jest ono zmienne i często niezdefiniowane (Batorowska, 2018a, s. 73).

W szerokim podejściu do problematyki bezpieczeństwa informacyjnego i miejsca człowieka w jego systemie należałoby skupić się na odporności człowieka na ataki informacyjne. W dzisiejszym świecie informacja podlega manipulacji i zniekształceniu, po to aby zdezinformować odbiorcę, który nieświadomie bierze udział w walce informacyjnej (Batorowska, 2018a, s. 75). Istotą tej walki jest podporządkowanie sobie przez agresora umysłu zaatakowanej osoby. Przewagą w niej jest umiejętność selekcjonowania otrzymanych wiadomości. Odbiorca, aby zachować bezpieczeństwo, powinien zastanowić się, czy wykorzystanie i posługiwanie się daną informacją jest bezpieczne dla niego samego oraz dla jego otoczenia. Ponadto powinien spróbować określić, czy informacja będzie oddziaływać na jego otoczenie pozytywnie, czy negatywnie (Batorowska, 2018a, s. 76).

Zjawisko to nie dotyczy jedynie jednostki, lecz także organizacji. W firmach kluczową rolę odgrywa ochrona informacji. Tam czujność pracowników na otrzymywane wiadomości musi być znacznie większa ze względu na znaczenie danych, których ujawnienie może negatywnie wpłynąć na funkcjonowanie firmy, a nawet doprowadzić do jej upadłości. Jak wynika z nowej edycji *CISCO Benchmark Study 2020*, rośnie liczba firm, w których aż 74 proc. pracowników umyślnie obchodzi systemy zabezpieczeń (http://globaleconomy.pl/). Co więcej, pracownicy korzystają ze smartfonów, tabletów i innych urządzeń mobilnych, które są trudne do ochrony przed atakiem (http://globaleconomy.pl/). Obecnie 42 proc. organizacji rezygnuje z wprowadzania innowacyjnych zabezpieczeń, tym samym rezygnując z ochrony przeciw zagrożeniami (http://globaleconomy.pl/). Zakłada się, że pracownicy są największym zagrożeniem dla bezpieczeństwa firmy.

Każdy indywidualny użytkownik Internetu ponosi ryzyko związane z kradzieżą danych. W bardzo szybkim tempie rośnie ilość zasobów dostępnych w Internecie, a w czasach, w których informacja jest towarem, przestępstwa internetowe są atrakcyjnym źródłem zysków. Dlatego ważne jest, aby każda z osób korzystająca z sieci miała świadomość zagrożeń w niej występujących. Niemal codziennie człowiek stwarza zagrożenia dla cyberbezpieczeństwa. Firma Ipswitch przeprowadziła badania, z których wynika, że 84 proc. pracowników korzysta z prywatnych e-maili w celu wysłania i odebrania plików służbowych, które są poufne. Osoby te nie robią tego świadomie, wynika to z ich niewiedzy lub braku kompetencji w zakresie dobrych praktyk dotyczących bezpieczeństwa informacji. Firma Kaspersky Lab przeprowadziła badania, z których wynika, że 40 proc. organizacji spotkało się z zatajeniem incydentu związanego z bezpieczeństwem IT (http://globaleconomy.pl/). Incydenty te dotyczyły odwiedzania niebezpiecznych stron komputerowych.

Człowiek jest kluczowym elementem bezpieczeństwa informacji, ale także najsłabszym. Szczególnie zauważalne może to być przy niskim wykształceniu, ludzie wtedy nie myślą o inwestowaniu w swoją przyszłość. Dostrzeganie szans, jakie niesie ze sobą rozwój cywilizacyjny, wiąże się z dostępem do informacji. Powinna ona być poparta rzetelną wiedzą i świadomością zachodzących mechanizmów, w tym zagrożeń.

Socjologiczne uwarunkowania bezpieczeństwa

Socjologia pozwala na objaśnienie rzeczywistości społecznej, która pozostaje niezmiernie złożonym systemem elementów. W strukturze uwarunkowań socjologicznych istnieje niezliczona ilość bytów, która warunkuje się, dopełnia i oddziałuje na siebie (Jaromoszko, Katalia, 2016, s. 128). Bezpieczeństwo jako idea, czynnik, proces i byt wypełnia przestrzenie społeczne. Jest jednym z podstawowych elementów, a nawet koniecznym do tego, aby zachować trwałość ukształtowanego ładu społecznego.

Warto zagłębić się w przeszłość, gdzie w przestrzeni filozoficznej można znaleźć cztery filary szeroko pojętego bezpieczeństwa, którymi są (Jagusiak, 2011, s. 65):

- prokreacja i edukacja,
- dostatek i dobrobyt,
- prawo (jako praworządność) i ustrój (zorganizowanie życia społeczno-politycznego,
- wolność i odpowiedzialność.

Idąc za słowami B. Jagusiaka: „Filary te implikowane są z natury człowieka, jej spełniania się i realizacji przeznaczenia lub powołania, albo funkcji, zadania itp." (Jagusiak, 2011, s. 65). Spełnianie się związane jest z wyzwaniami oraz problemami, które są nieodłącznym elementem naszego życia. Wartość społeczeństwa określana jest przez jego bezpieczeństwo w sferze moralnej i prawnej. Wynika to z tego, że obecne w życiu codziennym regulacje prawne, wytyczne czy sankcje niwelują wystąpienie stanu przeciwnego, jakim jest niebezpieczeństwo.

Aby lepiej zrozumieć socjologiczne uwarunkowania bezpieczeństwa, należy zwrócić uwagę na pierwsze przyczyny systemu społecznego, które zostały zaproponowane przez greckiego filozofa Arystotelesa, są to (Jagusiak, 2011, s. 65):

- zewnętrzna: materialna (budulcowa),
- wewnętrzna: sprawcza,
- zewnętrzna: formalna,
- wewnętrzna: celowa.

Ponadto filozoficzne pojmowanie bezpieczeństwa definiuje się poprzez trwanie przez prokreację i edukację (Jagusiak, 2011, s. 66). Przyczyny te oraz wcześniej wymienione elementy są ze sobą we wzajemnej relacji i stanowią o bezpieczeństwie (Jagusiak, 2011, s. 66).

Dzięki wiedzy z zakresu socjologii można ukształtować i wyznaczyć pewne instrumenty metodologiczne, które zapewniają brak zagrożeń w sytuacjach społecznych (Jagusiak, 2011, s. 129). Będą one nieco bardziej intuicyjne, ponieważ należy mieć wzgląd na to, że samo poczucie zagrożenia stanu bezpieczeństwa czy niepewności jest nieodłącznie związane z naszą egzystencją.

Idąc za słowami J. Maciejewskiego i D. Hofmana: „współczesny świat społeczny jest dynamicznym, bezustannie zmieniającym się procesem, prowadzącym do szeroko rozumianych zmian. Zjawiska m.in. takie jak: globalizacja, transformacja, regionalizacja przyczyniają się do powstania zależności pomiędzy różnymi kulturami i społeczeństwami, mają także wpływ na wszystkie elementy ich struktury" (Maciejewski, Hofman, 2014, s. 22). Oznacza to, że podejście do problematyki bezpieczeństwa z punktu socjologicznego jest wyzwaniem. Dla każdej z jednostek inną wartość będą miały zachodzące procesy społeczne. Mimo to socjologiczne podejście wskazuje, że poczucie bezpieczeństwa lub jego braku pojawia się wtedy, gdy istnieje zagrożenie cenionych przez nas wartości. Możemy do nich zaliczyć: zdrowie, życie, środowisko naturalne, funkcjonowanie zgodne z prawem czy inne sfery związane z rozumianą szeroko strefą publiczną (Jarmoszko, Katalia, 2016, s. 130). Jeżeli ww. wartości pozostawione zostaną bez nadzoru społecznego, należy spodziewać się zagrożenia bezpieczeństwa jednostek. Pomimo działań profilaktycznych, jakie podejmowane są na co dzień, nadal należy spodziewać się zagrożeń w obrębie różnych struktur społecznych. Istotnym faktem jest to, że „charakter zagrożeń jest zmienny strukturalnie, oznacza to, że w jednym obszarze zagrożeń przybywa, a w innym ubywa" (Jarmoszko, Katalia, 2016, s. 130). Wymusza to na władzy na wszystkich trzech poziomach jej sprawowania: ustawodawczym, wykonawczym i sądowniczym odpowiednie wcześniejsze przygotowanie oraz ustalenie kompetencji kadr zarządczych, tak aby zadbać o bezpieczeństwo militarne, paramilitarne czy cywilne państwa (Jarmoszko, Katalia, 2016, s. 130).

W kontekście bezpieczeństwa informacji pojawia się socjotechnika, która bazuje na naiwności i niewiedzy ludzi, żeby pozyskać poufne informacje (socjotechnika – ogół metod i działań zmierzających do uzyskania pożądanego zachowania jednostek i grup ludzkich, nauka o sposobach i wynikach świadomego wpływania na rzeczywistość społeczną; https://sjp.pwn.pl/). Te działania i metody polegają na wzbudzeniu zaufania poprzez grę na emocjach. Ich wątpliwie moralny charakter jest rodzajem ataku psychologicznego. Atakujący nakłania swoją ofiarę do wykonania jakiejś czynności. Socjotechnika nie jest niczym nowym, tak samo jak oszuści czy naciągacze. Jednak osoby odpowiedzialne za to działanie, najczęściej sprawnie działający informatycy, doskonale wiedzą, jak skuteczne jest użycie tych technik w Internecie. Umożliwia im to tzw. *wchodzenie w rolę*, czyli kreowanie zmyślonego scenariusza w celu przekonania ofiary do ujawnienia określonych informacji lub podjęcia konkretnych działań (Hadnagy, 2012, s. 104). Co więcej, odgrywanie roli, wcielanie się w kogoś innego stanowi nieodłączny element pracy socjotechnika.

Ch. Nickerson, światowej sławy socjotechnik, stwierdza, że wchodzenie w rolę nie polega na samym jej odegraniu, ale chodzi o faktyczne wcielenie się w daną osobę, „każda komórka ciała ma być tym, kogo udajesz" (Hadnagy, 2012, s. 104). Podstawowymi metodami socjotechniki są np. manipulacja, perswazja czy intensyfikacja lęku. Osoba, która chce uzyskać dostęp do naszych danych, bazuje nie tylko na emocjach, lecz także na intelekcie. Przykładem może być powoływanie się na dane statystyczne lub autorytety naukowe.

Jak twierdzi K. Mitnick: „(...) firma może wydać setki tysięcy dolarów na zapory sieciowe, szyfrowanie i inne technologie bezpieczeństwa, jednak, jeżeli atakujący znajdzie choć jedną podatną na sugestie osobę wewnątrz organizacji i osoba ta pozwoli sobą manipulować, wszystkie te pieniądze wyłożone na ochronę będą zmarnowaną inwestycją" (https://plblog.kaspersky.com/). Statystycznie cyberprzestępcy odchodzą już od przygotowywania ataków zaawansowanych z punktu technologicznego. Przestępcy mają świadomość, że za pomocą socjotechniki szybciej i być może niezauważenie dotrą do pożądanych danych. Niepokojący jest fakt, że istnieją strony internetowe, na których można poznać poszczególne techniki ataków, łącznie z przykładami, np. www.socialengineer.org.

W życiu codziennym, używając przekazu werbalnego, nieświadomie lub świadomie wpływamy na innych. Z punktu widzenia socjotechnika język nie jest na tyle dobrym narzędziem, ponieważ wraz z nim często świat przedstawiany jest subiektywnie. Dlatego przewagi socjotechnika można szukać w tym, że nie działa twarzą w twarz. Powołuje się lub wciela się w postać policjanta, lekarza, technika czy kolegi z pracy. Wszystkie te maski pomagają mu zbudować bliską więź z potencjalną ofiarą. Zaczyna wywierać presję, tak aby uzyskać pożądaną odpowiedź. Udaje się to ze względu na wymyśloną historię, która staje się kontekstem rozmowy. Podczas takiej konfrontacji nawet ułamek sekundy zawahania ze strony ofiary daje socjotechnikowi przewagę.

Ataki socjotechniczne w porównaniu z tymi cybernetycznymi mają przewagę ze względu na to, że *phishingowa* (*phishing* – zagrożenie polegające na wyłudzaniu prywatnych informacji ze szczególnym uwzględnieniem tych mogących przynieść korzyści materialne atakującemu. W tego rodzaju ataku wykorzystuje się elementy inżynierii społecznej; http://www.cyberbezpieczenstwo.pl/artykuly/co-to-phishing/) wiadomość e-mail może zostać wysłana do nieograniczonej liczby odbiorców. Wystarczy, że kilku nie będzie na tyle uważnych i kliknie w otrzymany link, który prowadzi do strony internetowej prowadzonej przez oszustów. Za pomocą sfabrykowanej strony przestępca otrzymuje dane, których nie wykrada, ale zostają podane dobrowolnie przez ofiarę. Za pomocą *phishingu* można dostać takie informacje jak: login, hasło, numer karty kredytowej. Najczęściej przestępca, aby wzbudzić zaufanie, podszywa się pod rozpoznawalną firmę lub instytucję.

Przez umiejętne uderzenie w czuły punkt – to jest życie rodzinne, zawodowe – można znaleźć cel idealny i najbardziej ułomny. Dlatego należy pamiętać, żeby

zawsze stosować zasadę ograniczonego zaufania. Ponadto nie wykonywać pewnych czynności automatycznie, np. pobierać plików nadesłanych w wiadomości e-mail. Powinno się zwracać uwagę na dane nadawcy, często adres zmieniony jest tylko o jedną literę lub zawiera niepełną nazwę firmy. Dodatkowo powszechne jest stosowanie sztuczek, np. zamiana litery „O" na „0" lub „l" na „1". Należy pamiętać, że jeżeli wiadomość od danej instytucji czy firmy budzi jakiekolwiek wątpliwości, istnieje możliwość kontaktu z jej przedstawicielem, np. za pomocą infolinii. Innym ważnym elementem jest zainstalowanie oprogramowania antywirusowego, które wraz z trzeźwym umysłem użytkownika może pomóc w uniknięciu stania się ofiarą ataku. *Phishing* może przybierać formę ściśle ukierunkowaną, co oznacza, że pomocna w dotarciu cyberprzestępcy do użytkownika może okazać się „lista życzeń" w sklepie internetowym czy „koszyk". Dlatego powinno się powstrzymać od umieszczania informacji na profilach społecznościowych (np. Facebook), gdyż to one mogą pomóc przestępcom określić preferencje interesanta, a także ustalić dokładną tożsamość.

Rola człowieka w zagrożeniach informacyjnych – autoświadomość mechanizmów manipulacyjnych

Zgodnie z artykułem 5 Konstytucji RP Rzeczpospolita zapewnia bezpieczeństwo swoim obywatelom (Konstytucja RP, 1997, art. 5). Wiąże się to z radzeniem sobie z postępującymi zagrożeniami, które mogą wpłynąć na chaos w strukturach państwowych i prywatnych. Bezpieczeństwo uznawane jest za proces, który zmienia się w zależności od rodzaju zagrożeń (Kubiak, Topolewski, 2016, s. 159). Mogą one wynikać z niewiedzy lub nieuwagi człowieka, a także być skutkiem nieznajomości oddziaływań manipulacyjnych.

Na potrzeby artykułu przeprowadzono badanie z wykorzystaniem metody ankiety internetowej. Za narzędzie badania posłużył kwestionariusz ankiety, mógł on zostać wypełniony przez wszystkich, którzy uzyskali dostęp do linku – niezależnie od płci, wieku, wykształcenia, miejsca zamieszkania oraz sytuacji zawodowej. W formularzu ankietowym znajdowały się 23 pytania, a w tym:

- pięć pytań związanych z metryczką,
- czternaście pytań ogólnych,
- cztery dotyczące dwóch fotografii przedstawiających wiadomości *phishingowe*.

Badanie zostało przeprowadzone w maju 2020 roku, trwało pięć dni. W tym czasie ankieta została wypełniona przez sto osób, które stanowią próbę badawczą. Metoda ankiety internetowej pozwoliła w szybki sposób zdobyć dane od respondentów. Celem badania było uzyskanie informacji o świadomości zagrożeń występujących w systemach informacyjnych, a także określenie wiedzy respondentów w temacie

bezpieczeństwa informacyjnego (treść ankiety stanowi załącznik do artykułu, dostępna jest na stronie internetowej: https://docs.google.com/forms/d/e/1FAIpQLScSTb_g3y12QhzOVjddaQgaIOQTzPjlYvZ61J-yusgzqd6cfA/viewform?gxids=7628).

Należy zaznaczyć, że przeprowadzone badanie nie może świadczyć o autoświadomości całego społeczeństwa polskiego, gdyż próba, na której zostało ono przeprowadzone, nie jest próbą właściwą. Jednak ze względu na ograniczenia czasowe, objętościowe, jak również możliwości materialne autorki uznały, że liczba stu respondentów stanowi grupę reprezentatywną dla przeprowadzenia niniejszych badań.

Jak wynika z badania, świadomość zagrożeń występujących w systemach informacyjnych jest niska, pomimo deklaracji respondentów zainteresowania tematem bezpieczeństwa informacyjnego. Zaskakujące jest to szczególnie w kontekście tego, że większość respondentów posiadała wykształcenie wyższe, była aktywna zawodowo oraz pochodziła z dużych aglomeracji miejskich. Zarówno ze względu na charakter pracy, jak i wykształcenie zdają sobie sprawę ze znaczenia informacji we współczesnym świecie, a mimo to dopuszczają się w swojej pracy wielu nieprawidłowości. Przykładowo, mimo deklaracji zainteresowania komunikatami podczas instalacji programów czy weryfikacji wiadomości, spora część z nich nie stosowała się do podstawowych zasad bezpieczeństwa w sieci – nie używała zmiennych haseł, nie korzystała z programów antywirusowych itp. Szczególnie zastanawiający jest fakt, że większość respondentów deklaruje brak zdania, jeżeli chodzi o pożyteczność szkoleń dotyczących bezpieczeństwa informacyjnego. Może to stać w opozycji do jednego z pytań dotyczących zachowań powodujących wyciek informacji. Znaczna część respondentów jako główne zagrożenie i zachowania powodujące wyciek informacji wskazała na niekompetentność pracowników. Podejmując próbę rozstrzygnięcia problemu, jakim jest niekompetentność w organizacji, być może mogłaby ona wynikać właśnie z braku odpowiednich szkoleń. Stanowią one szansę na zaznajomienie się z dobrymi praktykami oraz zagrożeniami występującymi w systemie bezpieczeństwa informacyjnego. Należy pamiętać, że do zdarzeń zagrażających bezpieczeństwu informacji dochodzi głównie przez błędy człowieka. Niewystarczająca wiedza czy brak świadomości jednostek doprowadzają do wycieku lub utraty ważnych z punktu funkcjonowania przedsiębiorstwa informacji. Pracownik powinien dbać przede wszystkim o bezpieczeństwo wokół siebie (chociażby zaczynając od zakrycia kamerki w komputerze, regularnych zmian hasła do kont służbowych czy nawet prywatnych, uważania, by w pośpiechu nie pozostawiać bez nadzoru w swoim miejscu pracy dokumentów zawierających istotne informacje itp.). Ujawnienie informacji chronionych nie musi być umyślne, może wynikać z niekompetencji lub niefrasobliwości. Niebezpieczniejsze staje się natomiast, jeżeli jest celowym działaniem, które zmierza do osiągnięcia korzyści np. politycznej lub dotyczy informacji istotnych z punktu widzenia obywateli, np. danych osobowych (Kubiak, Topolewski, 2016, s. 143).

Informacja drukowana na papierze, wypowiedziana czy przechowywana na nośniku informacji, jakim może być pendrive, stanowi istotny zasób wiedzy. Wiąże się to z nieustanną relacją, która zachodzi między człowiekiem a bezpieczeństwem informacyjnym – jeżeli chce on tę informację chronić. Zatem zainteresowanie problematyką bezpieczeństwa informacyjnego nie powinno słabnąć.

Z przeprowadzonego badania wynika, że ważnym elementem z punktu widzenia tego, co jeszcze można zrobić, aby udoskonalić bezpieczeństwo informacyjne w organizacji, jest prowadzenie działań informacyjnych dotyczących dobrych praktyk, kampanii czy ogólnodostępnych szkoleń, które umożliwiłyby poszerzenie wiedzy z zakresu bezpieczeństwa informacji i cyberbezpieczeństwa. Jak wynika z kwestionariusza, większość respondentów nie wie, gdzie powinno się zgłosić w razie wycieku informacji. Co więcej, połowa respondentów nie znała pojęć dotyczących przestępstw komputerowych, a co za tym idzie, jest bardziej podatna na stanie się ich ofiarą. O słuszności prowadzenia szkoleń oraz kampanii informacyjnych świadczy również fakt, że znacząca część respondentów nie korzysta wcale ze szkoleń dotyczących bezpieczeństwa informacyjnego, mimo iż połowa z nich uważa, że są one istotne.

Zakończenie

Postęp cywilizacyjny, który jest konsekwencją powstawania coraz nowszych zasobów informacji, wymusza na społeczeństwie stałe doskonalenie się. Proces komunikacji na przestrzeni lat uległ diametralnej zmianie i niesie ze sobą szczególny zbiór zagrożeń dla bezpieczeństwa informacyjnego. Zagrożenia te stale ewoluują, ze względu na rozwój społeczeństwa informacyjnego można je rozpatrywać w różnych obszarach, jednak najczęściej występującym jest obszar zagrożeń technologicznych. Pomimo zaawansowania technologicznego, licznych systemów informatycznych przetwarzających dane, wiele zależy od człowieka. Mimo że ma on wiedzę w danej dziedzinie, nie jest na tyle doskonały i stwarza potencjalne zagrożenie dla bezpieczeństwa informacyjnego. Dlatego tak ważnym elementem artykułu było określenie miejsca człowieka w systemie bezpieczeństwa informacyjnego oraz jego odporności na ataki informacyjne.

W sferze bezpieczeństwa informacyjnego pojawia się wiele wyzwań, na które należy odpowiedzieć jak najszybciej, ze względu na to, że te kraje, które w ciągu najbliższych lat wykorzystają swoją infrastrukturę informacyjną, będą miały szansę uzyskać trwałą przewagę na arenie międzynarodowej. Dodatkowo możliwe jest przekształcenie się obecnego społeczeństwa informacyjnego w cywilizację informacyjną. Wnioski takie nasuwają się ze względu na rosnącą rolę informacji, która nie tylko jest towarem, lecz także bronią. Ważne jest, aby podczas formowania się „nowej" cywilizacji organizacje zadbały o rzecz najistotniejszą, jaką jest zapewnienie środków bezpieczeństwa informacyjnego.

Zmiany zachodzące w dostępności do informacji wiążą się także z ciągłym doskonaleniem jej ochrony. Nie tylko systemowej, lecz także wynikającej z kompetencji człowieka. Dlatego warto na nim skupić uwagę i zastanowić się nad możliwymi metodami poszerzania jego kompetencji oraz ciągłej nauki. Potrzeba ta wynika z faktu, że bezpieczeństwo informacyjne stanowi proces, który warunkują zmiany technologiczne, a człowiek, aby stać na ich straży, musi być na bieżąco.

BIBLIOGRAFIA

[1] Batorowska, H., 2018a, Potrzeba edukacji w zakresie kultury bezpieczeństwa narodowego, *Bibliotheca Nostra*, 2/52.

[2] Batorowska, H., 2018b, Kultura bezpieczeństwa informacyjnego, *Edukacja–Technika–Informatyka*, 1/23.

[3] Batorowska, H., 2018c, Potrzeba edukacji w zakresie kultury bezpieczeństwa informacyjnego, *Śląski Kwartalnik Naukowy*, 2(52).

[4] Brzeziński, M., 2009, *Kategoria bezpieczeństwa*, [w:] Sulowski, S., Brzeziński, M. (red.), *Bezpieczeństwo wewnętrzne państwa. Wybrane zagadnienia*, Warszawa: Dom Wydawniczy Elipsa.

[5] Burgiewa-Czuma, S., Gawrol, K., 2011, *Definicje, właściwości i funkcje społeczeństwa informacyjnego*, Rzeszów: Uniwersytet Rzeszowski.

[6] Cieślarczyk, M., 2016, *Psychospołeczne i prakseologiczne aspekty bezpieczeństwa informacyjnego*, [w:] *Bezpieczeństwo informacyjne XXI wieku*, Siedlce: Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach.

[7] Department Of Defense Directive, 1996, *S-3600.1. Information Operations*, December.

[8] Dereń, A.M., 2001, *Prawna ochrona informacji w krajowym ustawodawstwie. Wybrane zagadnienia*, Bydgoszcz: OPO.

[9] FEHLER, W., 2015, Informacyjny wymiar zagrożeń dla bezpieczeństwa współczesnej Polski, *Przegląd Strategiczny*.

[10] Goban-Klas, T., 1988, Społeczeństwo niedoinformowane, *Polityka*, 22 (dodatek do numeru).

[11] Grobel-Kijanka, A., 2015, *Ochrona informacji niejawnych, biznesowych i danych osobowych*, Materiały XI Kongresu: *Czynnik ludzki jako kluczowy element systemów bezpieczeństwa informacji*, Katowice.

[12] Hadnagy, Ch., 2012, *Socjotechnika. Sztuka zdobywania władzy nad umysłami*, Gliwice: Onepress.

[13] Jagusiak, B., 2011, *Studia Bezpieczeństwa Narodowego*, Warszawa: Wojskowa Akademia Techniczna.

[14] Jarmoszko, S., Katalia, C., 2016, *Nauki społeczne wobec problemu bezpieczeństwa – wybrane zagadnienia*, Siedlce: Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach.

[15] Kemp, S., 2015, *Digital, Social, and Mobile in APAC*.

[16] *Konstytucja Rzeczypospolitej Polskiej* z dnia 2 kwietnia 1997 r.

[17] Kubiak, M., Topolewski, S., 2016, *Bezpieczeństwo informacyjne w XXI w.*, Siedlce: Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach.

[18] Liedel, K., 2008, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń: Adam Marszałek.

[19] Łoś-Nowak, T., 2003, *Bezpieczeństwo*, [w:] Antoszewski, A., Herbut, R. (red.), *Leksykon politologii*, Wrocław: Alta 2.

[20] Łuczak, J., Tyburski, M., 2009, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC*, Poznań.

[21] Maciejewski, J., Hofman, D., 2014, *Grupy dyspozycyjne wobec zagrożeń bezpieczeństwa w perspektywie socjologicznej*, [w:] Bogdalski, P., Bukowiecka, D., Częścik, R., Zdrodowski, B. (red.), *Grupy dyspozycyjne społeczeństwa w świetle potrzeb bezpieczeństwa państwa. Tom 1. Teoretyczne aspekty przygotowania i funkcjonowania grup dyspozycyjnych państwa*, Szczytno: WSP.

[22] Mitnick, K., Simon, W., 2003, *Sztuka podstępu. Łamałem ludzi, nie hasła*, Gliwice: Helion.

[23] Ołoszyn, J., Lula, P., 2001, *Informatyczne metody i środki ochrony zasobów informacyjnych przedsiębiorstwa*, [w:] Borowiecki, R. (red.), *System informacji strategicznej. Wywiad gospodarczy a konkurencyjność przedsiębiorstwa*, Warszawa: Difin.

[24] Raport Mediarecovery, 2013, *Efektywne zarządzanie bezpieczeństwem informacji*.

[25] *Słownik terminów z zakresu bezpieczeństwa narodowego*, 2002, Warszawa: AON.

[26] Szczepaniuk, H., 2014, *Wybrane problemy bezpieczeństwa informacyjnego państwa*, XX Forum Teleinformatyki.

[27] Szmyd, J., 2014, Poczucie bezpieczeństwa jako wartość społeczna, etyczna i egzystencjalna. Rozważania podstawowe, *Państwo i Społeczeństwo*, (XIV)2.

[28] Ustawa z dnia 23 kwietnia 1964 r. *Kodeks cywilny* (Dz.U.2019.0.1145).

[29] Więcaszek-Kuczyńska, L., 2015, Wybrane regulacje prawne w obszarze zagrożeń bezpieczeństwa informacyjnego, *Obronność. Zeszyty Naukowe*, Część II.

[30] Zięba, R., 2008, *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Warszawa: Wydawnictwa Akademickie i Profesjonalne.

NETOGRAFIA

[1] https://azure.microsoft.com/pl-pl/overview/what-is-cloud-computing/ (5.12.2019).

[2] https://www.rpo.gov.pl/pl/content/opinia-rpo-w-sprawie-projektu-ustawy-o-jawnosci-zycia-publicznego (13.11.2019).

[3] https://www.dailymail.co.uk/sciencetech/article-5147871/Social-networking-sites-controlling-mind.html (14.12.2019).

[4] https://mfiles.pl/pl/index.php/U%C5%BCyteczno%C5%9B%C4%87_informacji (13.03.2020).

[5] http://rocznikikae.sgh.waw.pl/p/roczniki_kae_z44_01.pdf, s. 12.

[6] http://globaleconomy.pl/doradztwo-biznesowe/porady-biznesowe/33900-rekomenduje-coraz-wiecej-firm-cierpi-na-tzw-cyberzmeczenie-przestaja-scigac-sie-z-hakerami-m-pastewski-dyrektor-ds-sprzedazy-rozwiazan-cyberbezpieczenstwa-cisco-systems-polska-l-bromirski-dyrektor-w-dziale-rozwiazan-bezpieczenstwa-cisco-systems-polska (4.04.2020).

[7] https://plblog.kaspersky.com/socjotechnika-lamanie-systemu-operacyjnego-czlowieka/750/ (5.04.2020).

[8] https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/ (21.05.2020).

[9] https://niebezpiecznik.pl/post/wyciek-danych-z-politechniki-warszawskiej-nazwiska-dane-kontaktowe-oceny/ (21.05.2020).

[10] https://docs.google.com/forms/d/e/1FAIpQLScSTb_g3y12QhzOVjddaQgaIOQTzPjlYvZ61J--yusgzqd6cfA/viewform?gxids=7628 (21.05.2020).

[11] https://legislacja.rcl.gov.pl/projekt/12304351 (13.11.2019).

[12] https://sjp.pwn.pl/sjp/bezpieczenstwo;2443939.html (5.12.2019).

[13] https://www.lexico.com/definition/infosphere (4.04.2020).
[14] https://sjp.pwn.pl/slowniki/socjotechnika.html (5.04.2020).
[15] https://www.gov.pl/web/cyfryzacja/rodo-informacje (30.04.2020).
[16] www.theguardian.com/new/2018/mar/17/cambridge-analytica (13.11.2019).
[17] https://panoptykon.org/wiadomosc/dane-w-chmurze-czyli-gdzie (5.12.2019).
[18] http://www.cyberbezpieczenstwo.pl/artykuly/co-to-phishing/ (5.04.2020).