Jacek Gerwatowski
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
ORCID: 0000-0002-9127-7528

Bezpieczeństwo informacyjne w jednostkach samorządu terytorialnego

Wprowadzenie

W obecnej chwili wykorzystanie komputera jako narzędzia pracy, komunikacji czy rozrywki jest niemal powszechne. Jednak niestety bardzo często poziom świadomości użytkowników na temat tego, jak przebiega proces wymiany informacji w sieci jest zbyt niski. Co za tym idzie niezadowalająca jest też wiedza dotycząca zagrożeń i pułapek związanych z nieodpowiednim użytkowaniem narzędzi, jakim są Internet i systemy informatyczne. Rodzajów zagrożeń, które czyhają na nieświadomego użytkownika komputera podłączonego do Internetu jest naprawdę wiele. Można zaryzykować stwierdzenie, że nawet najlepsze oprogramowanie antywirusowe nie gwarantuje bezpieczeństwa, jeżeli użytkownik nie ma świadomości potencjalnych zagrożeń. Co więcej, jeśli mamy do czynienia z brakiem świadomości zagrożeń ze strony użytkownika, lub z ich bagatelizowaniem, zasadnym wydaje się stwierdzenie, że to człowiek staje się w tej sytuacji najsłabszym punktem systemu. Wykonywanie zadań, zarówno przez jednostki samorządu terytorialnego, jak i przedsiębiorstwa komercyjne, wymaga najczęściej przetwarzania związanych z nimi zbiorów danych. Proces ten wymaga zaangażowania zasobów organizacji o wymiernej wartości. Straty związane z naruszeniem bezpieczeństwa informacji trudno oszacować. W rezultacie możemy mieć do czynienia z różnego typu następstwami – utratą płynności funkcjonowania organizacji, utratą własności intelektualnej, koniecznością wypłacenia odszkodowań oraz konsekwencjami prawnymi[1]. W odróżnieniu od tak zwanych „przeciętnych użytkowników" urzędnik powinien cechować się wyższym poziomem świadomości możliwych zagrożeń i co z tego wynika, być na nie podatny w zdecydowanie mniejszym stopniu. Zagrożenia bezpieczeństwa systemów

[1] P. Jatkiewicz, *Uwarunkowania zarządzania systemem bezpieczeństwa informacji w jednostkach samorządu terytorialnego*, praca doktorska, Uniwersytet Gdański, 2012, s. 8; T. Szatkowski (red.), *Bezpieczeństwo danych w sektorze publicznym*, Warszawa 2016, s. 57.

informatycznych, niezależnie od ich źródła, wywołane zarówno wskutek działań przestępczych, działań terrorystycznych czy niezamierzonych błędów, w szerszej skali mogą prowadzić do powstania zakłóceń w świadczeniu usług, które są dzisiaj uznawane za podstawowe, czyli w dostawach wody, usługach z zakresu opieki zdrowotnej, dostawach energii elektrycznej i usługach telefonii komórkowej.[2]

Mamy do czynienia z sytuacją, w której w coraz większym stopniu codzienne życie, interakcje społeczne i gospodarka uzależnione są od sprawnie funkcjonujących technologii informacyjno-komunikacyjnych. Technologie te stanowią obecnie fundament wzrostu gospodarczego i są zasobem o krytycznym znaczeniu. Opierają się na nich praktycznie wszystkie sektory gospodarki, począwszy od sektora finansowego, poprzez opiekę zdrowotną, energetykę i transport. Funkcjonowanie biznesu w wielu przypadkach opiera się na nieprzerwanej dostępności Internetu i na sprawnym funkcjonowaniu systemów informatycznych[3]. Należy rozgraniczyć pojęcia bezpieczeństwo informatyczne i bezpieczeństwo informacyjne. Chociaż są one ze sobą powiązane, nie należy używać ich zamiennie, ponieważ są to dwa odrębne pojęcia, pomiędzy którymi występują istotne różnice.

1. Pojęcie bezpieczeństwa w wymiarze informacyjnym i informatycznym

Pojęcie bezpieczeństwa może być definiowane w dwojaki sposób: w ujęciu negatywnym jako stan, w którym istotne z punktu widzenia podmiotu wartości nie są zagrożone, czyli jako przeciwieństwo zagrożenia. Bezpieczeństwo w ujęciu pozytywnym obejmuje kształtowanie pewności przetrwania, posiadania i swobód rozwojowych podmiotu, czyli jest rozumiane jako stan umożliwiający jednostce kreatywny rozwój[4]. Bezpieczeństwo nie jest danym „raz na zawsze" stanem mającym trwały charakter. Wręcz przeciwnie – jest dynamicznym, podlegającym ciągłym zmianom procesem społecznym, w ramach którego podmioty starają się doskonalić mechanizmy zapewniające im poczucie bezpieczeństwa. Bezpieczeństwo może być analizowane jedynie w określonym przedziale czasowym. Nie ma możliwości osiągnięcia „całkowitego bezpieczeństwa". Termin bezpieczeństwo jest pojęciem, które może być analizowane na wielu zróżnicowanych płaszczyznach. Na każdej płaszczyź-

[2] Zob. Wspólny Komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń* z dnia 7.02.2013, s. 3.

[3] Ibidem, s. 2.

[4] K. Gołaś, *Pojęcie bezpieczeństwa*, http://geopolityka.net/pojecie-bezpieczenstwa/ (data dostępu: 25.09.2019).

nie mogą istnieć luki w systemie bezpieczeństwa, powodujące spadek jego poziomu.

Pojęcie „bezpieczeństwo informacyjne" nie doczekało się jednoznacznej wykładni. Często bywa błędnie utożsamiane z bezpieczeństwem informatycznym. W rezultacie tego sposobu rozumienia problemu informacja byłaby chroniona jedynie tam, gdzie ma ona postać elektroniczną. Tymczasem na bezpieczeństwo informacyjne składa się szereg innych procesów, w trakcie których informacja jest generowana, modyfikowana i przesyłana (także w formie werbalnej)[5]. Problematyka bezpieczeństwa informacyjnego obejmuje zarówno zabezpieczenia przed niepożądaną ingerencją w informacje i dane osobowe, jak również formy zabezpieczenia systemów teleinformatycznych przed destrukcyjnymi działaniami zewnętrznych i wewnętrznych obiektów.

Jednym z warunków bezpieczeństwa informacyjnego jest uzasadnione zaufanie podmiotu do jakości oraz dostępności pozyskiwanej i wykorzystywanej informacji, pojęcie bezpieczeństwa informacyjnego dotyczy zatem podmiotu (człowieka, organizacji), który może być zagrożony utratą zasobów informacyjnych albo otrzymaniem informacji o nieodpowiedniej jakości[6].

Z pojęciem bezpieczeństwa związane są terminy: wyzwanie, szansa, ryzyko oraz zagrożenie. Wyzwanie jest pojęciem o najszerszym znaczeniu, zawierającym w sobie zarówno szanse, jak i zagrożenia. Wyzwanie można zdefiniować jako określoną sytuację lub informację o tej sytuacji. To, czy stanie się ono szansą, czy zagrożeniem, zależy od tego, czy we właściwym miejscu i czasie ta informacja zostanie właściwie odczytana i zinterpretowana, w efekcie czego zostaną podjęte adekwatne działania. Jeśli tak się dzieje, wyzwanie staje się szansą. W przeciwnym razie może stać się zagrożeniem[7].

W związku z rozwojem elektroniki, powszechnością urządzeń zapewniających dostęp do Internetu, rozwojem sieci społecznościowych, informacja stała się narzędziem, czynnikiem dającym wiedzę, ale i mającym decydujący wpływ na bezpieczeństwo obywateli, organizacji, a nawet całych państw. Należy zwrócić uwagę nie tylko na pozytywny, ale i negatywny aspekt rozwoju nowych technologii. Postęp techniczny powoduje zmianę natury zagrożeń na świecie, gdyż w czasach powszechnego dostępu do technik informatycznych, rodzą się nowe niebezpieczeństwa[8]. Są one ściśle powiązane

---

[5] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 22, L Więcaszek-Kuczyńska, *Wybrane regulacje prawne w obszarze zagrożeń bezpieczeństwa informacyjnego. Część pierwsza. Obronność*, „Zeszyty Naukowe" 3 (11)/2014, s.141.

[6] K. Liderman, op. cit., s. 22.

[7] Por. M. Cieślarczyk, *Kultura bezpieczeństwa i obronności*, Siedlce 2011, s. 120–122.

[8] K. Liderman, op. cit., s. 21–22.

z użytkowaniem sieci informatycznych i systemów informacyjnych, np. przestępstwa wykorzystujące komputer jako narzędzie, utrata informacji związana z włamaniami komputerowymi, złośliwymi kodami i wirusami, szpiegostwem czy sabotażem. Przykładem nowego rodzaju zagrożeń jest cyberterroryzm[9].

Cyberprzestępczość[10] jest jedną z najszybciej rozwijających się form przestępczości. Sprzyja temu specyficzny charakter sieci globalnej, który pozwala na częściową anonimowość sprawcy przestępstwa oraz łatwość dostępu do sieci. Jak wynika z danych policji w Polsce, w 2010 r. zgłoszono prawie 8 tysięcy przestępstw popełnionych w sieci, z czego w ponad 6 tysiącach przypadków zgłoszenia dotyczyły oszustw. W 2012 r. ogólna liczba przestępstw komputerowych oscylowała na poziomie 19 tysięcy, z czego około 3/4 przypadków stanowiły oszustwa. Według danych z 2015 r. liczba ta przekroczyła 20 tys. Znaczna liczba przestępstw komputerowych pozostaje ukryta w szarej strefie i nie zostaje ujęta w statystykach[11]. Specyficzny charakter przestępstw popełnianych w cyberprzestrzeni powoduje, że wiele tego typu czynów pozostaje niewykrytych lub nie są one poprawnie identyfikowane jako przestępstwa. Można założyć, że powodem takiego stanu rzeczy jest, z jednej strony, sam użytkownik komputera lub innego urządzenia, który nie zdaje sobie sprawy z tego, że padł ofiarą przestępstwa, z drugiej zaś zdarzenia, które są wykrywane i poprawnie kwalifikowane jako przestępne, ale nie zawsze zostają zgłoszone do ścigania[12]. Według danych z 2011 r. łączna wartość globalnych strat ponoszonych na skutek popełniania cyberprzestępstw kształtuje się na poziomie 388 miliardów dolarów rocznie. Kluczowe dla zapewnienia bezpieczeństwa jest to, by właściwe podmioty były w stanie odpowiednio szybko zdefiniować źródło potencjalnych zagrożeń i podjąć adekwatne działania[13]. Niewystarczająca liczba pracowników, wykwalifikowanych w dziedzinie bezpieczeństwa informacyjnego, brak systemu finansowania przedsięwzięć na rzecz zapewnienia bezpieczeństwa informacyjnego czy brak

[9] Cyberprzestępczość obejmuje różnego rodzaju działalność, w której komputery i systemy informatyczne są wykorzystywane jako podstawowe narzędzie przestępcze lub są głównym celem działania przestępczego. Obejmuje tradycyjne przestępstwa (np. nadużycia finansowe, fałszerstwa), przestępstwa związane z treściami (np. dystrybucja w sieci pornografii dziecięcej) oraz przestępstwa typowe dla komputerów i systemów informatycznych (np. ataki na systemy informatyczne, w tym ataki prowadzące do zablokowania usług/systemów, oraz złośliwe oprogramowanie).

[10] Por. K. Krassowski, *Kilka uwag o kryminalistyce w świecie informacji cyfrowej oraz stojących przed nią wyzwaniach*, „Studia Prawnoustrojowe" 2015, s. 153–154.

[11] Zob. M. Kliś, *Przestępczość w Internecie. Zagadnienia podstawowe*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1.

[12] J. Wasilewski-*Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, https://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-7/1304,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-15-8-2016.html (data dostępu: 25.09.2019).

[13] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006, s. 7.

efektywnego systemu kształcenia i szkolenia w zakresie bezpieczeństwa informacyjnego, stanowią potencjalne ryzyko[14].

Na podstawie przytoczonych informacji, z dużym prawdopodobieństwem można wnioskować, że skala zysków, które potencjalnie generuje cyberprzestępczość czyni ten rodzaj działalności jedną z najbardziej dochodowych gałęzi przestępczości. Proceder ten przyciąga nie tylko drobnych złodziei czy oszustów, lecz także cybergangi, które wyspecjalizowały się w nowoczesnych technologiach lub „konwencjonalne", zorganizowane grupy przestępcze, które chcą rozszerzyć swoją działalność. Przestępstwa dokonywane w cyberprzestrzeni zapewniają sprawcy wyższy poziom bezpieczeństwa niż inny rodzaj działalności przestępczej – zarówno jeśli chodzi o wymiar sprawiedliwości, ale również działania innych przestępców[15]. Techniki stosowane w cyberprzestępczości rozwijają się coraz szybciej, organy ścigania nie są w stanie zwalczać cyberprzestępczości przy użyciu przestarzałych narzędzi operacyjnych. Każdy słaby punkt systemów informatycznych może okazać się dla przestępcy potencjalnym atutem.

Zgodnie ze statystykami prowadzonymi przez policję, w 2016 r. stwierdzono 218 przestępstw dotyczących ujawnienia tajemnicy służbowej i zawodowej[16], w 139 przypadkach zostało wszczęte postępowanie. W tym samym roku zostało wszczętych 3401 postępowań dotyczących naruszenia tajemnicy korespondencji[17], w 2718 przypadkach stwierdzono popełnienie przestępstwa. W przypadku udaremniania lub utrudniania korzystania z informacji stwierdzono popełnienie 789 przestępstw tego rodzaju. Popełnienie przestępstw związanych z niszczeniem danych informatycznych stwierdzono w 6 przypadkach. W przypadku sabotażu komputerowego stwierdzone zostało popełnienie 38 przestępstw. Z kolei przestępstwo dotyczące wytwarzania programów komputerowych, służących do popełniania przestępstw, stwierdzono w 39 przypadkach[18]. Natomiast jeśli chodzi o rok 2017, postępowanie zostało wszczęte w 374 przypadkach, stwierdzono 179 przestępstw, wykryto 114. Globalna liczba przestępstw komputerowych w 2018 r. to 700 milionów[19].

---

[14] Doktryna Bezpieczeństwa Informacyjnego RP, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf (data dostępu: 25.09.2019); D. Sołodow, *Regulacje prawne dotyczące bezpieczeństwa w sieci Internet (na przykładzie prawa internetowego Federacji Rosyjskiej)*, „Studia Prawnoustrojowe" 2016, nr 31, s. 197–208.

[15] J. Wasilewski, *Cyberprzestępczość. Wybrane aspekty prawnokarne i kryminalistyczne*, praca doktorska, Uniwersytet w Białymstoku 2017, s. 74.

[16] Art. 266 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz.U. z 1997 r. Nr 88, poz. 553).

[17] Ibidem, art. 267.

[18] Przestępstwa przeciwko ochronie informacji, http://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-14 (data dostępu: 25.09.2019).

[19] A. Bera, *83 przerażające statystyki dotyczące cyberprzestępczości*, https://safeatlast.co/blog/cybercrime-statistics/ (data dostępu: 25.09.2018).

Zwalczanie cyberprzestępczości w państwach członkowskich Unii Europejskiej jest wspierane między innymi przy pomocy programów finansowania, w identyfikowaniu braków i zwiększaniu zdolności w zakresie prowadzenia dochodzeń i zwalczania cyberprzestępczości[20]. Komisja wspiera organy zapewniające kontakty między środowiskiem naukowym/akademickim, podmiotami odpowiedzialnymi za egzekwowanie prawa i sektorem prywatnym. Współpracuje również z utworzonym w ramach Europolu, Europejskim Centrum ds. Walki z Cyberprzestępczością (EC3) oraz z Eurojustem, w celu dostosowania rozwiązań politycznych do najlepszych praktyk z punktu widzenia operacyjnego[21]. Z uwagi na wielowymiarowy charakter zagrożeń należy wykorzystywać synergię między cywilnymi i wojskowymi koncepcjami dotyczącymi ochrony krytycznych zasobów cybernetycznych. Działania te powinny być wspierane przez bliższą współpracę między rządami, sektorem prywatnym i środowiskiem akademickim w UE oraz prace badawczo-rozwojowe[22]. Wsparciem w tych działaniach ma być program „Horyzont 2020"[23]. Podstawę współpracy międzynarodowej w dziedzinie zwalczania cyberprzestępczości stanowi konwencja budapeszteńska. Współpraca obejmuje między innymi wymianę najlepszych praktyk, dzielenie się informacjami, wydawanie wczesnych ostrzeżeń, wspólne ćwiczenia w zakresie reagowania na incydenty.

Istotną regulacją w zakresie cyberbezpieczeństwa jest Rozporządzenie Parlamentu Europejskiego i Rady UE 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie).

ENISA, m.in. poprzez oferowane doradztwo i pomoc, niezależność naukowo-techniczną oraz przejrzystość procedur działania, ma stanowić ośrodek wiedzy fachowej w dziedzinie cyberbezpieczeństwa. Katalog zadań i celów ENISA jest obszerny. Jako przykładowe cele ENISA można wymienić[24]:

– wsparcie w zakresie budowy potencjału i gotowości w całej Unii, poprzez pomoc instytucjom, organom i jednostkom organizacyjnym Unii, jak

[20] W 2013 r. – w ramach programu „Zapobieganie i walka z przestępczością" (ISEC). Po 2013 r. – w ramach Funduszu Bezpieczeństwa Wewnętrznego (instrument w ramach wieloletnich ram finansowych).

[21] Zob.: Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń z dnia 7.02.2013, s. 11–14.

[22] Zob. ibidem, s. 13.

[23] Zob. Horyzont 2020, http://www.kpk.gov.pl/?page_id=59 (data dostępu: 25.09.2019).

[24] Szerzej na ten temat zob. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17.04.2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie).

również państwom członkowskim oraz interesariuszom z sektora publicznego i prywatnego w zwiększeniu ochrony ich sieci i systemów informatycznych, tworzeniu i ulepszaniu cyberodporności i zdolności reagowania oraz w rozwijaniu umiejętności i kompetencji w dziedzinie cyberbezpieczeństwa;

– propagowanie współpracy, w tym wymiany informacji i koordynację na poziomie unijnym, pomiędzy państwami członkowskimi, instytucjami, organami i jednostkami organizacyjnymi Unii oraz odpowiednimi interesariuszami z sektora publicznego i prywatnego w kwestiach związanych z cyberbezpieczeństwem;

– przyczynianie się do zwiększania zdolności w zakresie cyberbezpieczeństwa na poziomie unijnym w celu wspierania działań państw członkowskich służących zapobieganiu cyberzagrożeniom i reagowaniu na nie, w szczególności w przypadku incydentów transgranicznych;

– propagowanie wysokiego poziomu wiedzy na temat cyberbezpieczeństwa, w tym cyberhigienę i umiejętności cyfrowe wśród obywateli, organizacji i przedsiębiorstw.

Z kolei do zadań ENISA należy między innymi[25]:

– wspieranie państw członkowskich przy wdrażaniu konkretnych, dotyczących cyberbezpieczeństwa, aspektów polityki i prawa Unii, związanych z ochroną danych i prywatnością, w tym poprzez zapewnianie doradztwa Europejskiej Radzie Ochrony Danych na jej wniosek;

– pomoc państwom członkowskim w ich staraniach na rzecz poprawy w zakresie zapobiegania cyberzagrożeniom i incydentom, ich wykrywania i analizowania oraz zdolności reagowania na cyberzagrożenia i incydenty – poprzez zapewnianie państwom członkowskim wiedzy fachowej;

– udzielanie pomocy państwom członkowskim w opracowywaniu krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych, jeżeli zwrócono się o taką pomoc na podstawie art. 7 ust. 2 dyrektywy (UE) 2016/1148, oraz promowanie działania na rzecz upowszechniania tych strategii i odnotowywanie postępów w ich wdrażaniu w całej Unii w celu propagowania najlepszych praktyk;

– przeprowadzanie analizy powstających technologii i przedstawianie tematycznych ocen dotyczących spodziewanego społecznego, prawnego, gospodarczego i regulacyjnego wpływu innowacji technologicznych na cyberbezpieczeństwo.

E. Nowak i M. Nowak definiują bezpieczeństwo informacyjne jako stan warunków zewnętrznych i wewnętrznych dopuszczających, aby państwo swobodnie rozwijało swoje społeczeństwo informacyjne Za warunki osiągnięcia bezpieczeństwa informacyjnego przywołani autorzy przyjmują:[26]

---

[25] Ibidem.

[26] L. Więcaszek-Kuczyńska, *Zagrożenia bezpieczeństwa informacyjnego, obronność*, „Zeszyty Naukowe" 2 (10)/2014, s. 4.

– niezagrożone strategiczne zasoby państwa;

– decyzje organów władzy podjęte na podstawie wiarygodnych, istotnych informacji;

– niezakłócony przepływ informacji pomiędzy organami państwa;

– niezakłócone funkcjonowanie sieci teleinformatycznych tworzących krytyczną infrastrukturę teleinformatyczną państwa;[27]

– zagwarantowaną przez państwo ochronę informacji niejawnych i danych osobowych obywateli;

– zasadę, że prawo do prywatności obywateli jest nienaruszane przez instytucje publiczne;

– swobodny dostęp obywateli do informacji publicznej.

Pojęcie bezpieczeństwa informacyjnego jest stosowane także do informacji spoza systemu teleinformatycznego, pojawiających się na nośnikach kiedyś standardowych, np. dokumentach papierowych, mikrofilmach, a polityka bezpieczeństwa informacji obejmuje proces korzystania z informacji bez względu na sposób jej przetwarzania i dotyka zarówno systemów prowadzonych tradycyjnie (archiwa, kartoteki, dokumenty papierowe), jak i systemów komputerowych[28].

W skład systemu teleinformatycznego wchodzą urządzenia, narzędzia, metody postępowania i procedury stosowane przez wyspecjalizowanych pracowników, w sposób zapewniający bezpieczne wytwarzanie, przechowywanie, przetwarzanie lub przekazywanie informacji[29]. Sieć teleinformatyczna to organizacyjne i techniczne połączenie systemów teleinformatycznych[30]. Sieci i systemy służące do przetwarzania informacji niejawnych podlegają akredytacji bezpieczeństwa teleinformatycznego przez służby ochrony państwa.

2. Klasyfikacja zagrożeń bezpieczeństwa informacyjnego

Zagrożenia można sklasyfikować w następujący sposób[31]:

– siły natury (pożar, powódź, epidemie), błędy ludzi i ich działania według błędnych lub niewłaściwych procedur, celowe, szkodliwe działanie ludzi, awarie sprzętu komputerowego, awarie oprogramowania, awarie zasilania;

---

[27] Do infrastruktury krytycznej państwa zaliczane są między innymi systemy informacyjne państw i przedsiębiorstw.

[28] A. Nowak, W. Scheffs, *Zarządzanie bezpieczeństwem informacyjnym*, Warszawa 2010, s. 40.

[29] Art. 3 ustawy z dnia 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005 r. Nr 64, poz. 565).

[30] Zob. *Sieć teleinformatyczna*, http://www.archiwistyka.pl/artykuly/slownik/siec_teleinformatyczna (data dostępu: 25.09.2019).

[31] P. Bączek, *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006, s. 72–73.

– zagrożenia losowe – klęski żywiołowe, katastrofy, wypadki, które wpływają na stan bezpieczeństwa informacyjnego organizacji (np. pożar budynku, w którym przechowywane są nośniki informacji);

– tradycyjne zagrożenia informacyjne – szpiegostwo, działalność dywersyjna lub sabotażowa, ofensywa dezinformacyjna prowadzona przez obce państwa lub osoby, podmioty, organizacje;

– zagrożenia technologiczne – zagrożenia związane z gromadzeniem, przetwarzaniem i przekazywaniem informacji w sieciach teleinformatycznych (m. in. cyberterroryzm);

– zagrożenia odnoszące się do praw obywatelskich osób lub grup społecznych, m.in. sprzedaż informacji, przekazywanie informacji podmiotom nieuprawnionym, naruszanie przez władze prywatności, bezprawne ingerencje służb specjalnych, ograniczenie jawności życia publicznego.

Przykładowymi technikami włamań do systemów informacyjnych są[32]:

– celowe inicjowanie awarii;

– wywoływanie fałszywych alarmów (uśpienie czujności);

– atak słownikowy[33];

– wirusy, robaki[34], konie trojańskie, inne aplikacje destabilizujące sprawność sytemu;

– programy wykorzystujące błędy w systemach operacyjnych i oprogramowaniu użytkowym;

– nieuprawnione ujawnienie informacji, tzw. wyciek lub przeciek;

– działalność grup celowo manipulujących przekazem informacji;

– walka informacyjna[35].

Często sami możemy zaobserwować działania, które przez brak wiedzy lub świadomości użytkowników prowadzą do ujawnienia bądź utraty ważnych informacji, np. tak oczywiste działania, jak naklejenie na monitor kartki z hasłami dostępu do stanowiska pracy, kont czy portali społecznościowych, bałagan na biurku, pozostawianie bez nadzoru dokumentów firmowych, finansowych lub handlowych, wyrzucanie na śmietnik korespondencji z istotnymi dla podmiotu informacjami, zagubienie nośnika danych. Informacje takie, jak wyniki sprzedaży, oferty, dane osobowe i finansowe, prawnie zastrzeżone szczegóły techniczne, plany podróży i transportu oraz wiele

---

[32] A. Żebrowski, W. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Kraków 2000, s. 73.

[33] Zob. Securelist, *atak słownikowy*, https://www.securelist.pl/glossary/7415,atak_slownikowy.html (data dostępu: 25.09.2019).

[34] Zob. Omegasoft, *Jak działa robak komputerowy,* https://www.omegasoft.pl/Robak-komputerowy (data dostępu: 25.09.2019).

[35] A. Żebrowski, *Walka informacyjna wsparciem terroryzmu islamskiego*, http://geopolityka.net/andrzej-zebrowski-walka-informacyjna-wsparciem-terroryzmu-islamskiego/ (data dostępu: 13.11.2018).

innych, których ujawnienie może spowodować szkody, są często przesyłane jako niechronione, nawet wtedy, kiedy pracownik posiada dostęp do chronionego systemu poczty elektronicznej. Podobne skutki może ponadto spowodować używanie haseł o niewystarczającym stopniu trudności. Każdego roku jest tworzona lista najczęściej używanych haseł w Internecie[36]. Takie zachowania możemy zaobserwować praktycznie w codziennym życiu. Dlatego ważna jest świadomość istniejących zagrożeń, korzystanie w sposób mądry i odpowiedzialny z możliwości, które daje technologia. Dla podniesienia poziomu bezpieczeństwa informacyjnego ważne jest, by ta kwestia była postrzegana jako priorytet, również przez firmy zajmujące się tworzeniem oprogramowania czy dostawców usług informacyjnych. Takim samym podejściem muszą wykazywać się też producenci urządzeń.

Mimo opisanych wcześniej zagrożeń związanych z rozwojem nowych technologii nie należy jednak zapominać o korzyściach, jakie ten rozwój ze sobą niesie. Niewątpliwie wśród takich korzyści należy wymienić rozwój potencjału naukowego. Kolejnym plusem jest szybkość przesyłania i dostępu do informacji czy możliwość szybkiej komunikacji z ludźmi na całym świecie. Nie bez znaczenia jest też rola technologii informacyjnych w przedsiębiorstwie. Dzięki niej może ono bardziej efektywnie realizować swoje zadania, poprzez automatyzację, przyspieszenie przebiegu procesów, redukcję kosztów. Zastosowanie nowych technologii pozwala na dotarcie do nowych grup klientów i wprowadzenie na rynek innowacyjnego produktu.

Dzięki zapewnieniu dostępu do usług publicznych drogą elektroniczną świadczenie usług administracyjnych może stać się bardziej produktywne i efektywne. Możliwe będzie zapewnienie najwyższej jakości usług dla obywateli i firm, przy możliwie najniższych kosztach dla podatników, a w rezultacie obsługa społeczeństwa stanie się tańsza i szybsza[37]. Rozwój systemu e-administracji (e-government)[38] może wpłynąć na odbiurokratyzowanie, odformalizowanie, dostępność, sprawność oraz szybkość działania administracji[39]. Komunikacja pomiędzy organem a obywatelem zostałaby pozbawiona zbędnych formalności, a to wpłynęłoby na oszczędność kosztów, a przede wszystkim czasu.

W konsekwencji urzędy mogłyby stać się bardziej przyjazne dla obywatela. Jednak warunkiem, aby tak się stało jest zmiana sposobu podejścia

---

[36] Lista najpopularniejszych haseł w 2017 r., https://pclab.pl/news76521.html (data dostępu: 25.09.2019).

[37] M. Butkiewicz, *Internet w instytucjach publicznych. Zagadnienia prawne*, Warszawa 2006, s. 60.

[38] R. Biskup, M. Ganczar, *Komunikacja elektroniczna w postępowaniu administracyjnym*, „Państwo i Prawo" 2008, nr 1, s. 59.

[39] Szerzej na ten temat: W. Kasprzak, *Zagrożenie bezpieczeństwa cyfrowego Polski na przykładzie cyberwojny w Estonii*, „Studia Prawnoustrojowe" 2016, nr 31, s. 109–110.

kadr do załatwiania spraw oraz prowadzenie aktywnych działań podnoszących świadomość obywateli na temat użyteczności rozwiązań elektronicznych[40].

3. Zadania jednostek samorządu terytorialnego w zakresie ochrony bezpieczeństwa informacyjnego

3.1. Dostęp do informacji publicznej i jego ograniczenia

Termin informacja publiczna został zdefiniowany jako każda informacja o sprawach publicznych. W szczególności są to informacje o: polityce wewnętrznej i zagranicznej, organach władzy publicznej, informacja o stanie państwa, samorządów i ich jednostek organizacyjnych, majątku publicznym[41]. Do udostępniania informacji publicznych zobowiązane są między innymi podmioty reprezentujące państwowe osoby prawne albo osoby prawne samorządu terytorialnego, jednostki organizacyjne samorządu terytorialnego albo podmioty reprezentujące zgodnie z odrębnymi przepisami Skarb Państwa[42].

Prawo dostępu do informacji publicznej przysługuje każdemu i obejmuje uzyskanie informacji publicznej przetworzonej w zakresie istotnym dla interesu publicznego, wgląd do dokumentów urzędowych oraz posiedzeń kolegialnych organów władzy publicznej.

Udostępnienie informacji publicznej następuje w drodze publikacji w BIP, wyłożenia czy wywieszenia w miejscach ogólnie dostępnych, zainstalowanie w tych miejscach urządzenia umożliwiającego zapoznanie się z tą informacją, jak również udzielenie jej w formie pisemnej lub ustnej. Dotyczy to również udostępniania materiałów, w tym audiowizualnych i teleinformatycznych, dokumentujących posiedzenia kolegialnych organów władzy publicznej[43]. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji nakłada obowiązek, aby informacje publiczne zawarte w BIP były dostępne dla odwiedzających przez całą dobę bez przerwy, z wyjątkiem sytuacji awaryjnych. W przypadku awarii, brak dostępności dla odwiedzających strony BIP nie może przekraczać 24 godzin. Strony BIP muszą mieć zaimplementowane rozwiązania chroniące przed celowym spowolnieniem lub uniemożli-

---

[40] Szerzej na ten temat zob. D. Fleszer, *Funkcjonowanie Elektronicznej Administracji na Przykładzie EPUAP*, „Roczniki Administracji i Prawa" Rok XII (2012), s. 119–138.

[41] Zob. art. 6 ustawy z dnia 6.09.2001 r. o dostępie do informacji publicznej (Dz.U. z 2001 r. Nr 112, poz. 1198).

[42] Ibidem, art. 4.

[43] Por. K. Wilko, *Jakie są zasady udostępniania informacji publicznej*, https://samorzad.infor.pl/temat_dnia/387047,Jakie-sa-zasady-udostepniania-informacji-publicznej.html (data dostępu: 25.09.2019).

wieniem dostępu do ich zasobów. Podmioty prowadzące BIP mają obowiązek wyznaczenia osób odpowiedzialnych za zmiany treści udostępnionej informacji publicznej. Mają one dostęp do panelu administracyjnego strony BIP w oparciu o mechanizmy identyfikacji i autoryzacji, nad którymi nadzór sprawuje administrator BIP. Do zadań administratora należy również kontrola w każdy powszedni dzień, dziennika zmian treści strony, w który musi być ona wyposażona i który działa w sposób automatyczny. Strony BIP winny być chronione przez programowy lub programowo-sprzętowy moduł bezpieczeństwa, zapobiegający zniszczeniu lub nieuprawnionej modyfikacji informacji publicznych, zawartych w BIP. Nie później niż dobę po zaistnieniu zmiany treści informacji jest wykonywana kopia bazy informacji na odrębnym nośniku danych[44].

Prawo dostępu do informacji publicznej w określonych na podstawie ustawy sytuacjach podlega ograniczeniu. Przesłanki do ograniczenia tego prawa stanowi między innymi ochrona wolności i praw innych osób i podmiotów gospodarczych oraz ochrona porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa[45] .W art. 22 ustawy o dostępie do informacji publicznej wskazano m.in. następujące „tajemnice", które mogą być powodem ograniczenia: ochrona danych osobowych, tajemnica służbowa, skarbowa, statystyczna. Wymienione przykłady nie stanowią zamkniętego katalogu, ograniczenie dostępu do informacji publicznej może też wynikać z przepisów innych ustaw.

3.2. Ochrona informacji niejawnych

Termin informacja niejawna został zdefiniowany jako informacja, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania[46]. Zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, podmiotami ustawy z mocy prawa są m.in.:

– Sejm i Senat;
– Prezydent Rzeczypospolitej Polskiej;
– organy administracji rządowej, w tym Prezes Rady Ministrów, ministrowie;

---

[44] Por. M. Grzegorczyk, *Zasady działania i wymagania techniczne BIP,* http://www.bip.nia.org.pl/pl/page/17/zasady-dzialania-i-wymagania-techniczne-bip.html (data dostępu: 16.11.2018).

[45] Por. art. 31 ust. 3 i art. 61 ust. 3 Konstytucji Rzeczypospolitej Polskiej z dnia 2.04.1997 r. (Dz.U. z 1997 r. Nr 78, poz. 483). Por. art 5. ustawy z dnia 6.09.2001 r. o dostępie do informacji publicznej (Dz.U. z 2001 r. Nr 112, poz. 1198).

[46] Art. 1 ustawy z dnia 5.08.2010 r. o ochronie informacji niejawnych (Dz.U. z 2010 r. Nr 182, poz. 1228).

– organy jednostek samorządu terytorialnego, a także inne podległe im jednostki organizacyjne lub przez nie nadzorowane, w tym wójtowie, burmistrzowie i prezydenci miast, radni;

– sądy i trybunały;

– Narodowy Bank Polski.

Za ochronę informacji niejawnych odpowiada kierownik jednostki organizacyjnej, która je przetwarza oraz powołany przez niego pełnomocnik do spraw ochrony informacji niejawnych[47]. Do zadań pełnomocnika, jego zastępcy oraz wyspecjalizowanej komórki zwanej pionem ochrony należy[48]:

– zapewnienie ochrony informacji niejawnych, w tym ich ochrony fizycznej;

– zapewnienie ochrony systemów i sieci teleinformatycznych, w których są wytwarzane, przetwarzane, przechowywane lub przekazywane informacje niejawne;

– kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji;

– okresowa kontrola ewidencji, materiałów i obiegu dokumentów;

– szkolenie pracowników w zakresie ochrony informacji niejawnych.

Informacje niejawne o przyznanej klauzuli tajności mogą być wytwarzane, przetwarzane, przekazywane oraz przechowywane w warunkach, które uniemożliwiają ich nieuprawnione ujawnienie. Warunki te określa rozporządzenie Rady Ministrów w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych. Kancelaria tajna powinna być zlokalizowana w strefie bezpieczeństwa – obszarze o ograniczonym dostępie osób trzecich i spełniać określone w rozporządzeniu warunki dotyczące budowy i wyposażenia w środki ochrony fizycznej.

Wyróżniamy następujące klauzule tajności: ściśle tajne, tajne, poufne i zastrzeżone[49]. Chronione bez względu na upływ czasu pozostają dane identyfikujące funkcjonariuszy, żołnierzy i pracowników służb i instytucji uprawnionych do wykonywania czynności operacyjno-rozpoznawczych oraz osób, które udzielały im pomocy[50]. Dostęp do informacji niejawnych mogą mieć jedynie osoby uprawnione, posiadające poświadczenie bezpieczeństwa wydane przez odpowiednie służby, po przeprowadzeniu postępowania sprawdzającego, które przeszły odpowiednie szkolenie oraz jednostki organizacyjne wykonujące umowy związane z ich przetwarzaniem[51]. Jednostki te mają jed-

[47] Ibidem, art. 14.

[48] Ibidem, art. 15.

[49] Ibidem, art. 5.

[50] Ibidem, art. 7.

[51] Por. M. Cyrankiewicz, *Kto może mieć dostęp do informacji niejawnych*, https://www.rp.pl/artykul/941574-Kto-moze-miec-dostep-do-informacji-niejawnych.html (data dostępu: 25.09.2019); Bezpieczeństwo przemysłowe, https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-przemys/148,BEZPIECZENSTWO-PRZEMYSLOWE.html (data dostępu: 25.09.2019); Bezpieczeństwo osobowe, http://www.iniejawna.pl/pomoce/przyc_pom/6_bezpieczenstwo_osobowe.html (data dostępu: 25.09.2019).

nak obowiązek zapewnienia odpowiednich warunków ochrony potwierdzonych świadectwem bezpieczeństwa przemysłowego, wydawanym przez Służbę Kontrwywiadu Wojskowego lub Agencję Bezpieczeństwa Wewnętrznego.

4. Obowiązki inspektora ochrony danych oraz administratora bezpieczeństwa systemów informatycznych

4.1. Obowiązki inspektora ochrony danych

Inspektor ochrony danych jest powołany przez administratora danych osobowych w celu sprawowania nadzoru nad bezpieczeństwem danych osobowych w firmie lub organizacji[52]. Wypełnia również zadania, wskazane w ustawie o ochronie danych osobowych oraz rozporządzeniach wykonawczych[53]. Do zadań inspektora ochrony danych należy między innymi informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tym zakresie, monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora danych lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacji przetwarzania oraz powiązane z tym audyty[54].

Dotychczas, powołanie inspektora ochrony danych nie było obowiązkowe, jednak z dniem 25 maja 2018 r. weszło w życie rozporządzenie ogólne Parlamentu Europejskiego w sprawie ochrony danych osobowych. Jego celem jest ujednolicenie przepisów dotyczących ochrony danych osobowych na terenie całej Unii Europejskiej. Rozporządzenie nakłada na administratorów danych konieczność powołania takiego podmiotu w organizacji.

Jego powołanie stało się obowiązkowe dla trzech rodzajów podmiotów. Po pierwsze są to wszystkie podmioty sektora publicznego, z wyłączeniem

---

[52] *Niezbędnik administratora bezpieczeństwa informacji*, Warszawa 2017, s. 7.

[53] Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11.05.2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz.U. z 2015 r., poz. 745); rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11.05.2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz.U. z 2015 r., poz. 719).

[54] Szerzej na ten temat: *RODO – Inspektor Ochrony Danych Osobowych zamiast Administratora Bezpieczeństwa Informacji*, http://4itsecurity.pl/blog/2-Dane-osobowe/93-rodo-inspektor-ochrony-danych-osobowych-zamiast-administratora-bezpieczenstwa-informacji.html (data dostępu: 25.09.2019).

sądów. Drugą grupę podmiotów stanowią podmioty, które przetwarzają dane osobowe na dużą skalę i stanowi to ich główny profil działalności, jak również te podmioty, które przetwarzają dane na ich zlecenie. Do trzeciej grupy należą podmioty, których głównym profilem działalności jest przetwarzanie danych osobowych, danych dotyczących wyroków skazujących i naruszeń prawa (tak zwanych wrażliwych danych) oraz podmioty, które na ich zlecenie zajmują się przetwarzaniem takich danych[55].

4.2. Obowiązki administratora systemów informatycznych

Administrator systemów informatycznych[56] współpracuje z inspektorem ochrony danych oraz dba o bezpieczeństwo przetwarzanych danych pod kątem teleinformatycznym. Funkcja administratora systemów informatycznych nie wynika wprost z przepisów prawa, ukształtowała się w ramach praktyki. Osobą pełniącą funkcję administratora systemów informatycznych może być pracownik zatrudniony w firmie na podstawie umowy cywilnoprawnej lub umowy o pracę (osoba z wewnątrz organizacji) lub ktoś spoza niej (tzw. outsourcing ASI). Osoba z wewnątrz organizacji, oprócz odpowiedniej wiedzy w zakresie IT[57], powinna posiadać nadane upoważnienie do przetwarzania danych osobowych. Do zadań administratora systemów informatycznych należy[58]:

– systematyczne kontrolowanie zastosowanych środków technicznych i organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych, odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, w szczególności kontrola pod kątem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Systemy informatyczne służące do przetwarzania danych osobowych, zgodnie z ustawą o ochronie danych osobowych, powinny być sprawdzane przynajmniej raz na 5 lat;

---

[55] K. Gałaj-Emiljańczyk, *Administrator bezpieczeństwa informacji, Inspektor ochrony danych, Kompetencje, obowiązki i odpowiedzialność*, Gdańsk 2017, s. 22; art. 37 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

[56] D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016, s. 29.

[57] Technologia informacyjna (ang. information technology, IT) – całokształt zagadnień, metod, środków i działań związanych z przetwarzaniem informacji. Stanowi połączenie zastosowań informatyki i telekomunikacji, obejmuje również sprzęt komputerowy oraz oprogramowanie, a także narzędzia i inne technologie związane ze zbieraniem, przetwarzaniem, przesyłaniem, przechowywaniem, zabezpieczaniem i prezentowaniem informacji.

[58] Zob. *Przykładowy katalog zadań administratora systemów informatycznych (ASI),* http://cognitio.edu.pl/przykladowy-katalog-zadan-administratora-systemow-informatycznych-asi/ (data dostępu: 25.09.2019).

– zapewnienie ciągłości działania systemu, w tym zabezpieczenie zbiorów danych oraz programów służących do przetwarzania danych osobowych poprzez systematyczne wykonywanie kopii zapasowych. Wykonane kopie należy przechowywać w miejscu zabezpieczającym je przed nieuprawnionym dostępem, modyfikacją, uszkodzeniem lub zniszczeniem, na zaszyfrowanych nośnikach zewnętrznych, przechowywanych w zabezpieczonym przed dostępem osób nieupoważnionych miejscu, w innej strefie pożarowej niż dane oryginalne. Kopie zapasowe należy usuwać niezwłocznie po ustaniu ich użyteczności;

– zapewnienie awaryjnego źródła zasilania oraz zabezpieczenie przed zakłóceniami w sieci zasilającej systemów informatycznych, służących do przetwarzania danych osobowych, których nagła przerwa w pracy mogłaby spowodować utratę danych lub naruszenie ich integralności. Do tego celu najczęściej wykorzystywane jest urządzenie typu UPS, podtrzymujące sieć oraz serwery, przynajmniej krytycznych systemów, do czasu ich bezpiecznego wyłączenia;

– nadzór nad naprawą oraz likwidacją urządzeń komputerowych – urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe przeznaczone do likwidacji pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie. Urządzenia, dyski lub inne elektroniczne nośniki informacji zawierające dane osobowe, przeznaczone do naprawy, pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie, albo naprawia się je pod nadzorem osoby upoważnionej;

– zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem oprogramowania złośliwego, którego celem może okazać się uzyskanie nieuprawnionego dostępu do danych[59], również do systemów teleinformatycznych znajdujących się na służbowych smartfonach czy tabletach;

– zabezpieczenie pomieszczenia serwerowni przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych[60],

– ochrona przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem, w tym m.in.[61]:

– rozdzielenia sieci na podsieci ze względu na grupy użytkowników, usług informatycznych i systemów,

– stosowanie filtracji MAC adresów urządzeń, które mogą uzyskać dostęp do sieci,

---

[59] J. Kowalewski, M. Kowalewski *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*, Warszawa 2017, s. 39–59.

[60] Ibidem, s. 137–149.

[61] *Zasady ochrony przed cyberatakiem*, http://www.ue.wroc.pl/pracownicy/5066/zasady_ochrony_przed_cyberatakiem.html (data dostępu: 25.09.2019).

– odseparowanie bezprzewodowej sieci dla gości,
– nadzorowanie stosowania zasady „czystego ekranu”[62].

Podsumowanie

Informacja może przybierać wiele postaci, między innymi postać elektroniczną, werbalną czy postać tradycyjnych dokumentów papierowych. Musi być skutecznie chroniona przed niepożądaną ingerencją, dotyczy to również szeregu procesów, w których jest generowana, modyfikowana i przesyłana. Należy stale udoskonalać procedury i narzędzia przeciwdziałające zagrożeniom bezpieczeństwa informacyjnego, aby w konsekwencji nie dopuścić do wystąpienia dezinformacji, którą w najprostszy sposób można zdefiniować jako celowe przekazanie fałszywej informacji wprowadzającej odbiorców w błąd. Dezinformacja odgrywa znaczną rolę, zarówno w sferze obronności, jak również w środkach masowego przekazu czy polityce. Celem dezinformacji jest kształtowanie określonego typu postrzegania, którego efektem jest podejmowanie przez ofiarę dezinformacji działań korzystnych dla dezinformującego.

Znaczny wpływ na poprawę poziomu bezpieczeństwa informacyjnego ma kształtowanie świadomości na temat potencjalnych zagrożeń. Dotyczy to nie tylko pracowników administracji i urzędów, którzy na co dzień w swojej pracy wykorzystują zbiory danych, generują i przetwarzają informacje, ale również społeczeństwa jako całości. Żadne, nawet najbardziej zaawansowane i kompleksowe narzędzia i procedury, nie zapewnią nam bezpieczeństwa, jeżeli sami nie będziemy potrafili mądrze i odpowiedzialnie podejść do tego zagadnienia i zadbać o zwiększenie poziomu bezpieczeństwa informacyjnego w swoim najbliższym otoczeniu.

Wykaz literatury

Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006.
Biskup R., Ganczar M., *Komunikacja elektroniczna w postępowaniu administracyjnym*, „Państwo i Prawo” 2008, nr 1.
Butkiewicz M., *Internet w instytucjach publicznych. Zagadnienia prawne*, Warszawa 2006.
Cieślarczyk M., *Kultura bezpieczeństwa i obronności*, Siedlce 2011.
Gałaj-Emiljańczyk K., *Administrator bezpieczeństwa informacji, Inspektor ochrony danych, Kompetencje, obowiązki i odpowiedzialność*, Gdańsk 2017.
Jatkiewicz P., *Uwarunkowania zarządzania systemem bezpieczeństwa informacji w jednostkach samorządu terytorialnego*, praca doktorska, Uniwersytet Gdański, 2012.

[62] M. Kaleta, *Podstawowe zasady przetwarzania danych na co dzień*, http://itls.pl/252/podstawowe-zasady-przetwarzania-danych-na-co-dzien/ (data dostępu: 25.09.2019).

Kasprzak W., *Zagrożenie bezpieczeństwa cyfrowego Polski na przykładzie cyberwojny w Estonii,* „Studia Prawnoustrojowe" 2016, nr 31.
Fleszer D., *Funkcjonowanie Elektronicznej Administracji na Przykładzie EPUAP*, „Roczniki Administracji i Prawa" 2012, nr XII.
Kliś M., *Przestępczość w Internecie. Zagadnienia podstawowe*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1.
Kowalewski J., Kowalewski M., *Zagrożenia informacji w cyberprzestrzeni, cyberterroryzm*, Warszawa 2017.
Krassowski K., *Kilka uwag o kryminalistyce w świecie informacji cyfrowej oraz stojących przed nią wyzwaniach*, „Studia Prawnoustrojowe" 2015.
Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.
Lisiak-Felicka D., Szmit M., *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016.
Niezbędnik administratora bezpieczeństwa informacji, praca zbiorowa, Warszawa 2017.
Nowak A., Scheffs W., *Zarządzanie bezpieczeństwem informacyjnym*, Warszawa 2010.
Sołodow D., *Regulacje prawne dotyczące bezpieczeństwa w sieci Internet (na przykładzie prawa internetowego Federacji Rosyjskiej)*, „Studia Prawnoustrojowe" 2016, nr 31.
Szatkowski T. (red.), *Bezpieczeństwo danych w sektorze publicznym*, Warszawa 2016.
Wasilewski J., *Cyberprzestępczość. Wybrane aspekty prawnokarne i kryminalistyczne*, praca doktorska, Uniwersytet w Białymstoku, 2017.
Więcaszek-Kuczyńska L., *Wybrane regulacje prawne w obszarze zagrożeń bezpieczeństwa informacyjnego. Część pierwsza. Obronność*, „Zeszyty Naukowe" 3 (11)/2014, ISSN 2299-2316.
Więcaszek-Kuczyńska L., *Zagrożenia bezpieczeństwa informacyjnego, obronność*, „Zeszyty Naukowe" 2 (10)/2014, ISSN 2299-2316.
Żebrowski A., Kwiatkowski W., *Bezpieczeństwo informacji III Rzeczypospolitej*, Kraków 2000.

Summary

Information safety in local government units

Key words: safety, information safety, information security threats, cyber-terrorism, public information.

This article analyses issues in the field of information and IT security and attempts to explain what is meant by information security and presents potential opportunities and threats in this field. The article discusses various types of information security threats, from those with a "traditional" character, such as espionage, through to threats resulting from the development of new technologies, e.g. cyber-terrorism and threats resulting from the activities of natural forces. The article presents the tasks of public administration and local government units in the field of information security resulting, *inter alia*, from the provisions of the Act on access to public information or regulations on the protection of personal data.