BIBLIOTECZKA IZBY RZECZOZNAWCÓW PTI

Przemysław Jatkiewicz

Ochrona danych osobowych
Teoria i praktyka

POLSKIE TOWARZYSTWO INFORMATYCZNE

POLSKIE TOWARZYSTO INFORMATYCZNE

Przemysław Jatkiewicz

Ochrona danych osobowych
Teoria i praktyka

WARSZAWA 2015

ISBN 978–83–60810–71–2 (e-book)

Recenzenci:
dr hab. Pawel Fajgielski, profesor Katolickiego Uniwersytetu Lubelskiego
dr inż. Adrian Kapczyński, Politechnika Śląska w Gliwicach
dr mecenas Ryszard Skarbek, Uniwersytet Gdański

Korekta: Ewa Ignaczak
Skład: Marek W. Gawron

Wydawca:
POLSKIE TOWARZYSTWO INFORMATYCZNE
01-003 Warszawa, al. Solidarności 82A/ 5
tel. +48 22 838 47 05
e-mail: pti@pti.org.pl
www.pti.org.pl

Spis treści

Szanowni Państwo,

mamy przyjemność przekazać w Państwa ręce drugą książkę z cyklu wydawniczego Polskiego Towarzystwa Informatycznego ***Biblioteczka Izby Rzeczoznawców PTI***.

Celem cyklu jest przedstawienie treści mogących zainteresować zarówno osoby zajmujące się zawodowo informatyką, jak i tych z Państwa, którzy w swojej pracy stykają się z zagadnieniami i problemami związanymi z informatyką.

Autorem drugiego tomu z cyklu ***Biblioteczka Izby Rzeczoznawców PTI*** jest rzeczoznawca Izby Rzeczoznawców PTI, dr inż. Przemysław Jatkiewicz. Monografia poświęcona jest zagadnieniom związanym z ochroną danych osobowych. Szczegółowo omówiono w niej przepisy ustawy o ochronie danych osobowych wraz z aktami wykonawczymi. Przedstawiono nową rolę i zadania administratora bezpieczeństwa informacji, jakie zostały mu narzucone poprzez tegoroczne, tj. wydane w roku 2015, akty prawne. W pracy zawarto liczne komentarze, wyroki i decyzje wydane przez sądy administracyjne i GIODO dotyczące problemów, na jakie natknąć się można przy przetwarzaniu danych osobowych. W monografii ujęto również obszerny opis środków technicznych, których odpowiedni dobór i implementacja jest niezbędny celem ochrony danych, a w szczególności danych osobowych.

Zapraszamy do lektury niniejszego oraz poprzedniego i kolejnych tomów z serii ***Biblioteczka Izby Rzeczoznawców PTI***.

Marian Noga

Prezes
Polskiego Towarzystwa Informatycznego

Tomasz Szatkowski

Dyrektor Izby Rzeczoznawców
Polskiego Towarzystwa Informatycznego

Warszawa 1 sierpnia 2015 roku

Wstęp. Dlaczego powinniśmy chronić nasze prywatne dane?

Poza wymaganiami prawnymi, nakazującymi podejmowanie działań w celu ochrony danych, powinniśmy sobie zdawać sprawę, iż informacje o nas mogą być wykorzystywane przez osoby, których interesy są sprzeczne z naszymi.

Najbardziej jaskrawym przykładem jest kradzież danych pozwalających na dostęp do kont bankowych czy kart kredytowych. Proces nielegalnego wykorzystania kart kredytowych doczekał się nawet swojego własnego terminu – *carding*[1]. W roku 2008 miało miejsce największe w historii włamanie, w efekcie którego skradziono 134 mln numerów kart kredytowych z bazy danych firmy Heartland Payment Systems[2]. Problem nie dotyczy jedynie banków oraz organizacji finansowych zza oceanu. Według danych Biura Informacji Kredytowej, średnio w ciągu roku wykrywa się w Polsce próby wyłudzenia kredytów na podstawie fałszywych danych osobowych na kwotę blisko 108,5 mln zł[3].

Nie tylko nasze finanse są zagrożone. Informacje o miejscu zamieszkania, numerze telefonu czy adresie e-mailowym mogą zostać wykorzystane do *stalkingu* czyli uporczywego nękania mogącego wywołać poczucie zagrożenia. Badania przeprowadzone przez Instytut Wymiaru Sprawiedliwości pod koniec 2009 roku wykazały, że prawie 10% badanych padło ofiarą *stalkingu*[4].

---

[1] L.J. Trautman, *Cybersecurity: What About US Policy?*, artykuł niepublikowany, 2015, http://works.bepress.com/lawrence_trautman/26.

[2] T. Armerding, *The 15 worst data security breaches of the 21st Century*, portal CSO, http://www.csoonline.com/article/2130877/data-protection/data-protection-the-15-worst-data-security-breaches-of-the-21st-century.html.

[3] *infoDOK. Raport o dokumentach. 18 edycja: II kwartał 2014 r.*, Związek Banków Polskich 2014.

[4] W. Olszewska, *Paragraf na stalkera*, „Na wokandzie" 2010, nr 3.

Problem jest na tyle poważny, iż za czyn ten w artykule 190a Kodeksu karnego przewidziano karę nawet do 10 lat więzienia[5].

Te same dane kontaktowe służyć mogą nieuczciwym przedsiębiorcom do wysyłania *spamu*, czyli niezamówionej informacji handlowej. Polskie prawodawstwo w artykule 10 ust. 1 ustawy o świadczeniu usług drogą elektroniczną zakazuje przesyłania środkami komunikacji elektronicznej niezamówionej informacji handlowej do osoby fizycznej. Za informację handlową uważa się „każdą informację przeznaczoną bezpośrednio lub pośrednio do promowania towarów, usług lub wizerunku przedsiębiorcy lub osoby wykonującej zawód, której prawo do wykonywania zawodu jest uzależnione od spełnienia wymagań określonych w odrębnych ustawach, z wyłączeniem informacji umożliwiającej porozumiewanie się za pomocą środków komunikacji elektronicznej z określoną osobą oraz informacji o towarach i usługach niesłużącej osiągnięciu efektu handlowego pożądanego przez podmiot, który zleca jej rozpowszechnianie, w szczególności bez wynagrodzenia lub innych korzyści od producentów, sprzedawców i świadczących usługi”[6].

Niezgodne z prawem jest także, wedle ustawy Prawo Komunikacyjne, „używanie telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących do celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na to zgodę”[7].

Przedsiębiorcy bezpodstawnie uważają, że umieszczenie w wiadomości marketingowej prośby o wyrażenie zgody na otrzymywanie informacji handlowej jest zgodne z prawem. Ponieważ szczególną formą wyrażenia zgody jest udostępnienie adresu elektronicznego, adresy e-mail zbierane z sieci Internet powszechnie wykorzystywane są do celów reklamowych, chociaż cel ich udostępniania był zupełnie inny.

Rozróżnienie adresów osób prawnych lub organizacji, które nie mają osobowości prawnej od adresów osób fizycznych może sprawić wiele problemów ze względu na adresy służbowe pracowników zarejestrowane w domenie pracodawcy. W dokumencie Opinia nr 5/2004 Grupy Roboczej Art. 29 w sprawie niezamówionych komunikatów do celów marketingowych,

[5] Ustawa z 6 czerwca 1997 r. Kodeks karny, Dz.U. z 1997 r. Nr 88, poz. 553.

[6] Ustawa z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. z 2002 r. Nr 144, poz. 1204.

[7] Ustawa z 16 lipca 2004 r. Prawo telekomunikacyjne, Dz.U. 2004 Nr 171, poz. 1800.

zawarte są wytyczne wskazujące, iż to nadawca musi ustalić, czy konkretny adres e-mail należy do osoby prawnej, czy osoby fizycznej[8].

W praktyce przepisy te są trudno egzekwowalne, czego doświadcza każdy przeciętny użytkownik poczty elektronicznej. Badania wskazują, że około 70% wszystkich wiadomości pocztowych to spam, a 27% przeciętnych internautów odbiera dziennie co najmniej 11 niechcianych wiadomości[9].

[8] Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, ARTICLE 29 Data Protection Working Party, 11601/EN WP 90, Adopted on 27 February 2004.

[9] *Raport z X Badania wykorzystania poczty elektronicznej w Polsce*, Sare S.A., http://sare.pl/ [2014].

Rozdział 1. Geneza ochrony danych osobowych

Problematyka ochrony danych osobowych swoimi korzeniami sięga XIX wieku. Związana była z konstytucyjnym prawem do zachowania prywatności. Pierwsze regulacje prawne o zasięgu krajowym pojawiły się we wczesnych latach 70. zeszłego wieku.

Na arenie międzynarodowej zagadnienie ochrony danych osobowych po raz pierwszy pojawia się w rezolucji nr 34/169 Zgromadzenia Ogólnego ONZ. Artykuł 4 wymienia między innymi informacje o życiu prywatnym, które uzyskane przez funkcjonariuszy organów ścigania, wykorzystywane mogą być jedynie w toku wykonywania obowiązków służbowych lub dla potrzeb wymiaru sprawiedliwości. Ujawnienie ich do innych celów jest całkowicie niewłaściwe[10].

Pierwszą powszechną definicję danych osobowych znajdujemy w Rekomendacji Organizacji Współpracy Gospodarczej i Rozwoju (OECD) z 23 września 1980 roku w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami[11]. Dane osobowe oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Dokument ten wskazuje także administratora danych jako stronę, która zgodnie z prawem krajowym jest właściwa do rozstrzygania o zawartości i wykorzystaniu danych osobowych, niezależnie od tego, czy takie dane są gromadzone, przechowywane, przetwarzane i rozpowszechniane przez tę stronę, czy przez podmiot w jej imieniu.

Rekomendacja wymienia siedem zasad, którymi należy się kierować przy przetwarzaniu danych osobowych:

---

[10] Code of conduct for Law Enforcement Officials adopted by General Assembly resolution 34/169 of 17 December 1979, A/RES/34/16.

[11] Recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data, OECD 23 September 1980.

1) zasada ograniczonego pozyskiwania (ang. *Collection Limitation Principle*),
2) zasada adekwatności danych (ang. *Data Quality Principle*),
3) zasada celowości (ang. *Purpose Specification Principle*),
4) zasada ograniczonego użytkowania (ang. *Use Limitation Principle*),
5) zasada otwartości (ang. *Openness Principle*),
6) zasada indywidualnego udziału (ang. *Individual Participation Principle*),
7) zasada odpowiedzialności (ang. *Accountability Principle*).

Według zasady ograniczonego pozyskiwania, dane mogą być pozyskiwane jedynie zgodnie z zasadami prawa oraz za wiedzą i zgodą osoby, której one dotyczą. Powinny być adekwatne w stosunku do celu, w jakim są zbierane. Winny być dokładne, kompletne i aktualne (zasada adekwatności). Cele, dla których dane osobowe są gromadzone, muszą być określone nie później niż w momencie ich zbierania. Późniejsze wykorzystanie danych ogranicza się do wypełnienia tych celów lub innych, które nie są z nimi sprzeczne (zasada celowości).

Zasada ograniczonego użytkowania mówi o tym, że dane osobowe nie powinny być ujawnione, udostępnione lub w inny sposób wykorzystywane do celów innych niż te, w jakich je zbierano za wyjątkiem sytuacji, gdy na takie działania uzyskano zgodę ich właściciela lub sądu. Należy je chronić poprzez odpowiednie zabezpieczenia przed takimi zagrożeniami, jak utrata, nieuprawniony dostęp, zniszczenie, nieuprawnione używanie, modyfikowanie lub ujawnienie.

Polityka postępowania ze zbiorami danych osobowych powinna być jawna, zaś charakter zawartych w nich danych, cele stosowania oraz nazwa i siedziba administratora łatwe do ustalenia (zasada otwartości).

Należy każdemu zapewnić możliwość uzyskania informacji odnośnie do posiadanych przez administratora danych osobowych zainteresowanego. Powinien on mieć prawo do żądania przekazania mu ich:

- w rozsądnym terminie,
- za opłatą, jeśli nie jest zbyt wysoka,
- w sposób racjonalny,
- w formie łatwo dla niego zrozumiałej.

W przypadku odmowy przekazania danych administrator winien odmowę taką uzasadnić. Zainteresowany może jednak ją zakwestionować. Na żądanie, dane go dotyczące powinny być usunięte, poprawione, uzupełnione lub zmienione (zasada indywidualnego udziału).

Zasada odpowiedzialności narzuca administratorowi danych osobowych obowiązek dopilnowania przestrzegania wszystkich wyszczególnionych zasad.

Rekomendacja OECD nie jest dokumentem wiążącym, a jedynie zbiorem zaleceń, które dotyczą ochrony prywatności podczas przepływu danych osobowych przez granice. Podkreśla, że narzucenie zbyt rygorystycznych ograniczeń przez przepisy krajowe, może mieć niekorzystny wpływ na światowy rozwój gospodarczy.

Dokumentem wiążącym jest podpisana w Strasburgu 28 stycznia 1981 roku Konwencja nr 108 Rady Europy, która weszła w życie dopiero cztery lata później. Wprowadzono w niej zupełnie odmienną definicję danych osobowych. „Dane osobowe – oznaczają wszelką informację dotyczącą osoby fizycznej o ustalonej tożsamości albo dającej się zidentyfikować" [12]. Zapisy Konwencji dotyczą ochrony zautomatyzowanych zbiorów danych, czyli zestawów danych podlegających automatycznemu przetwarzaniu, które zdefiniowano w następujący sposób: „Automatyczne przetwarzanie oznacza następujące operacje wykonywane w całości lub części przy pomocy metod zautomatyzowanych: rejestrowanie danych, z zastosowaniem do nich operacji logicznych i/albo arytmetycznych, ich modyfikowanie, usuwanie, odzyskiwanie lub rozpowszechnianie"[13].

Następnym dokumentem poruszającym tematykę bezpieczeństwa danych osobowych była Rezolucja 45/95 Zgromadzenia Ogólnego ONZ[14]. Przywoływała ona wraz ze zmianami Rezolucję 44/132 z dnia 15 grudnia 1989[15].

[12] Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu 28 stycznia 1981 r., Dz.U. z 2003 r. Nr 3, poz. 25.

[13] Ibidem.

[14] Guidelines for the Regulation of Computerized Personal Data Files, A/RES/45/95 of 14 December 1990.

[15] Guidelines for the Regulation of Computerized Personal Data Files, G.A. res. 44/132, 44 U.N. GAOR Supp. (No. 49) at 211, U.N. Doc. A/44/49 (1989).

W rezolucji prowadzono sześć zasad, którymi kierować się mają ustawodawcy krajowi, opracowując akty prawne dotyczące danych osobowych zawartych w plikach komputerowych.

1. zasada legalności i rzetelności (ang. *Principle of lawfulness and fairness*),
2. zasada dokładności (ang. *Principle of accuracy*),
3. zasada celowości (ang. *Principle of the purpose-specification*),
4. zasada dostępności (ang. *Principle of interested-person access*),
5. zasada niedyskryminacji (ang. *Principle of non-discrimination*),
6. zasada bezpieczeństwa (ang. *Principle of security*).

Zgodnie z powyższymi regułami, dane personalne nie powinny być gromadzone i przetwarzane w sposób nieuczciwy lub niezgodny z prawem. Nie mogą też być użyte do celów sprzecznych z celami i zasadami Karty Narodów Zjednoczonych.

Osoby odpowiedzialne za przetwarzanie zbiorów danych osobowych mają obowiązek przeprowadzania regularnych kontroli poprawności i adekwatności zarejestrowanych danych, które muszą być aktualizowane systematycznie lub w momencie, gdy informacje w nich zawarte są używane. Pliki winne być aktualizowane tak długo, jak są one przetwarzane.

Cele, którym służy gromadzenie danych personalnych, muszą być jasno określone, uzasadnione i podane do wiadomości zainteresowanym. Dane winny być aktualne i adekwatne do celu, w jakim je zbierano. Nie mogą być ujawniane ani wykorzystywane do innych zadań bez zgody osób, których dotyczą. Okres, w którym dane osobowe są przechowywane, nie może przekraczać czasu potrzebnego do osiągnięcia określonych celów.

Każdy, kto potrafi dowieść swojej tożsamości, ma prawo wiedzieć, czy dane o nim są przetwarzane. Informację taką musi otrzymać w zrozumiałej formie, bez zbędnej zwłoki i kosztów. Musi mieć też możliwość dokonania odpowiednich korekt lub usunięcia wpisów, jeśli zostały one dokonane niezgodnie z prawem. Koszt sprostowania ponosi osoba odpowiedzialna za te sprawy.

Dane, które mogą prowadzić do dyskryminacji, w tym informacje na temat wierzeń, pochodzenia rasowego lub etnicznego, koloru skóry, życia seksualnego, przekonań politycznych, religijnych, filozoficznych i innych, jak również członkostwa w stowarzyszeniach lub związkach zawodowych, nie

powinny być gromadzone. Odstępstwo od tej reguły jest dozwolone w przypadkach, gdy dane są konieczne do ochrony bezpieczeństwa narodowego, porządku i zdrowia publicznego oraz innych, wyraźnie określonych przez prawo przypadkach, lecz w granicach określonych przez Międzynarodową Kartę Praw Człowieka i inne, istotne instrumenty z dziedziny ochrony praw człowieka i przeciwdziałania dyskryminacji.

Należy podjąć odpowiednie środki w celu ochrony plików, zarówno przed naturalnymi zagrożeniami, jak i nieautoryzowanym dostępem, oszustwem lub nadużyciem danych oraz zainfekowaniem przez wirusy komputerowe.

Unia Europejska najszerzej opracowała zagadnienia ochrony danych osobowych w Dyrektywie 95/46/WE[16]. W stosunku do poprzednio omówionych dokumentów uszczegółowiona została definicja danych osobowych: „Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (osoby, której dane dotyczą); osoba możliwa do zidentyfikowania, to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka specyficznych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość".

Poza definicjami znaleźć w niej można ogólne zasady legalności przetwarzania danych osobowych. Podzielone są one na dziewięć części:

Część I. Zasady dotyczące jakości danych;
Część II. Kryteria legalności przetwarzania danych;
Część III. Szczególne kategorie przetwarzania danych;
Część IV. Przekazywanie informacji osobie, której dane dotyczą;
Część V. Prawo dostępu do danych osoby, której dane dotyczą;
Część VI. Zwolnienia i ograniczenia;
Część VII. Prawo sprzeciwu przysługujące osobie, której dane dotyczą;
Część VIII. Poufność i bezpieczeństwo przetwarzania danych;
Część XI. Powiadomienie.

Część I nie wnosi istotnych nowości w stosunku do omówionych już zasad legalności i rzetelności, dokładności oraz celowości, oprócz zobowiązania

[16] Dyrektywa Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych 95/46/WE, Dz.U. WE OJ L 281, 23.11.1995.

państw członkowskich do stworzenia odpowiednich zabezpieczeń dla danych przechowywanych przez dłuższe okresy dla potrzeb historycznych, statystycznych i naukowych.

Część II rozszerza zasadę ograniczonego pozyskiwania, gdyż według rezolucji dane osobowe mogą być przetwarzane nie tylko wówczas, gdy osoba, której dane dotyczą, jednoznacznie wyraziła na to zgodę, lecz także w przypadku, gdy przetwarzanie danych jest konieczne dla:

a) realizacji umowy, której stroną jest osoba, której dane dotyczą,
b) zgodności z zobowiązaniem prawnym,
c) ochrony żywotnych interesów osoby, której dane dotyczą,
d) realizacji zadania wykonywanego w interesie publicznym lub dla sprawowania władzy publicznej,
e) potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, przed którą ujawnia się dane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą[17].

O ile przypadki zawarte w punktach a, b i d wydają się uzasadnione, o tyle określenie żywotnych interesów osoby, której dane dotyczą, a także uzasadnionych interesów administratora i osób trzecich, może prowadzić do nadużyć.

Część III zawiera zasadę niedyskryminacji, rozszerzając jednocześnie katalog odstępstw od niej o sytuacje, gdy przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby w przypadku, gdy osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do udzielenia zgody.

Zasada nie dotyczy także danych podawanych do publicznej wiadomości przez osoby, których one dotyczą, lub przetwarzanych w ramach legalnej działalności przez fundacje, stowarzyszenia lub inne niekomercyjne instytucje, których cele mają charakter polityczny, filozoficzny, religijny lub związkowy. Warunkiem jest, aby przetwarzanie odnosiło się wyłącznie do członków tej instytucji lub osób mających z nią regularny kontakt w związku z jej celami.

Zasady niedyskryminacji nie stosuje się również w przypadku, gdy przetwarzanie danych wymagane jest dla celów medycyny prewencyjnej,

[17] M. Polok, *Bezpieczeństwo danych osobowych*, C.H. BECK, Warszawa 2008.

diagnostyki medycznej, świadczenia opieki, leczenia oraz zarządzania opieką zdrowotną, jak również w przypadkach, gdy dane są przetwarzane przez podmiot służby zdrowia zgodnie z przepisami prawa krajowego lub zasadami określonymi przez właściwe krajowe instytucje, podlegający obowiązkowi zachowania tajemnicy zawodowej czy też przez inną osobę również zobowiązaną do zachowania tajemnicy.

Część IV narzuca administratorowi danych obowiązek powiadomienia osoby, której dane są pozyskiwane i przechowywane, o tożsamości administratora danych i ewentualnie jego przedstawiciela, celach przetwarzania danych, odbiorcach lub kategoriach odbiorców danych, dobrowolności udzielania informacji lub jej braku oraz o prawie do dostępu do swoich danych i ich poprawienia.

Prawo dostępu do danych osoby, której dane dotyczą, zawarte w części V, mówi o braku ograniczeń do uzyskiwania od administratora danych informacji o przechowywaniu danych, celach i zasadach tego składowania oraz możliwości poprawienia, usunięcia lub zablokowania danych, których przetwarzanie jest niezgodne z prawem, szczególnie ze względu na niekompletność lub niedokładność danych. Wspomina też o zawiadomieniu osób trzecich, którym dane zostały ujawnione, o każdym poprawieniu, usunięciu lub zablokowaniu danych, o ile nie okaże się to niemożliwe lub nie będzie wymagało niewspółmiernie dużego wysiłku.

Część VI zawiera katalog ograniczeń stosowania praw i obowiązków związanych z przetwarzaniem danych osobowych. Są to:

- bezpieczeństwo narodowe,
- obronność,
- bezpieczeństwo publiczne,
- działania prewencyjne, prowadzenie czynności dochodzeniowo-śledczych i prokuratorskich w sprawach kryminalnych lub sprawach o naruszenie zasad etyki w zawodach podlegających regulacjom,
- ważny interes ekonomiczny lub finansowy państwa członkowskiego lub Unii Europejskiej,
- funkcje kontrolne, inspekcyjne i regulacyjne, związane z wykonywaniem władzy publicznej,
- ochrona osoby, której dane dotyczą oraz praw i wolności innych osób.

Wątpliwości mogą budzić ograniczenia związane z interesami państw członkowskich oraz funkcjami kontrolnymi, inspekcyjnymi oraz regulacyjnymi. Dlatego też w części VII zawarto zapisy dające prawo zainteresowanym do sprzeciwu w tych przypadkach. Sprzeciw, na wniosek i bez opłaty, może dotyczyć również przetwarzania danych dla potrzeb marketingu bezpośredniego. Przyznawane jest także prawo niepodlegania decyzji, która wywołuje skutki prawne, opartej wyłącznie na zautomatyzowanym przetwarzaniu danych, którego celem jest dokonanie oceny niektórych dotyczących aspektów o charakterze osobistym.

Część VIII zobowiązuje administratora danych do zastosowania odpowiednich środków technicznych i organizacyjnych w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem, utratą, zmianą, niedozwolonym ujawnieniem lub dostępem oraz wszelkimi innymi nielegalnymi formami przetwarzania.

W przypadku powierzenia przetwarzania danych, administrator powinien wybrać przetwarzającego o wystarczających gwarancjach odnośnie do technicznych środków bezpieczeństwa oraz rozwiązań organizacyjnych. Przetwarzanie danych musi być regulowane przez umowę lub akt prawny, sporządzane na piśmie lub w innej równorzędnej formie.

Środki podjęte w celu zabezpieczenia danych powinny być adekwatne do zagrożeń przy uwzględnieniu stanu wiedzy oraz kosztów realizacji.

Część IX narzuca administratorowi danych obowiązek powiadomienia utworzonego przez państwo członkowskie organu nadzorczego o rozpoczęciu przetwarzania danych. Organ ten będzie uprawniony do przeprowadzania kontroli. Ma też za zadanie prowadzenie rejestru przetwarzanych danych, a państwa członkowskie dołożą starań w celu jego upublicznienia.

W polskim prawodawstwie ochronę danych osobowych zapewnia Konstytucja Rzeczypospolitej Polskiej w art. 47 o brzmieniu: „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym". Znacznie szerzej odnosi się do niej art. 51:

> „1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

> 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
> 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
> 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
> 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa"[18].

Problem stanowi jednak jasne sprecyzowanie znaczenia słowa prywatny. *Słownik języka polskiego* definiuje określenie „prywatny" jako „dotyczący kogoś osobiście, czyichś spraw osobistych, stanowiący czyjąś osobistą własność, niezwiązany z żadną instytucją; osobisty; niepaństwowy; nieurzędowy"[19]. Według tej definicji dane zgromadzone przez przedsiębiorcę oraz urzędy, a uzyskane w toku prowadzenia działalności nie stanowią danych prywatnych.

Jednakże, w świetle orzecznictwa sądów[20], do sfery prywatnej człowieka należą:

a) życie osobiste oraz rodzinne, w tym stosunki małżeńskie, a także konkubinat,
b) tożsamość jednostki i jej przeszłość,
c) sfera intymna – sprawy uczuć i seksu, zdrowia,
d) wyznanie i praktyki religijne,
e) stan majątkowy, w tym dane o wysokości otrzymywanego wynagrodzenia za pracę, stan zadłużenia,
f) tryb życia człowieka, sposób spędzania wolnego czasu, rozrywki, hobby,
g) karalność, informacje o popełnionych przestępstwach lub wykroczeniach.

Ponieważ pojęcie prywatności, chociaż używane powszechnie, nie jest łatwe do precyzyjnego zdefiniowania, autorzy piszący o nim oraz sądy orzekające

[18] Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r., Dz.U. z 1997 r. Nr 78, poz. 483.
[19] *Słownik języka polskiego*, (red.) M. Szymczak, PWN, Warszawa 1979, t. II, s. 553.
[20] J. Sieńczyło-Chlebowicz, *Naruszenie prywatności osób publicznych przez prasę. Analiza cywilnoprawna*, Zakamycze, Kraków 2006.

w kwestiach z nią związanych starają się raczej ustalić, jakie sprawy należą do sfery prywatnej, a jakie do tzw. sfery powszechnej dostępności[21].

Ochronę prywatności, jako jednego z dóbr osobistych, zapewniają także przepisy Kodeksu cywilnego. Artykuł 23 mówi iż:

> „Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach"[22].

Kodeks pracy również, choć nie bezpośrednio, odnosi się do informacji prywatnych. Artykuł 11 brzmi: „Pracodawca jest obowiązany szanować godność i inne dobra osobiste pracownika"[23].

[21] T. Liszcz, *Ochrona prywatności pracownika w relacjach z pracodawcą*, „Monitor Prawa Pracy" 2007, nr 1.

[22] Ustawa z 23 kwietnia 1964 r. – Kodeks cywilny, Dz.U. z 1964 r. Nr 16, poz. 93.

[23] Ustawa z 26 czerwca 1974 r. Kodeks pracy, Dz.U. z 1974 r. Nr 24, poz. 141.

Rozdział 2. Zakres stosowania ustawy o ochronie danych osobowych i definicje podstawowych pojęć

Ustawa z 29 sierpnia 1997 roku o ochronie danych osobowych[24], zwana w dalszej części niniejszej publikacji UODO, jest podstawowym aktem prawnym odnoszącym się do zagadnienia ochrony danych osobowych. Przepisy szczególne, branżowe czy tematyczne, mają jednak – zgodnie z zasadą *lex specialis derogat legi generali* – pierwszeństwo przed jej przepisami.

Przykładowo, Ustawa z 16 lipca 2004 roku Prawo telekomunikacyjne[25] ustala 12. miesięczny okres retencji danych, czyli obowiązek zatrzymywania i przechowywania danych telekomunikacyjnych, takich jak dane użytkownika inicjującego połączenie czy też użytkownika, do którego jest ono kierowane. Ustawa z 15 kwietnia 2011 roku o systemie informacji oświatowej[26] nakazuje gromadzenie szczegółowych danych o poszczególnych uczniach w System Informacji Oświatowej. Jawność ksiąg wieczystych na mocy Ustawy z 6 lipca 1982 roku o księgach wieczystych i hipotece[27] daje możliwość wglądu w dane osobowe właścicieli nieruchomości.

W art. 1 ust. 1 UODO zapisano, iż „Każdy ma prawo do ochrony dotyczących go danych osobowych". Nie wszyscy zobowiązani są jednak do jej stosowania:

- organy państwowe,
- organy samorządu terytorialnego,
- państwowe i komunalne jednostki organizacyjne,
- podmioty niepubliczne realizujące zadania publiczne,

[24] Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych, Dz. U. z 2014 r. poz. 1182.
[25] Ustawa z 16 lipca 2004 r. Prawo telekomunikacyjne, Dz.U. z 2004 r. Nr 171, poz. 1800.
[26] Ustawa z 15 kwietnia 2011 r. o systemie informacji oświatowej, Dz.U. z 2011 r. Nr 139, poz. 814.
[27] Ustawa z 6 lipca 1982 r. o księgach wieczystych i hipotece, Dz.U. z 1982 r. Nr 19, poz. 147.

- osoby fizyczne i osoby prawne oraz jednostki organizacyjne niebędące osobami prawnymi.

Dodatkowo osoby fizyczne, prawne oraz jednostki organizacyjne, aby podlegać ustawie, winny przetwarzać dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych. Muszą też mieć siedzibę albo miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystaniu środków technicznych znajdujących się na terytorium RP. Przez państwo trzecie rozumie się państwo nienależące do Europejskiego Obszaru Gospodarczego. Ustawy nie stosuje się więc do osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych oraz podmiotów mających siedzibę lub miejsce zamieszkania w państwie trzecim, wykorzystujących środki techniczne znajdujące się na terytorium naszego kraju wyłącznie do przekazywania danych.

UODO nie obejmuje prasowej działalności dziennikarskiej w rozumieniu ustawy z 26 stycznia 1984 roku[28]. Jednakże prowadzący wspomnianą działalność podlegają kontroli Generalnego Inspektora Ochrony Danych Osobowych (GIODO). Zakres obowiązków i uprawnień GIODO zostanie omówiony w dalszej części tej publikacji. Obowiązani są również do stosowania odpowiednich zabezpieczeń technicznych i organizacyjnych. W związku z powyższym, zaleca się dużą ostrożność w przekazywaniu mediom informacji zawierających dane osobowe. Wykluczeniu podlega również działalność literacka i artystyczna, chyba że wolność wyrażania swoich poglądów i rozpowszechniania informacji istotnie narusza prawa i wolności osoby, której dane dotyczą.

Ustawodawca przewidział także, że UODO nie obowiązuje, gdy umowa międzynarodowa, której stroną jest Polska, stanowi inaczej. Przepis ten jest szczególnie istotny w przypadku przekazywania danych osobowych do państw, których system prawny nie zapewnia należytej ich ochrony. Przykładem może być program „Safe Harbour", zatwierdzony przez Unię Europejską decyzją Komisji 2000/520/WE z 26 lipca 2000 roku[29]. Przewiduje on między innymi powołanie specjalnego panelu, w skład którego wchodzą przedstawiciele różnych organów ochrony danych osobowych działających

[28] Ustawa z dnia 26 stycznia 1984 r. Prawo prasowe, Dz.U. z 1984 r. Nr 5, poz. 24.

[29] Decyzja Komisji Europejskiej 2000/520/WE z 26 lipca 2000 r., O.J. L 215, 25.08.2000, s. 7-47.

w Unii Europejskiej. Celem pracy powołanego panelu jest rozpatrywanie skarg na naruszenie zasad ochrony danych osobowych.

Kraje członkowskie Unii Europejskiej udostępniają także dane osobowe na podstawie tzw. umowy parasolowej dotyczącej przekazywania danych pomiędzy UE a USA w ramach współpracy policyjnej lub sądowej czy też dane PNR (*Passenger Name Record*) związane z rezerwacją biletów lotniczych.

Szczególną ochroną objęte są informacje związane z bezpieczeństwem państwa oraz jego funkcjonowaniem. Do przetwarzania tego typu danych stosuje się przepisy tych ustaw, które przewidują dalej idącą ich ochronę, niż zapisane w UODO. Należy do nich Ustawa z 5 sierpnia 2010 roku o ochronie informacji niejawnych[30]. Informacjom tym nadaje się następujące klauzule w zależności od zawartości oraz szkodliwości spowodowanej ich ujawnieniem:

- ściśle tajne,
- tajne,
- poufne,
- zastrzeżone.

Definicja danych osobowych zawarta w ustawie jest tożsama z definicją umieszczoną w Rekomendacji Organizacji Współpracy Gospodarczej i Rozwoju z 23 września 1980 roku, o której wspomniano w rozdziale 1. Precyzuje ona jednak określenie „osoba możliwa do zidentyfikowania". Według UODO, dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, czyli osoby, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

Ta szeroka definicja ma jedno ograniczenie. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Żadne przepisy nie określają ilościowo kosztów i czasu, które moglibyśmy uznać za nadmierne. Zależne są one w głównej mierze od możliwości, jakimi dysponujemy. Adresy IP komputerów dla przeciętnej osoby nie stanowią danych osobowych. Jednakże Opinia

[30] Ustawa z 5 sierpnia 2010 roku o ochronie informacji niejawnych, Dz.U. z 2010 r. Nr 182, poz. 1228.

Grupy Roboczej ds. Ochrony Danych uznała je za dane osobowe stwierdzając, że:

> „dostawcy usług internetowych oraz menedżerowie lokalnych sieci mogą, stosując rozsądne środki, zidentyfikować użytkowników internetu, którym przypisali adresy IP ponieważ systematycznie zapisują w plikach daty, czas trwania oraz dynamiczny adres IP (czyli ulegający zmianie po każdym zalogowaniu) przypisany danej osobie. To samo odnosi się do dostawców usług internetowych, którzy prowadzą rejestr (logbook) na serwerze http. Nie ma wątpliwości, że w takich przypadkach można mówić o danych osobowych, w rozumieniu art. 2 Dyrektywy"[31].

Generalny Inspektor Ochrony Danych Osobowych w swojej interpretacji wykazał, że nie zawsze w praktyce możliwe jest jednoznaczne przypisanie adresu IP do konkretnej, zidentyfikowanej osoby. Adres IP będzie więc uznawany za dane osobowe jedynie wówczas, gdy podmiot przetwarzający go ma jednocześnie dostęp do danych łączących adres IP z innymi danymi identyfikującymi osobę[32].

Podobnych wątpliwości co do kwalifikacji danych osobowych jest wiele. Czy pominięcie w adresie numeru budynku lub mieszkania sprawia, że nie mamy do czynienia z danymi osobowymi? Gdy miejscem zamieszkania będzie tzw. falowiec (budynek wielorodzinny w Gdańsku zamieszkiwany przez ok. 6 tys. lokatorów) z pewnością nie, chyba że będziemy mieli do czynienia z lokatorem o nazwisku Archeminiwiriłokotoczerepepenczewiczakowska (nazwisko oryginalne). Każde z nazwisk mieszkańców wsi Luboszów należy jednak traktować jako dane osobowe. Tę najmniejszą w Polsce wieś zamieszkują 2 osoby.

Szczególnym przypadkiem danych osobowych są numery PESEL. Zdefiniowany w art. 15 Ustawy z 24 września 2010 roku o ewidencji ludności[33],

[31] Opinia 4/2007 w sprawie pojęcia danych osobowych, 01248/07/PL WP 136, 20 czerwca 2007 r., Grupa Roboczej ds. Ochrony Danych powołanej na mocy Art. 29, http://www.giodo.gov.pl/462/id_art/2375/j/pl/.

[32] *Adres IP może być w pewnych przypadkach uznany za dane osobowe*, Portal GIODO, zakładka Odpowiedzi na pytania dotyczące ustawy o ochronie danych osobowych definicji danych osobowych, pytanie: Czy adres IP komputera należy do danych osobowych?, http://www.giodo.gov.pl/319/id_art/2258/j/pl/.

[33] Ustawa z 24 września 2010 r. o ewidencji ludności, Dz.U. 2010 Nr 217 poz. 1427.

numer ten jest 11-cyfrowym stałym symbolem numerycznym, jednoznacznie identyfikującym osobę fizyczną, w którym sześć pierwszych cyfr oznacza datę urodzenia (rok, miesiąc, dzień), kolejne cztery – liczbę porządkową i płeć osoby, a ostatnia jest cyfrą kontrolną, służącą do komputerowej kontroli poprawności nadanego numeru ewidencyjnego. Z samej jego definicji wynika, że stanowi daną osobową, podlega nawet bez zestawienia z innymi informacjami o osobie, wszelkim rygorom przewidzianym w UODO.

Za dane osobowe nie są uważane dane osób zmarłych, a powoływanie się przez różne instytucje na ustawę o ochronie danych osobowych przy odmowie udzielenia o nich informacji jest bezpodstawne[34]. Kwestia możliwości wprowadzenia ochrony danych osobowych osób zmarłych, podniesiona w interpelacji pani poseł Renaty Rochnowskiej z 26 czerwca 2007 roku została odrzucona, gdyż obowiązujące przepisy kodeksowe odnoszące się do kwestii ochrony kultu pamięci osób zmarłych, w aspekcie prywatnoprawnym zapewniają dostateczną ochronę danych osobowych osób nieżyjących.

W odpowiedzi na interpelację Andrzej Duda, podsekretarz stanu w Ministerstwie Sprawiedliwości, wyjaśnił:

> „Z chwilą śmierci osoby fizycznej, aczkolwiek nie następuje sukcesja prawa zmarłego do ochrony danych osobowych, to jednak prawa zmarłego odżywają jako prawa osób za życia mu bliskich. Chodzi tutaj przede wszystkim o prawo do poszanowania niezakłóconego spokoju psychicznego, w którym to pojęciu mieści się kultywowanie pamięci zmarłego. W tym aspekcie wkroczeniem w sferę objętą ochroną będzie nie każde posłużenie się danymi, ale tylko takie, które – według typowych, przeciętnych reakcji – powoduje tego rodzaju zakłócenie. Konsekwencją bezprawności działania będzie możliwość skorzystania przez pokrzywdzonego z ochrony przewidzianej w art. 24 k.c. oraz art. 448 k.c"[35].

W kontekście osób zmarłych UODO obejmuje dane osobowe, zawarte w:

- kartotekach,
- skorowidzach,

[34] Decyzja GIODO, GI-DP-97/99.

[35] Odpowiedź podsekretarza stanu w Ministerstwie Sprawiedliwości – z upoważnienia ministra – na interpelację nr 8701 w sprawie ochrony danych osobowych osób zmarłych, SPS-023-8701/07.

- księgach,
- wykazach,
- innych zbiorach ewidencyjnych,
- systemach informatycznych także w przypadku przetwarzania danych poza zbiorem danych.

Za zbiór danych uważa się każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie. Przetwarzanie danych to jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Przez pojęcie system informatyczny rozumie się zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

Powyższe definicje nie pozostawiają zbyt szerokiego pola do interpretacji. Użycie wymogu ustrukturyzowania w celu wyeliminowania zastosowania definicji zbioru w stosunku do pewnych danych jest bardzo trudne do praktycznego wykonania. W zasadzie dla każdego zestawu danych można opracować jakieś kryteria ich podziału.

W sposób szczególny w UODO traktowane są systemy informatyczne. Szerokie definicje obejmują również pojedyncze programy oraz wszystkie operacje, jakie mogą być przez nie wykonywane na danych. Problemy interpretacyjne precyzuje Wojciech Wiewiórowski, były Generalny Inspektor Ochrony Danych Osobowych, w wypowiedzi na forum grupy dyskusyjnej GoldenLine:

> „W skrajnych przypadkach może być tak, że w zależności od konfiguracji:
> a) całość infrastruktury teleinformatycznej oraz całość oprogramowania pracuje na potrzeby jednego systemu, do którego wszyscy użytkownicy mają dostęp (w takim samym lub różnym zakresie),
> albo

> b) istnieje -naście lub -dziesiąt systemów logicznie od siebie oddzielonych, ale pracujących na tej samej infrastrukturze teleinformatycznej, gdzie mamy do czynienia z -nastoma lub -dziesiątkami zbiorów"[36].

W stosunku do zbiorów danych osobowych sporządzanych doraźnie, zgodnie z zapisami w UODO, ochrona stosowana jest jedynie w zakresie zabezpieczania. Zbiory sporządzane doraźnie to zbiory tworzone wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych. Po ich wykorzystaniu muszą być niezwłocznie usuwane lub poddane anonimizacji. Czas, przez jaki mogą być one użytkowane, powinien być relatywnie krótki. Kryteria doraźności są na tyle ogólne, że zachodzi konieczność odwołania się do konkretnych okoliczności towarzyszących przetwarzaniu przez administratora danych dla określonych, precyzyjnie wskazanych celów. Jeśli sporządzony doraźnie zbiór danych osobowych nie jest związany z celem towarzyszącym działalności administratora danych, to nie możemy mówić o jego doraźności.

Przykłady zbiorów danych osobowych, których doraźność została potwierdzona przez GIODO, obejmują:

- dane osobowe zebrane w wyniku umowy z firmą marketingową, wykorzystane do celu jednorazowej akcji promocyjnej[37],
- dane osobowe przetwarzane przez samodzielny publiczny zakład opieki zdrowotnej, w związku z realizowanym programem badań przesiewowych w celu wczesnego rozpoznawania raka szyjki macicy, które po zakończeniu i ostatecznym rozliczeniu programu z Ministrem Zdrowia oraz instytucją finansującą zostają komisyjnie usunięte[38],
- dane osobowe przetwarzane przez pracownię medycyny rodzinnej uniwersytetu, działającą w porozumieniu z instytucją finansującą prowadzącą badania satysfakcji pacjenta z usług lekarzy pierwszego kontaktu, wyłącznie do wysyłania respondentom ankiety i listów przypominających, a po zakończeniu wysyłki poddane anonimizacji[39].

[36] W. Wiewiórowski, wypowiedź na forum GoldenLine w temacie *Zbiór danych w elektronicznym obiegu*, http://www.goldenline.pl/grupy/Pozostale/abi/zbior-danych-w-elektronicznym-obiegu,2996230/.

[37] Decyzja GIODO, GI-DP-403/1473/00.

[38] Decyzja GIODO, GI-DEC-DS-59/02.

[39] Decyzje GIODO: GI-DP-430/37/02/, GI-DP-024/855/02.

Generalny Inspektor Danych Osobowych nie uznaje doraźnego charakteru zbiorów danych osób uczestniczących w konkursach promocyjnych, których zwycięzcy są umieszczani na stronach internetowych. Usunięcie ich po okresie publikacji sprawia jednak, że można mówić o zbiorach doraźnych sporządzonym w celach technicznych[40].

Definicję anonimizacji zawiera Ustawa z 16 września 2011 roku o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej[41]. Jest to „przekształcenie danych osobowych w sposób uniemożliwiający przyporządkowanie poszczególnych informacji do określonej lub możliwej do zidentyfikowania osoby fizycznej albo jeżeli przyporządkowanie takie wymagałoby niewspółmiernych kosztów, czasu lub działań". Trudno jest jednak rozróżnić usunięcie danych osobowych od anonimizacji bez uwzględnienia okoliczności, w których zwykle dokonuje się tych czynności.

Po usunięciu danych osobowych podmiot, który je przetwarzał, traci faktyczną możliwość korzystania z nich. Anonimizację wykonuje się często w celu ujawnienia informacji zawierających dane osobowe. Odbiorca informacji nie ma więc dostępu do danych osobowych, jednakże udostępniający podmiot nadal nimi dysponuje. Anonimizacja danych zebranych w związku z prowadzonymi badaniami naukowymi zwykle prowadzi do sytuacji, gdy pozostawiane są jedynie informacje wynikające z pierwotnie posiadanych danych osobowych[42].

UODO w ograniczony sposób dotyczy działania podmiotów zgłaszających kandydatów lub list kandydatów w wyborach na urząd Prezydenta RP, do Sejmu, do Senatu i do organów samorządu terytorialnego, a także w wyborach do Parlamentu Europejskiego, pomiędzy dniem zarządzenia wyborów a dniem głosowania. Na jej podstawie nie można również nakazywać usunięcia danych osobowych zebranych w toku czynności operacyjno-rozpoznawczych prowadzonych na podstawie przepisów prawa. Stąd też Ministerstwo Spraw Wewnętrznych podjęło działania legislacyjne mające na celu wydanie rozporządzenia w sprawie przetwarzania informacji przez policję.

[40] A. Drozd, *Ustawa o ochronie danych osobowych: komentarz: wzory pism i przepisy*, LexisNexis, Warszawa 2004.

[41] Ustawa z 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, Dz. U. 2011 Nr 230, poz. 1371.

[42] M. Kamiński, *Anonimizacja i usuwanie danych osobowych*, „Safety and Security" 2015, nr 1.

Rozdział 3. Organ ochrony danych osobowych

Organem do spraw ochrony danych osobowych jest powoływany i odwoływany przez Sejm Rzeczypospolitej Polskiej za zgodą Senatu Generalny Inspektor Ochrony Danych Osobowych.

Funkcję tę od roku 1998 przez dwie 4-letnie kadencje sprawowała dr Ewa Kulesza, następnie Michał Serzycki, a przez ostatnią niepełną kadencję dr Wojciech Wiewiórowski. Obecnie stanowisko to sprawuje dr Edyta Bielak-Jomaa. W roku 2001 w strukturach Unii Europejskiej utworzono stanowisko Europejskiego Inspektora Ochrony Danych (EDPS). Dba on o to, aby wszystkie instytucje i organy UE szanowały przy przetwarzaniu danych osobowych prawa obywateli do prywatności. Od 4 grudnia 2014 roku funkcję zastępcy Europejskiego Inspektora Ochrony Danych Osobowych sprawuje Wojciech Wiewiórowski[43].

Główne zadania EDPS to:

- monitorowanie przetwarzania danych osobowych w instytucjach i organach europejskich,
- konsultacje z Komisją Europejską, Parlamentem Europejskim i Radą Unii Europejskiej w kwestiach związanych z ochroną danych,
- współpraca z innych organami ochrony danych w zakresie spójnego podejścia do ochrony danych na obszarze całej Europy[44].

Obywatel, którego prawo do prywatności zostało naruszone przez instytucję lub organ UE, zwraca się najpierw do osób przetwarzających jego dane osobowe. Kolejną instancją jest właściwy inspektor ochrony danych.

[43] Decyzja Parlamentu Europejskiego i Rady z 4 grudnia 2014 r. w sprawie mianowania Europejskiego Inspektora Ochrony Danych i jego zastępcy, 2014/886/UE.

[44] Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz.U. L. 8 z 12.1.2001 r.

Jeśli skarżący nie zgadza się z opinią inspektora, może wnieść sprawę do Trybunału Sprawiedliwości.

Na stanowisko Generalnego Inspektora w Polsce może być powołana osoba, która spełnia łącznie cztery warunki:

1) jest obywatelem polskim i stale zamieszkuje na terytorium Rzeczypospolitej Polskiej,
2) wyróżnia się wysokim autorytetem moralnym,
3) posiada wyższe wykształcenie prawnicze oraz odpowiednie doświadczenie zawodowe,
4) nie była karana za przestępstwo.

Piastuje je maksymalnie dwie kadencje, podczas których nie wolno jej wykonywać innych zajęć zawodowych ani zajmować innego stanowiska, z wyjątkiem stanowiska profesora szkoły wyższej. Stąd też wynikła konieczność ustąpienia Wojciecha Wiewiórowskiego z funkcji GIODO[45] przy objęciu przez niego stanowiska zastępcy EDPS. Nie może także należeć do partii politycznej, związku zawodowego ani prowadzić działalności publicznej niedającej się pogodzić z godnością jego urzędu. Posiada immunitet i odpowiada jedynie przed Sejmem Rzeczypospolitej Polskiej.

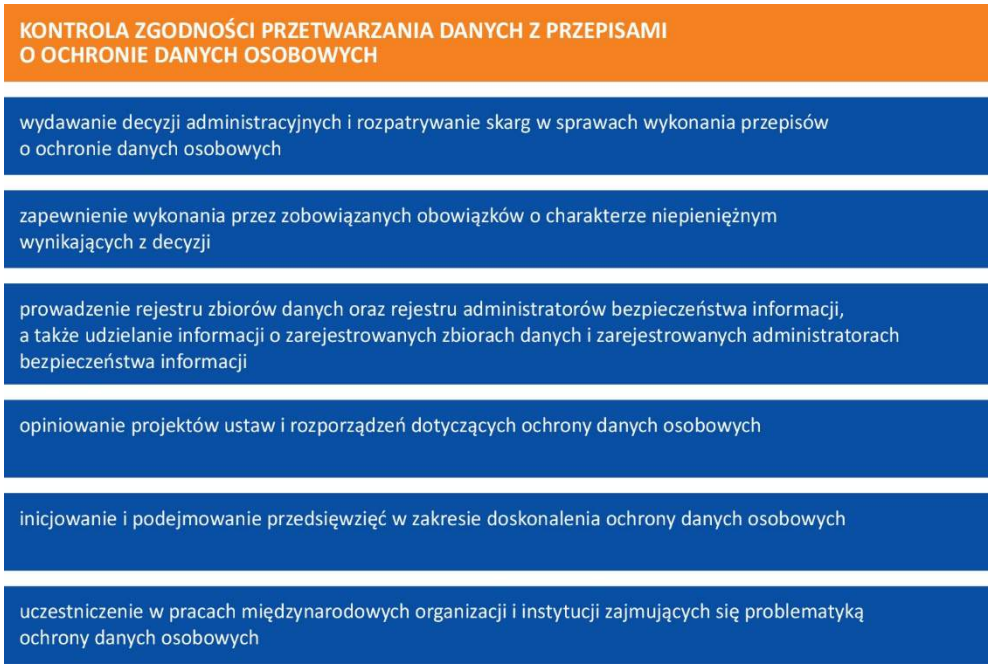
Odwołanie GIODO jest możliwe jedynie gdy:

1) zrzekł się stanowiska,
2) stał się trwale niezdolny do pełnienia obowiązków na skutek choroby;
3) sprzeniewierzył się złożonemu ślubowaniu,
4) został skazany prawomocnym wyrokiem sądu za popełnienie przestępstwa.

Główne zadania GIODO zostały pokazane na rysunku 1.

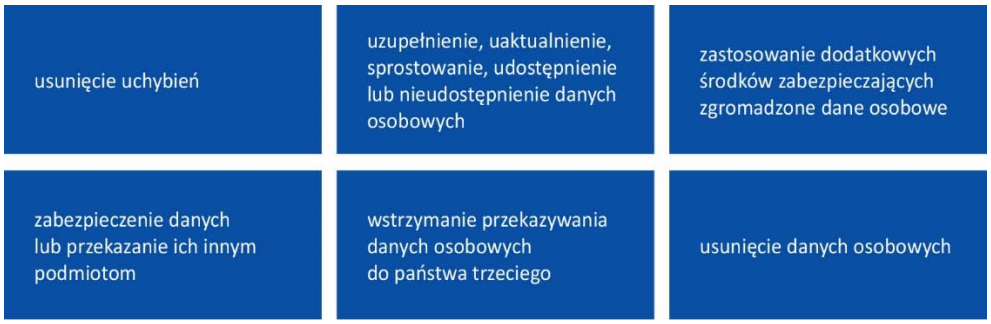
Wykonując swoje zadania przy pomocy Biura Generalnego Inspektora Ochrony Danych Osobowych, w przypadku naruszenia przepisów o ochronie danych osobowych wykrytych wskutek prowadzonej w drodze decyzji administracyjnej kontroli, nakazuje przywrócenie stanu zgodnego z prawem.

[45] Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 3 grudnia 2014 r. w sprawie odwołania Generalnego Inspektora Ochrony Danych Osobowych.



Rys. 1. Zadania Generalnego Inspektora Ochrony Danych Osobowych
Źródło: opracowanie własne.

Rodzaje decyzji wydawanych przez Biuro Generalnego Inspektora Ochrony Danych Osobowych zostały pokazane na rysunku 2.



Rys. 2. Decyzje GIODO
Źródło: opracowanie własne.

Biuro Generalnego Inspektora Ochrony Danych Osobowych uzyskało statut w drodze Rozporządzenia prezydenta RP z 3 listopada 2006 roku[46], jego schemat organizacyjny przedstawia rysunek 3.

Rys. 3. Schemat organizacyjny Biura Generalnego Inspektora Ochrony Danych Osobowych

Źródło: *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013*, http://www.giodo.gov.pl/data/filemanager_pl/sprawozdaniaroczne/2013.pdf.

Generalny Inspektor, w przypadkach uzasadnionych charakterem i liczbą spraw z zakresu ochrony danych osobowych na danym terenie, może wykonywać swoje zadania przy pomocy jednostek zamiejscowych Biura. Przewidziane jest utworzenie takich jednostek w Katowicach (jednostka ta ma obejmować obszar województwa śląskiego, opolskiego, dolnośląskiego, małopolskiego i podkarpackiego) oraz w Gdańsku (obszar województwa pomorskiego, warmińsko-mazurskiego i zachodniopomorskiego).

Kontrolą zgodności przetwarzania danych z przepisami, wydawaniem decyzji administracyjnych i rozpatrywaniem skarg zajmują się upoważnieni pracownicy Biura GIODO, zwani inspektorami. Mają oni prawo wstępu

[46] Rozporządzenie Prezydenta Rzeczypospolitej Polskiej z 3 listopada 2006 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych Dz.U. z 2006 r., Nr 203, poz. 1494.

– w godzinach od 6°° do 22°°, za okazaniem imiennego upoważnienia i legitymacji służbowej – do pomieszczeń, w których zlokalizowany jest zbiór danych oraz pomieszczeń, w których przetwarzane są dane poza zbiorem danych, a także przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności danych z ustawą. Wzór imiennego upoważnienia zawarty jest w załączniku nr 1 niniejszego opracowania, zaś wzór legitymacji służbowej w załączniku nr 2.

Inspektorzy mogą żądać złożenia wyjaśnień oraz wzywać i przesłuchiwać osoby w zakresie niezbędnym do ustalenia stanu faktycznego. Są uprawnieni do wglądu do wszelkich dokumentów i danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii. Mogą przeprowadzać oględziny urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych, jak również zlecać sporządzanie ekspertyz i opinii. Inspektorowi przysługuje prawo wglądu do zbioru zawierającego dane osobowe jedynie za pośrednictwem upoważnionego przedstawiciela kontrolowanej jednostki organizacyjnej.

Chociaż UODO nie reguluje kwestii wcześniejszego informowania o zamiarze przeprowadzenia kontroli, to można przyjąć, że kontrolowany administrator danych powinien być poinformowany o terminie kontroli. Inspektor może jednak, w przypadku gdy zachodzi podejrzenie o możliwości ukrywania dowodów popełnienia czynów zabronionych, rozpocząć kontrolę bez wcześniejszej zapowiedzi. W odniesieniu do przedsiębiorców obowiązują przepisy Ustawy z 2 lipca 2004 roku o swobodzie działalności gospodarczej. Artykuł 79 ust. 4. brzmi: „Kontrolę wszczyna się nie wcześniej niż po upływie 7 dni i nie później niż przed upływem 30 dni od dnia doręczenia zawiadomienia o zamiarze wszczęcia kontroli. Jeżeli kontrola nie zostanie wszczęta w terminie 30 dni od dnia doręczenia zawiadomienia, wszczęcie kontroli wymaga ponownego zawiadomienia”[47].

Kierownik kontrolowanej jednostki organizacyjnej oraz kontrolowana osoba fizyczna będąca administratorem danych osobowych są obowiązani umożliwić inspektorowi przeprowadzenie kontroli.

Po dokonaniu czynności kontrolnych sporządzany jest protokół zawierający:

[47] Ustawa z 2 lipca 2004 r. o swobodzie działalności gospodarczej, Dz.U. z 2004 r. Nr 173, poz. 1807.

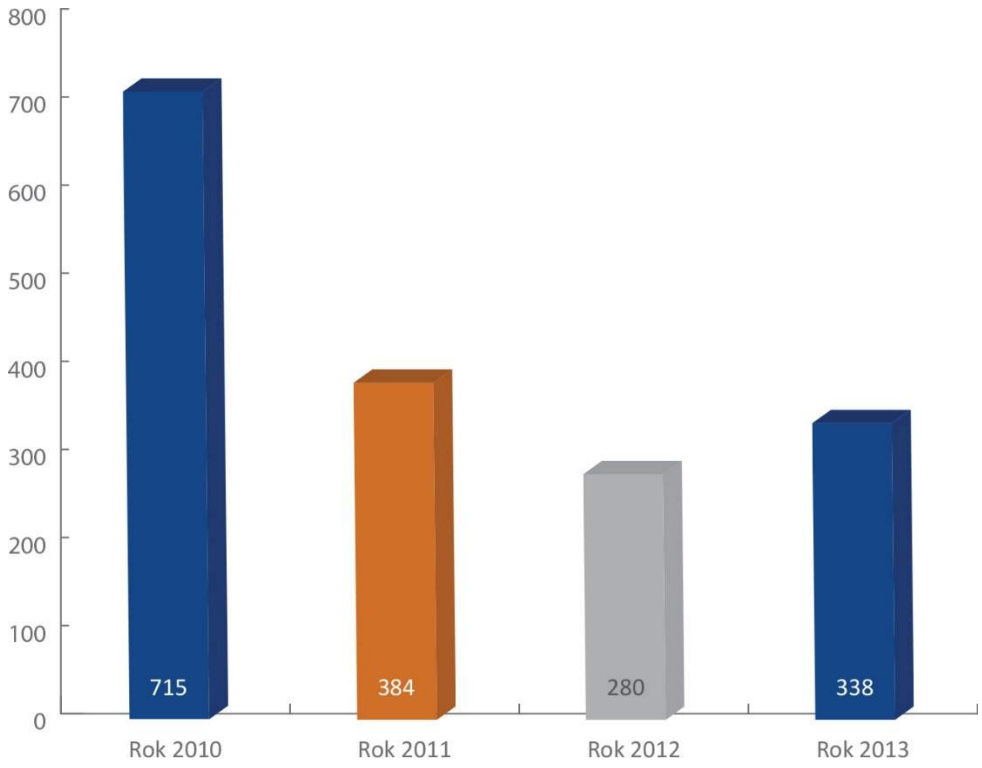
- nazwę podmiotu kontrolowanego w pełnym brzmieniu i jego adres,
- imię i nazwisko, stanowisko służbowe, numer legitymacji służbowej oraz numer upoważnienia inspektora,
- imię i nazwisko osoby reprezentującej podmiot kontrolowany oraz nazwę organu reprezentującego ten podmiot,
- datę rozpoczęcia i zakończenia czynności kontrolnych, z wymienieniem dni przerw w kontroli,
- określenie przedmiotu i zakresu kontroli,
- opis stanu faktycznego stwierdzonego w toku kontroli oraz inne informacje mające istotne znaczenie dla oceny zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
- wyszczególnienie załączników stanowiących składową część protokołu,
- omówienie dokonanych w protokole poprawek, skreśleń i uzupełnień,
- parafy inspektora i osoby reprezentującej podmiot kontrolowany na każdej stronie protokołu,
- wzmiankę o doręczeniu egzemplarza protokołu osobie reprezentującej podmiot kontrolowany,
- wzmiankę o wniesieniu lub niewniesieniu zastrzeżeń i uwag do protokołu,
- datę i miejsce podpisania protokołu przez inspektora oraz przez osobę lub organ reprezentujący podmiot kontrolowany.

Kontrolowany administrator danych może wnieść do protokołu umotywowane zastrzeżenia i uwagi lub odmówić podpisania, przedstawiając w terminie 7 dni swoje stanowisko na piśmie Generalnemu Inspektorowi.

Wyróżnić można następujące kontrole:

1. Kontrola z urzędu – wykonywana z inicjatywy własnej Generalnego Inspektora Ochrony Danych Osobowych.
2. Kontrola na wniosek – wykonywana wskutek wniosku instytucji, organizacji, przedsiębiorstwa lub osoby fizycznej.
3. Kontrola kompleksowa – obejmuje wszystkie zbiory danych osobowych jednego administratora danych oraz wszystkie wymogi UODO.
4. Kontrola częściowa – dotyczy określonych zagadnień będących przedmiotem skargi, problemów pojawiających się w toku rejestracji, zgodności informacji podanych w zgłoszeniu zbioru ze stanem faktycznym czy też zabezpieczenia danych.

W roku 2013 inspektorzy dokonali sprawdzenia 338 systemów informatycznych podczas 173 kontroli. Biorąc pod uwagę, że Departament Inspekcji (DIS) Biura Generalnego Inspektora Danych Osobowych liczy 14 osób, spośród których nie wszyscy mają wykształcenie informatyczne, liczba ta wydaje się całkiem duża. Na rysunku 4 przedstawiono liczbę skontrolowanych systemów informatycznych w latach 2010-2013. Tendencja spadkowa tłumaczona jest większym stopniem integracji systemów w kontrolowanych jednostkach. W tabeli 1 zamieszczono zestawienie liczby kontroli w wybranych obszarach.

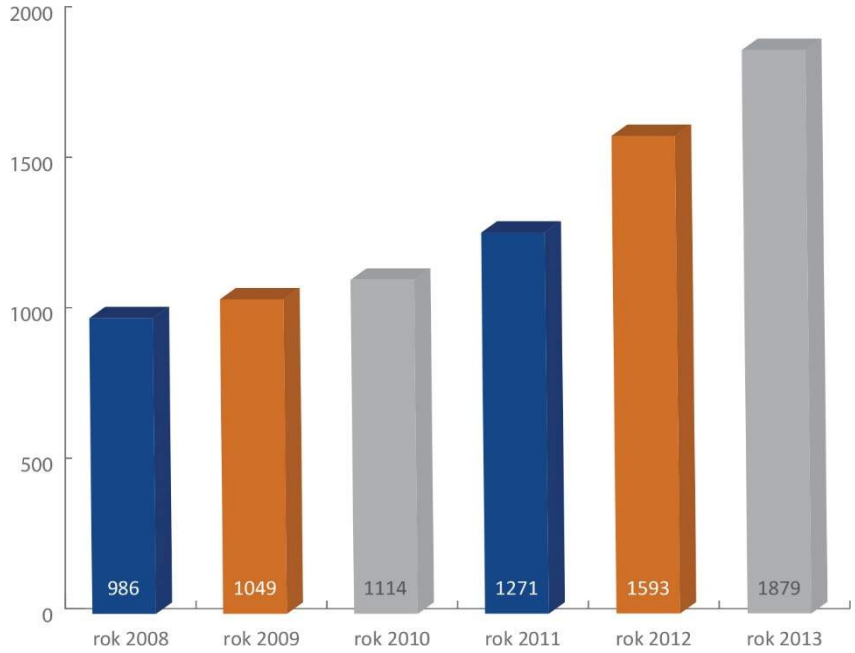


Rys. 4. Liczba skontrolowanych systemów informatycznych w latach 2010-2013
Źródło: *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013*, op. cit.

Tabela 1. Kontrola przetwarzania danych osobowych w wybranych obszarach

Obszar	Liczba kontroli
Przetwarzanie danych osobowych w Krajowym Systemie Informatycznym (KSI)	14
Placówki służby zdrowia	6
Placówki oświatowe	5
Dostawcy usług telekomunikacyjnych	14
Podmioty prowadzące serwisy internetowe	10
Podmioty przetwarzające dane osobowe w związku z wykorzystaniem technologii automatycznej identyfikacji radiowej (Radio Frequency Identification, RFID).	8
Podmioty prowadzące programy lojalnościowe	7

Źródło: opracowanie własne, na postawie *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013*, op. cit.



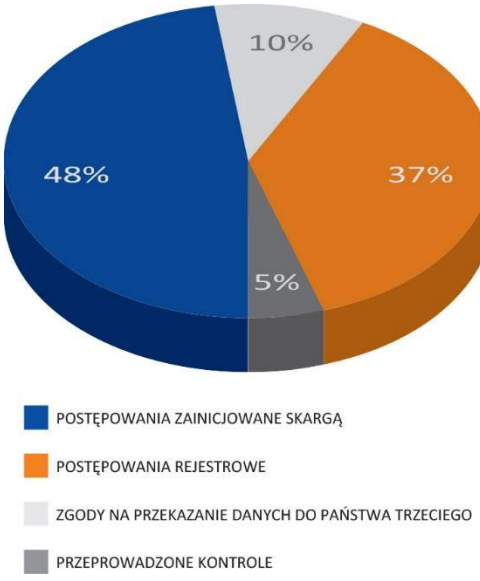
Rys. 5. Liczba skarg skierowanych do GIODO w latach 2010-2013
Źródło: *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013*, op. cit.

W roku 2013 do GIODO wpłynęło 1879 skarg. Jak wynika z danych zaprezentowanych na rysunku 5, ich liczba z roku na rok stale rośnie. Świadczy to o coraz większej wadze, jaką przykładają obywatele do ochrony swoich danych osobowych.

Nie przekłada się ona jednak na wiedzę i znajomość przepisów. Porównując dane z rysunków 5 i 6, można stwierdzić, iż nie każda ze skarg kończy się kontrolą. Znaczną część z nich GIODO jest w stanie rozpatrzyć na podstawie informacji uzyskiwanych od stron sporu.

W przypadku naruszenia przepisów o ochronie danych osobowych stwierdzonych podczas kontroli Generalny Inspektor, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem. Dodatkowo inspektor może żądać wszczęcia postępowania dyscyplinarnego lub innego przewidzianego prawem postępowania przeciwko osobom winnym dopuszczenia do uchybień.

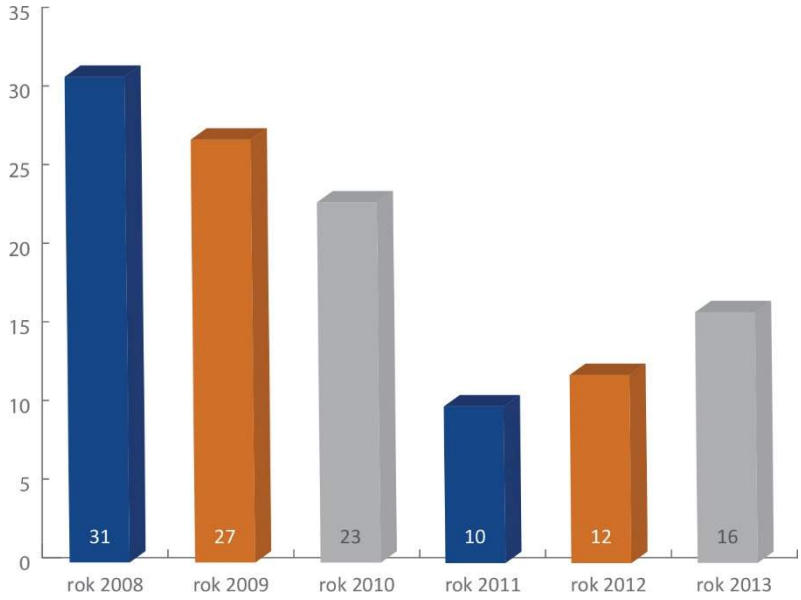
Rysunek 6 prezentuje liczbę decyzji wydanych w roku 2013, w podziale na rodzaje postępowań.



Rys. 6. Decyzje administracyjne GIODO wydane w 2013 roku w podziale na rodzaje postępowań

Źródło: *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013*, op. cit.

Generalny Inspektor Ochrony Danych Osobowych w przypadku wykrycia lub zaniechania działań, które wyczerpują znamiona przestępstwa, kieruje zawiadomienie do organów ścigania wraz ze zgromadzoną dokumentacją. Przetwarzanie i administrowanie danymi osobowymi niezgodne z prawem, jak również udaremnianie czy utrudnianie wykonania czynności kontrolnej, zagrożone jest karą grzywny, karą ograniczenia wolności albo pozbawienia wolności nawet do 2 lat. Liczbę zgłoszeń tego typu złożonych przez GIODO w latach 2008-2013 obrazuje rysunek 7.



Rys. 7. Liczba zgłoszeń o możliwości popełnienia przestępstwa złożonych przez GIODO w latach 2008-2013

Źródło: *Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013*, op. cit.

Od roku 2012, na mocy porozumienia pomiędzy Generalnym Inspektorem Danych Osobowych a Państwową Inspekcją Pracy (PIP), strony zobowiązały się do zgłaszania sobie nawzajem zauważonych nieprawidłowości[48]. Podkreślić należy, że porozumienie nie uprawnia PIP-u do dokonywania

[48] *Państwowa Inspekcja Pracy i GIODO zawarły porozumienie o współpracy*, Portal GIODO, zakładka Aktualności, http://www.giodo.gov.pl/259/id_art/5767/j/pl.

kontroli prawidłowości przetwarzania danych osobowych, a jedynie do zgłaszania nieprawidłowości zauważonych podczas kontroli przestrzegania przepisów Kodeksu pracy. Ponieważ jednak art. 22^1 Kodeksu pracy mówi, w jakim zakresie pracodawca może przetwarzać dane pracownika lub kandydata do pracy, zakres obu kontroli może się częściowo pokrywać.

Niezależnie od przysługującego GIODO prawa przeprowadzania kontroli, może on zwrócić się do administratora bezpieczeństwa informacji o dokonanie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych. Wskazuje przy tym zakres i termin sprawdzenia. Wynikowe sprawozdanie zostaje przekazane GIODO poprzez administratora danych. Funkcja administratora bezpieczeństwa informacji (ABI) zostanie omówiona w dalszej części tej publikacji.

Kontrolowany może zwrócić się do Generalnego Inspektora z wnioskiem o ponowne rozpatrzenie sprawy. Ma też prawo złożenia skargi do sądu administracyjnego. Postępowanie w sprawach nieuregulowanych w UODO prowadzi się według przepisów Kodeksu postępowania administracyjnego.

Rozdział 4. Zasady przetwarzania danych osobowych

Przetwarzanie danych osobowych – co do zasady – jest możliwe, gdy osoba której dane te dotyczą, wyrazi na to zgodę. Zgoda ta nie musi mieć formy pisemnej, nie może być jednak domniemana lub dorozumiana z oświadczenia woli o innej treści. Należy jednak zadbać o to, aby możliwe było udowodnienie złożonej deklaracji, stąd operatorzy telekomunikacyjni nagrywają rozmowy, podczas których klienci zezwalają na przetwarzanie swoich danych. Zgoda nie jest wymagana dla jednej z formy przetwarzania, jaką jest usunięcie danych.

Przetwarzanie danych osobowych bez zgody osoby, której dane dotyczą jest możliwe, gdy:

- jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,
- jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,
- jest nieodzowne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,
- jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą, w tym:
    - marketingu bezpośredniego własnych produktów lub usług administratora danych,
    - dochodzenia roszczeń z tytułu prowadzonej działalności gospodarczej.

Konstytucyjne uprawnienie do nauki legalizuje przetwarzanie danych osobowych przez placówki oświatowe. Gromadzą one dane uczniów na podstawie Ustawy z 15 kwietnia 2011 roku o systemie informacji oświatowej[49].

Innym przykładem może być przetwarzanie informacji stanowiących tajemnicę bankową, dotyczącą osób fizycznych, przez Biuro Informacji Kredytowej po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub inną instytucją, bez zgody osoby, której informacje dotyczą, dla celów statystycznych. Możliwe jest ono na mocy art. 128 Prawa bankowego[50].

Narodowy Fundusz Zdrowia jest uprawniony do przetwarzania danych osobowych na podstawie przepisów Ustawy z 27 sierpnia 2004 roku o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych[51]. Przetwarza on informacje dotyczące świadczeniodawców – lekarzy i świadczeniobiorców – pacjentów bez ich zgody.

Przetwarzanie danych osobowych bez zgody, przy dochodzeniu roszczeń, zostało potwierdzone przez GIODO w decyzji dotyczącej opublikowania danych osobowych na stronie internetowej, w celu sprzedaży wierzytelności. Dane te zawierały wysokość i podstawę zadłużenia, imię i nazwisko, kod pocztowy, miasto i ulicę bez numeru domu i lokalu (niepełne dane adresowe). W uzasadnieniu odrzucenia skargi stwierdzono:

> „(...) dłużnik musi liczyć się z tym, że popadając w zwłokę w spełnieniu zobowiązania jego prawo do prywatności może zostać ograniczone ze względu na dochodzenie przez wierzyciela należnych kwot. W przeciwnym wypadku mogłoby dojść do sytuacji, w której dłużnik, powołując się na prawo do ochrony danych osobowych, skutecznie uchyliłby się od spoczywającego na nim obowiązku spełnienia świadczenia i sytuacja taka ograniczałaby prawo wierzyciela do uzyskania należnej zapłaty”[52].

[49] Ustawa z 15 kwietnia 2011 r. o systemie informacji oświatowej, Dz.U. z 2011 r. Nr 139, poz. 814.
[50] Ustawa z 29 sierpnia 1997 r., Prawo bankowe, Dz.U. z 1997 r. Nr 140, poz. 939.
[51] Ustawa z 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, Dz.U. z 2004 r. Nr 210, poz. 2135.
[52] Decyzja GIODO z 26 lipca 2011 r. odmawiająca uwzględnienia wniosku skarżącej, która kwestionowała istnienie swojego zadłużenia wobec telefonii komórkowej i w związku z tym poddała w wątpliwość legalność udostępnienia jej danych osobowych na stronie internetowej przez firmę windykacyjną, DOLiS/DEC-609/11, http://www.giodo.gov.pl/305/id_art/4672/j/pl/.

Zgoda na przetwarzanie danych osobowych może obejmować przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.

W przypadku, gdy przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą, a niemożliwym jest uzyskanie od niej zgody, dopuszcza się przetwarzanie do czasu, gdy uzyskanie zgody będzie możliwe. Interesem takim jest na przykład ratowanie zdrowia i życia. Z przepisów ustawy o Państwowym Ratownictwie Medycznym[53] wynika, że osoba udzielająca pierwszej pomocy, kwalifikowanej pierwszej pomocy oraz podejmująca medyczne czynności ratunkowe, może poświęcić dobra osobiste innej osoby, inne niż życie lub zdrowie, a także dobra majątkowe w zakresie, w jakim jest to niezbędne dla ratowania życia lub zdrowia osoby znajdującej się w stanie nagłego zagrożenia zdrowotnego.

Administrator danych, zbierając dane osobowe od osoby, której one dotyczą, obowiązany jest poinformować ją o pełnej nazwie i adresie siedziby lub imieniu, nazwisku i adresie zamieszkania, gdy administrator jest osobą fizyczną. Ciekawym przypadkiem jest osoba fizyczna prowadząca działalność gospodarczą. W myśl przepisów ustawy o swobodzie działalności gospodarczej[54], podaje ona miejsce swojego zamieszkania, nawet gdy jest różne od miejsca prowadzenia działalności.

Na szczególną uwagę zasługuje przepis o konieczności podawania celu zbierania danych, a zwłaszcza o znanych w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych. Naczelny Sąd Administracyjny w wyroku z 4 kwietnia 2003 roku zawarł stwierdzenie, iż:

> „Zgoda na przekazywanie danych musi mieć charakter wyraźny, a jej wszystkie aspekty muszą być jasne dla podpisującego w momencie jej wyrażania. Czynności takiej nie konwaliduje późniejsze poinformowanie o treści regulaminu, ani możliwość zgłoszenia zastrzeżeń wobec pewnych form przetwarzania danych"[55].

[53] Ustawa z 8 września 2006 r. o Państwowym Ratownictwie Medycznym, Dz.U. z 2006 r. Nr 191, poz. 1410.

[54] Ustawa z 2 lipca 2004 r. o swobodzie działalności gospodarczej, Dz.U. z 2004 r. Nr 173, poz. 1807.

[55] Wyrok NSA w Warszawie z 4 kwietnia 2003 r. dotyczący wyrażenia zgody na przetwarzanie danych osobowych Skarżących w celach marketingu produktów i usług Spółki, Sygn. akt II SA 2135/2002, http://www.giodo.gov.pl/496/id_art/188/j/pl/.

Przekazujący winien być poinformowany również o przewidywanych odbiorcach lub kategoriach odbiorców danych, prawie dostępu do treści swoich danych oraz ich poprawiania, a także dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.

Za odbiorcę danych nie uważa się:

- osoby, której dane dotyczą,
- osoby upoważnionej do przetwarzania danych,
- przedstawiciela podmiotu przetwarzającego dane osobowe, który ma siedzibę albo miejsce zamieszkania w państwie trzecim,
- organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.

Nie ma konieczności udzielania powyżej przedstawionych informacji jeśli osoba podająca swoje dane osobowe już je posiada lub gdy przepis innej ustawy zezwala na przetwarzanie danych bez ujawniania faktycznego celu ich zbierania.

Niewiele jest jednak przepisów, które w sposób wyraźny zezwalałyby na zbieranie danych bez ujawnienia celu w jakim mogłyby one być wykorzystywane. Do nielicznych przykładów należy ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, która w artykule 34 mówi:

> „Ujawnienie osobom nieuprawnionym, w tym także stronom transakcji lub posiadaczom rachunku, faktu poinformowania Generalnego Inspektora o transakcjach, których okoliczności wskazują, że wartości majątkowe mogą pochodzić z prania pieniędzy albo o rachunkach podmiotów, co do których zachodzi uzasadnione podejrzenie, że mają związek z finansowaniem terroryzmu oraz o transakcjach dokonywanych przez te podmioty, jest zabronione”[56].

Istnieją przepisy zezwalające na przetwarzanie danych osobowych bez wiedzy i zgody osoby, której dane dotyczą. Nie można uznać ich za jednoznaczne ze zgodą na zbieranie bez podawania celu ich wykorzystania [57].

[56] Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U. z 2000 r. Nr 116, poz. 1216.

[57] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych: komentarz*, Wolters Kluwer, Warszawa 2011.

Podobny obowiązek informacyjny spoczywa na administratorze danych, gdy zbiera on dane osobowe nie od osoby, której one dotyczą. Zakres przekazywanych informacji uzupełniony winien być o źródło danych oraz powiadomienie o możliwości wniesienia sprzeciwu lub żądania zaprzestania przetwarzania. Obowiązek jest realizowany bezpośrednio po utrwaleniu zebranych danych. UODO nie nakazuje administratorowi informowania o rodzaju danych, jakie pozyskał. Zainteresowany może z własnej inicjatywy wystąpić o dalsze bardziej szczegółowe informacje. Nie wskazuje także formy przekazania. Ze względu na potencjalny materiał dowodowy zaleca się jednak formę pisemną.

Dodatkowo w stosunku do sytuacji zbierania danych bezpośrednio od osoby, której dotyczą, informowanie nie jest konieczne, gdy:

a) dane te są niezbędne do badań naukowych, dydaktycznych, historycznych, statystycznych lub badania opinii publicznej, ich przetwarzanie nie narusza praw lub wolności osoby, której dane dotyczą, a spełnienie wymagań informacyjnych wymagałoby nadmiernych nakładów lub zagrażałoby realizacji celu badania,
b) dane są przetwarzane przez organy państwowe, organy samorządu terytorialnego oraz państwowe i komunalne jednostki organizacyjne oraz podmioty niepubliczne realizujące zadania publiczne, na podstawie przepisów prawa.

Administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest obowiązany zapewnić, aby dane te były:

- przetwarzane zgodnie z prawem,
- zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
- merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
- przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Zasadę przetwarzania zgodnego z prawem podkreślił Naczelny Sąd Administracyjny w wyroku z 4 marca 2002 roku, w którym przywołał opinię Prezesa Narodowego Banku Polskiego z 19 października 2000 roku, według której żadne względy natury organizacyjno-finansowej nie powinny być

traktowane jako podstawy do sprzecznego z prawem przetwarzania danych osobowych przez banki i przez zainteresowanego[58].

Przetwarzanie danych w innym celu niż ten, dla którego zostały zebrane, jest dopuszczalne, jeżeli nie narusza praw i wolności osoby, której dane dotyczą, oraz następuje w celach badań naukowych, dydaktycznych, historycznych lub statystycznych z zachowaniem obowiązków informacyjnych z ich zastrzeżeniami.

Problem długości przechowywania danych dotyczy w szczególności kopii zapasowych. Jednakże Naczelny Sąd Administracyjny w wyroku z 3 lipca 2009 roku[59] wyraził pogląd, że nakaz usuwania danych osobowych z *backupów* nie jest prawidłową interpretacją ustawy o ochronie danych osobowych. Rozporządzenie ministra spraw wewnętrznych i administracji z 19 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych wprowadza w § 5 pkt 4 pojęcie kopii zapasowych[60]. Administrator ma jednak prawo przechowywać dane osobowe tak długo, jak w ogóle ma prawo przetwarzać te informacje.

Ustawa o ochronie danych osobowych jako pierwszy akt prawny w Polsce formalnie zakazuje automatyzacji decyzji w sprawach indywidualnych[61]. Artykuł 26a stanowi, iż:

> „1. Niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym.
>
> 2. Przepisu ust. 1 nie stosuje się, jeżeli rozstrzygnięcie zostało podjęte podczas zawierania lub wykonywania umowy i uwzględnia

[58] Wyrok Naczelnego Sądu Administracyjnego z 4 marca 2002 r., II SA 3144/01.

[59] Wyrok Naczelnego Sądu Administracyjnego z 3 lipca 2009 r., I OSK 633/08.

[60] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U. z 2004 r. Nr 100, poz. 1024.

[61] J. Janowski, *Elektroniczny obrót prawny*, Wolters Kluwer, Warszawa 2008.

wniosek osoby, której dane dotyczą, albo jeżeli zezwalają na to przepisy prawa, które przewidują również środki ochrony uzasadnionych interesów osoby, której dane dotyczą"[62].

Szczególną kategorią danych są dane wrażliwe[63], inaczej zwane sensytywnymi[64]. Oba pojęcia spotykane w literaturze odnoszą się do danych wyszczególnionych w artykule 27 UODO, ujawniających:

- pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub filozoficzne,
- przynależność wyznaniową, partyjną lub związkową,
- informacje o stanie zdrowia,
- informacje o kodzie genetycznym,
- informacje oraz dane o nałogach lub życiu seksualnym,
- informacje dotyczące skazań, orzeczeń o ukaraniu i mandatach karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Przetwarzanie wyszczególnionych powyżej danych jest generalnie zakazane, chyba że osoba, której dane dotyczą, wyrazi na to zgodę. Zgoda ta musi jednak przyjąć formę pisemną. Dopuszczalne jest również na mocy przepisów szczególnych innych ustaw oraz, gdy jest to niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora.

Dochodzenie praw przed sądem, realizacja praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym, prowadzenie prac naukowych, ochrona zdrowia i życia to okoliczności dopuszczające przetwarzanie danych wrażliwych. Publikacje powstałe w wyniku prowadzonych prac badawczych nie mogą jednak pozwalać na identyfikację konkretnych osób, których dane zbierano.

[62] Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych, op. cit.

[63] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer, Warszawa 2010.

[64] P. Wacławska, *Jak dobrać bezbłędnych pracowników: czyli minimalizowanie ryzyka osobowego na etapie poprzedzającym nawiązanie stosunku pracy*, Wolters Kluwer, Warszawa 2008.

Osoba, która podała do publicznej wiadomości swoje dane osobowe, zrzeka się tym samym praw do ich ochrony. Przetwarzać dane sensytywne może także administrator danych przy zatrudnianiu pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie. Podobnie związki wyznaniowe, stowarzyszenia, organizacje niezarobkowe lub instytucje o celach politycznych, naukowych, religijnych, filozoficznych czy związkowych mogą przetwarzać dane wrażliwe swoich członków lub osób utrzymujących z nimi stałe kontakty, w związku z ich działalnością, i zapewnione są pełne gwarancje ochrony przetwarzanych danych. Gwarancja ta jest dyskusyjna, gdyż pomimo że związki wyznaniowe zobowiązane są do przestrzegania UODO, to przepisy gwarantują im możliwość posługiwania się wewnętrznie ustalonym prawem, a GIODO nie może wydawać decyzji administracyjnych, rozpatrywać skarg ani dokonywać w nich kontroli.

Jak już wspominano, numery PESEL, nawet występujące samodzielnie, stanowią dane osobowe. UODO nie zabrania ich przetwarzania, jednak określa, jakie informacje mogą być zawarte w numerze porządkowym stosowanym w ewidencji ludności. Są to:

- oznaczenie płci,
- data urodzenia,
- numer nadania,
- liczba kontrolna.

Równocześnie UODO zabrania stosowania wszelkich ukrytych znaczeń elementom numerów porządkowych w systemach ewidencjonujących osoby fizyczne.

Administrator danych może powierzyć innemu podmiotowi przetwarzanie danych. Dzięki instytucji powierzenia, można skorzystać ze specjalistycznej wiedzy innych podmiotów. Nie jest wymagana zgoda osoby, której dane dotyczą. Ustawa wymaga natomiast, aby umowa łącząca zleceniodawcę i zleceniobiorcę zawarta była na piśmie oraz wyraźnie określała zakres i cel przetwarzania danych. Podmiot, któremu powierzono przetwarzanie danych, nie staje się ich administratorem, jednakże ponosi na równi z nim odpowiedzialność i może być tak samo jak on kontrolowany przez GIODO. Z tego też względu administrator danych upoważniony jest do kontroli podmiotu, któremu dane powierzono, w zakresie przestrzegania zapisów umowy powierzenia oraz zabezpieczenia danych zgodnie z UODO.

Rozdział 5. Prawa osoby, której dane dotyczą

Prawa osoby, której dane dotyczą, zostały opisane w rozdziale 4 ustawy o ochronie danych osobowych. Związane są w dużej mierze z obowiązkami administratora danych. Administrator zobowiązany jest do informowania osoby w przypadku zbierania o niej danych. Osoba, której dane dotyczą, ma prawo do kontroli ich przetwarzania w zbiorach danych. Kontroli nie podlegają dane zawarte w przeróżnego rodzaju pismach, wiadomościach itp., które nie mają charakteru zbioru danych i nie stanowią jego części.

Przytoczone w UODO prawa kontrolne można podzielić na 3 grupy, wyszczególnione w tabeli 2.

Opisane uprawnienia, przysługujące każdemu obywatelowi, są kłopotliwe dla administratora danych, szczególnie gdy zbiory prowadzone są poza systemem informatycznym. Czas wyszukiwania, jaki niezbędny jest do pozyskania informacji, jak również duża liczba wniosków może sparaliżować jego pracę. Dlatego też ustawodawca narzucił kilka ograniczeń.

Osoba zainteresowana może skorzystać z prawa do informacji, wnioskując o nią nie częściej niż raz na 6 miesięcy, a termin, w jakim administrator danych jest obowiązany udzielić odpowiedzi, wynosi 30 dni. Na wniosek osoby zainteresowanej informacja udzielana jest w formie pisemnej.

Administrator może odstąpić od informowania osób o przetwarzaniu ich danych, jeżeli dane są przetwarzane dla celów naukowych, a realizacja obowiązku informacyjnego pociągałaby za sobą nakłady niewspółmierne z zamierzonym celem.

Tabela 2. Prawa osoby, której dane dotyczą

Grup praw	Prawo
Prawa do uzyskania informacji	Prawo do uzyskania wyczerpującej informacji, czy taki zbiór istnieje, oraz do ustalenia administratora danych, adresu jego siedziby i pełnej nazwy, a w przypadku gdy administratorem danych jest osoba fizyczna – jej miejsca zamieszkania oraz imienia i nazwiska.
	Prawo do uzyskania informacji o celu, zakresie i sposobie przetwarzania danych zawartych w takim zbiorze.
	Prawo do uzyskania informacji, od kiedy przetwarza się w zbiorze dane jej dotyczące, oraz podania w powszechnie zrozumiałej formie treści tych danych.
	Prawo do uzyskania informacji o źródle, z którego pochodzą dane jej dotyczące, chyba że administrator danych jest zobowiązany w tym zakresie do zachowania w tajemnicy informacji niejawnych lub zachowania tajemnicy zawodowej.
	Prawo do uzyskania informacji o sposobie udostępniania danych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym dane te są udostępniane.
	Prawo do uzyskania informacji o przesłankach podjęcia rozstrzygnięcia, indywidualnej sprawy osoby, której dane dotyczą.
Prawa do korygowania informacji	Prawo do żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.
	Prawo do wniesienia do administratora danych żądania ponownego, indywidualnego rozpatrzenia sprawy rozstrzygniętej wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym.
Prawa do zakazywania	Prawo do wniesienia pisemnego, umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację, gdy przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego lub dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych.
	Prawo wniesienia sprzeciwu wobec przetwarzania danych, gdy administrator danych zamierza je przetwarzać w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych, w przypadku, gdy przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego lub dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych.

Źródło: opracowanie własne.

Administrator danych może odmówić udzielenia informacji osobie, której dane dotyczą, w następujących przypadkach:

- informacje należą do kategorii informacji niejawnych,
- ujawnienie informacji może spowodować zagrożenie dla obronności lub bezpieczeństwa państwa, życia i zdrowia ludzi lub bezpieczeństwa i porządku publicznego,
- ujawnienie informacji może stanowić zagrożenie dla podstawowego interesu gospodarczego lub finansowego państwa,
- ujawnienie informacji stanowi istotne naruszenie dóbr osobistych osób, których dane dotyczą, lub innych osób.

Trudno sobie jednak wyobrazić sytuację, gdy udzielenie informacji osobie, której dane dotyczą, naruszałoby jej dobra osobiste.

Pamiętając, iż przepisy innych ustaw mają pierwszeństwo przed UODO, należy zadać pytanie, czy administrator danych w instytucji publicznej nie powinien stosować Kodeksu postępowania administracyjnego, a odpowiedzi traktować jako Zaświadczenia, dla którego termin wydania został ustalony na 7 dni. W literaturze przeważa jednak stanowisko, iż udzielenie informacji jest jednak czynnością faktyczną.

Następnym problemem, z jakim spotyka się administrator danych, jest obowiązek podania treści danych w powszechnie zrozumiałej formie. Związane jest to zazwyczaj z wyjaśnieniem stosowanych skrótów i oznaczeń. Koniecznym może być zdefiniowanie pojęć, opisanie kontekstu czy stosowanych kategorii. Równie wymagającym przepisem jest wymóg podawania źródła. Niewystarczającym jest określenie kategorii takich jak ogólnodostępne źródła, strony internetowe czy prasa powszechna. Konieczność wskazania konkretnego źródła sprawia, iż administrator powinien rejestrować, skąd zaczerpnął wiedzę o każdej z danych dotyczących konkretnej osoby. Dość często spotykana jest bowiem sytuacja, że dane osobowe pojedynczej osoby pochodzą z wielu różnych źródeł.

Jak wynika z tabeli 2, zainteresowany może wnieść sprzeciw wobec przetwarzania jego danych lub żądanie zaprzestania przetwarzania. Żądanie musi mieć formę pisemną i być umotywowane. Administrator może je uznać i zaprzestać przetwarzania lub przekazać, bez zbędnej zwłoki, Generalnemu Inspektorowi Ochrony Danych Osobowych celem rozpatrzenia i wydania decyzji. Wniesienie sprzeciwu skutkuje koniecznością usunięcia danych. Ustawodawca dopuszcza jednak pozostawienie w zbiorze imienia lub imion

i nazwiska oraz numeru PESEL lub adresu, wyłącznie w celu uniknięcia ponownego wykorzystania danych tej osoby w celach objętych sprzeciwem.

Podobnie jak sprzeciw wobec przetwarzania, wniesienie żądania ponownego, indywidualnego rozpatrzenia sprawy, rozstrzygniętej automatycznie w systemie informatycznym, narzuca administratorowi danych obowiązek rozpatrzenia sprawy lub przekazania jej wraz z uzasadnieniem swojego stanowiska Generalnemu Inspektorowi, który wydaje stosowną decyzję.

Uprawnienie osoby, której dane dotyczą, do uaktualniania czy sprostowania danych osobowych, jest korzystne również dla administratora danych, gdyż prowadzi do uzyskania zgodności danych ze stanem faktycznym. Pamiętać należy, że jest to prawo, a nie obowiązek osoby, której dane dotyczą. Administrator danych nie może żądać jedynie na podstawie UODO, aby korygowała lub uaktualniała ona swoje dane. Niekompletność, nieaktualność, niezgodność z prawdą, podobnie jak zebranie danych z naruszeniem prawa, jak również nieadekwatność w stosunku do realizacji celu przetwarzania, pociągają za sobą konsekwencje.

Gdy osoba, której dane dotyczą, wskaże choć jedną z wymienionych przesłanek, administrator danych jest obowiązany, bez zbędnej zwłoki, do uzupełnienia, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru. Wyjątkiem jest sytuacja, gdy tryb uzupełnienia, uaktualnienia lub sprostowania określają odrębne ustawy. Ustawą taką jest Ustawa z 13 października 1995 roku o zasadach ewidencji i identyfikacji podatników i płatników[65], która nakłada na podatników obowiązek dokonania zgłoszenia aktualizacyjnego do naczelnika urzędu skarbowego, nie później niż w terminie 7 dni od dnia, w którym nastąpiła zmiana danych.

W razie niedopełnienia przez administratora danych obowiązku korygowania informacji, osoba, której dane dotyczą, może się zwrócić do Generalnego Inspektora z wnioskiem o nakazanie dopełnienia tego obowiązku. Nie może on jednak nakazać sprostowania danych osobowych w decyzjach

[65] Ustawa z 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników, Dz.U. z 1995 r. Nr 142, poz. 702.

administracyjnych innych organów administracji publicznej[66]. Zdaniem Naczelnego Sądu Administracyjnego osoba, której dane dotyczą, nie może się powoływać na UODO w sprawie oczywistych omyłek w decyzjach administracyjnych, gdyż pomyłki takie prostuje organ, który je uczynił, w drodze postanowienia, na które służy zażalenie[67].

Uaktualnienie czy sprostowanie danych w zbiorze prowadzonym przez administratora danych nakłada na niego następny obowiązek, którym jest poinformowanie bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych, o dokonanych zmianach. Nie obowiązuje jednak w przypadku korekty danych osobowych przetwarzanych poza zbiorem. W zakresie tym UODO spotkało się z falą krytyki ze względu na brak określenia horyzontu czasowego. Odbiorcy, którym administrator danych osobowych udostępnił jednorazowo zbiór przed kilkudziesięciu laty, z dużym prawdopodobieństwem nie będą już zainteresowani korygowaniem danych w nim zawartych. Korekty te mogą dotyczyć również zupełnie nieistotnych zmian, np. literówek.

Krytykowane jest również zawężenie obowiązku tylko do informowania administratorów, którym udostępniono zbiory. W przypadku udostępniania samych informacji ze zbioru konieczność informowania o korektach już nie zachodzi.

[66] G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Dom Wydawniczy ABC, Warszawa 2003.

[67] Postanowienie Naczelnego Sądu Administracyjnego z 9 listopada 1999 r., II SAB 153/99.

Rozdział 6. Zabezpieczenie danych osobowych

UODO zobowiązuje administratora danych do stosowania środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną. W szczególności wyróżnia zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Mamy tu do czynienia z klasycznymi atrybutami bezpieczeństwa informacji wyszczególnionymi w normie PN-ISO/IEC 27001[68], którymi są:

- poufność – właściwość polegająca na tym, że informacja nie jest udostępniana lub ujawniana nieautoryzowanym osobom, podmiotom lub procesom,
- integralność – właściwość polegająca na zapewnieniu dokładności i kompletności informacji,
- dostępność – właściwość bycia dostępnym i użytecznym na żądanie autoryzowanego podmiotu[69].

Jednym ze środków organizacyjnych jest prowadzenie przez administratora danych osobowych (ADO) odpowiedniej dokumentacji. Może ją prowadzić administrator bezpieczeństwa informacji (ABI), powołany przez administratora danych. Kandydat na administratora bezpieczeństwa informacji winien charakteryzować się:

---

[68] Polska Norma PN-ISO/IEC 27001:2014-12, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, PKN, Warszawa 2012.

[69] Polska Norma PN-ISO/IEC 27000:2012, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia, PKN, Warszawa 2012.

- zdolnością do czynności prawnych oraz korzystaniem z pełni praw publicznych,
- niekaralnością za umyślne przestępstwo,
- odpowiednią wiedzą w zakresie ochrony danych osobowych.

UODO nie określa wykształcenia, jakie powinien posiadać ABI. W ustawie poruszane są zarówno aspekty techniczne, jak i prawne. Idealnym kandydatem byłaby osoba, której nieobce są oba typy zagadnień. Ponad połowa administratorów bezpieczeństwa informacji w administracji publicznej to informatycy[70].

ADO może powołać także zastępców ABI oraz administratorów systemów informatycznych (ASI). ABI musi posiadać niezależność organizacyjną, podlegać jedynie kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych oraz dysponować odpowiednimi środkami.

Wyznaczony ABI musi być zarejestrowany w jawnym rejestrze administratorów bezpieczeństwa informacji prowadzonym przez GIODO, dostępnym pod adresem https://egiodo.giodo.gov.pl/abi_register.dhtml, którego wygląd ekranów został zaprezentowany na rysunku 8.

Wzór druku zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji, wprowadzony przez rozporządzenie Ministra Administracji i Cyfryzacji z 10 grudnia 2014 roku[71], zawiera załącznik 3.

Na chwilę pisania rozdziału rejestr prowadzony przez GIODO nie umożliwiał wprowadzania wniosków.

Administrator bezpieczeństwa informacji ma za zadanie sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych. Nadzoruje opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych osobowych oraz przestrzegania zasad w niej określonych. Zajmuje się szkoleniem osób upoważnionych przez ADO do przetwarzania danych osobowych w zakresie UODO oraz funkcjonujących w organizacja zasadach.

[70] M. Meszczyński, *Edukacja przede wszystkim*, „IT w administracji" marzec 2010.

[71] Rozporządzenie Ministra Administracji i Cyfryzacji z 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji, Dz.U. z 2014 r., poz. 1934.

Rys. 8. Wygląd ekranów rejestru administratorów bezpieczeństwa informacji prowadzonego przez GIODO

Źródło: portal e-GIODO, https://egiodo.giodo.gov.pl/index.dhtml.

Zadania kontrolne administratora bezpieczeństwa informacji sprecyzowane zostały w Rozporządzeniu Ministra Administracji i Cyfryzacji z 11 maja 2015 roku w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji[72]. Określa ono sposób sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych wraz ze sposobem opracowania sprawozdania oraz prowadzenia nadzoru nad opracowaniem i aktualizowaniem dokumentacji opisującej sposób przetwarzania danych, jak również nad środkami technicznymi i organizacyjnymi zapewniającymi ochronę oraz nad przestrzeganiem zasad określonych w dokumentacji.

Sprawdzenie zostało zdefiniowane jako czynności mające na celu zweryfikowanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, w szczególności w wyniku zwrócenia się o dokonanie sprawdzenia przez Generalnego Inspektora Ochrony Danych Osobowych.

Rysunek 9 przedstawia rodzaje sprawdzeń.

Sprawdzenia planowe odbywają się według planu przygotowanego przez administratora bezpieczeństwa informacji. Obejmuje on przynajmniej jedno sprawdzenie w okresie czasowym, nie krótszym niż kwartał i nie dłuższym niż rok. Plan ten musi być przedłożony administratorowi danych nie później niż 2 tygodnie przed rozpoczęciem okresu objętego planem. Uwzględnia potrzebę:

- weryfikacji zgodności zasad przetwarzania danych osobowych,
- kontroli zabezpieczenia danych osobowych,
- weryfikacji zgodności z zasadami przekazywania danych osobowych,
- kontroli przestrzegania obowiązku zgłoszenia zbiorów danych do rejestracji i ich aktualizacji.

Przy tworzeniu planu należy wziąć pod uwagę, iż każdy ze zbiorów danych osobowych oraz program służący do ich przetwarzania należy poddać sprawdzeniu nie rzadziej niż co 5 lat.

[72] Rozporządzenie Ministra Administracji i Cyfryzacji z 11 maja 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.

Sprawdzanie doraźne wykonywane jest niezwłocznie po uzyskaniu przez administratora bezpieczeństwa informacji o naruszeniu ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia. Przed przeprowadzeniem sprawdzenia ABI musi jednak zawiadomić administratora danych o jego rozpoczęciu.

Rys. 9. Rodzaje sprawdzania

Źródło: opracowanie własne.

Dokumentowanie czynności w toku sprawdzania może polegać na utrwaleniu danych z systemów informatycznych na nośnikach danych lub dokonaniu wydruku tych danych, oraz na sporządzeniu w formie papierowej lub dokumentów elektronicznych:

- notatki z czynności,
- protokoły z ustnych wyjaśnień lub oględzin,
- kopie otrzymanych dokumentów,
- kopie obrazu wyświetlonego na ekranie urządzenia,
- kopie zapisów rejestrów systemów informatycznych,
- kopie zapisów konfiguracji technicznych środków zabezpieczeń.

Czynności ABI w wykorzystanym systemie informatycznym służącym do przetwarzania danych są wykonywane w obecności osób upoważnionych, a w szczególności administratora systemu. Podobnie osoba odpowiedzialna za przetwarzanie bierze udział w sprawdzeniu lub umożliwia jego wykonanie administratorowi bezpieczeństwa informacji. Kierownik jednostki organizacyjnej poddanej sprawdzeniu powiadamiany jest co najmniej 7 dni sprzed terminem rozpoczęcia. Administrator bezpieczeństwa informacji może pominąć wspomniane powiadomienie, gdy wymagana jest niezwłoczna interwencja w celu przywrócenia stanu zgodnego

z prawem lub weryfikacji czy naruszenie prawa miało miejsce. Możliwe jest również, iż termin sprawdzenia, wyznaczony przez GIODO, nie pozwoli na terminowe powiadomienie kierownika jednostki poddanej sprawdzeniu. Posiadanie informacji przez wspomnianego kierownika o terminie sprawdzenia zwalnia również ADO z omawianego obowiązku.

Sprawdzanie kończy się przygotowaniem przez ABI sprawozdania. Termin sporządzenia sprawozdania uzależniony jest od rodzaju sprawdzenia, i tak:

- dla sprawdzenia planowego – termin określony w planie nie dłuższy niż 30 dni od zakończenia sprawdzenia,
- dla sprawdzenia pozaplanowego – niezwłoczne po zakończeniu sprawdzenia,
- dla sprawdzenia zleconego przez GIODO – termin umożliwiający zachowanie terminu przez administratora danych.

Nadzór nad dokumentacją przetwarzania danych osobowych realizowany jest w ramach omawianych powyżej sprawdzeń lub na podstawie zgłoszeń od osób trzecich. W przypadku stwierdzenia nieprawidłowości, administrator bezpieczeństwa zawiadamia o tym fakcie ADO, przedstawiając do wdrożenia dokumenty korygujące, poucza lub instruuje osoby odpowiedzialne za naruszenie zasad. Zawiadomienia i pouczenia mogą mieć formę zarówno pisemną, jak i elektroniczną.

6.1. Dokumentacja przetwarzania danych osobowych

Sposób prowadzenia dokumentacji przetwarzania danych osobowych regulowany jest przede wszystkim rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 roku[73]. Dokumentacja ta wdrażana jest przez administratora danych osobowych i prowadzona w formie pisemnej. Składa się na nią polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych. Ich zawartość została zaprezentowana w tabeli 3.

[73] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U. z 2004 r. Nr 100, poz. 1024.

Tabela 3. Zawartość polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Polityka bezpieczeństwa	Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe	Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności
Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem
Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu
Sposób przepływu danych pomiędzy poszczególnymi systemami	Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania
Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	Sposób, miejsce i okres przechowywania: • elektronicznych nośników informacji zawierających dane osobowe • kopii zapasowych
	Sposób zabezpieczenia systemu informatycznego przed działalnością szkodliwego oprogramowania
	Sposób realizacji wymogów rejestracji przez system informacji związanych z przetwarzaniem danych osobowych
	Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych

Źródło: opracowanie własne.

W wykazie budynków, pomieszczeń lub części pomieszczeń należy umieścić nie tylko obszary, w których pracownicy wykonują swoje obowiązki służbowe, lecz także serwerownie, archiwa czy magazyny z zepsutymi komputerami lub wycofywanymi nośnikami danych. Są to także pomieszczenia, w których przetwarza się dane osobowe. Dodatkowo konieczne jest wprowadzenie informacji o podmiotach, którym umożliwiano przetwarzanie zdalne, za wyjątkiem sytuacji, gdy system zapewnia zgodny z prawem dostęp o charakterze publicznym.

Prowadzenie wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych z pozoru nie wydaje się trudne. Jednakże zalecenia GIODO mówiące, iż powinien zawierać „informacje precyzujące lokalizację miejsca (budynek, pomieszczenie, nazwa komputera lub innego urządzenia, np. macierzy dyskowej, biblioteki optycznej), w którym znajdują się zbiory danych osobowych przetwarzane na bieżąco oraz nazwy i lokalizacje programów (modułów programowych) używanych do ich przetwarzania”[74] sprawia wiele kłopotów w realizacji.

Większość użytkowanych systemów informatycznych pozwala na wielodostęp do jednej lub wielu baz danych, które nie zawsze odpowiadają wprost zbiorom danych. Podział systemów na odpowiednie moduły, powiązane z wyodrębnionymi z baz zbiorami i przyporządkowanie im urządzeń oraz obszarów przetwarzania to zadanie wymagające silnego zaangażowania również administratora systemu informatycznego.

Nie mniejszy kłopot sprawia opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi. Nie tylko użytkownik, ale często i administrator systemu nie zna wspomnianej struktury, gdyż powszechnie stosowane relacyjne bazy danych składają się często z setek połączonych ze sobą tabel. Producenci niechętnie zdradzają ich strukturę, ograniczając się jedynie do wyszczególnienia pól zawierających dane osobowe. Jeszcze bardziej rygorystycznie traktują zagadnienia związane z przepływem danych pomiędzy modułami systemu lub swoimi systemami.

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, poza środkami proceduralnymi, wymaga z reguły wiedzy specjalistycznej. Środki te winny być adekwatne do zagrożeń. Ich wdrożenie powinno być więc poprzedzone analizą ryzyka, o której będzie mowa w dalszej części pracy.

UODO narzuca konieczność utrzymania przez ABI rejestru zbiorów danych osobowych, które nie zawierają danych wrażliwych. Szczegółowe zasady jego prowadzenia zamieszczone są w rozporządzeniu Ministra

[74] *ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych*, GIODO, Wydawnictwo Sejmowe, Warszawa 2007, s. 12.

Administracji i Cyfryzacji, które zostanie omówione w dalszej części niniejszego tomu.

Kolejnym rejestrem, którego prowadzenie jest niezbędne do zgodnego z prawem przetwarzania danych osobowych, jest zbiór upoważnień. Winien on zawierać dane pozwalające na jednoznaczną identyfikację upoważnionej osoby, a więc jej imię i nazwisko oraz PESEL lub serię i numer dowodu tożsamości. Każdej z nich należy przypisać zbiory danych osobowych wraz z zakresem przetwarzania, do którego są upoważnione. Pomocne jest również zamieszczenie loginów użytkowników systemów informatycznych, służących do przetwarzania danych osobowych. Zaleca się odnotowanie obszarów, w których są uprawnieni do przebywania. Należy pamiętać, że zarówno rejestr, jak i same upoważnienia dotyczą nie tylko pracowników, lecz również osób związanych pośrednio z organizacją, jak praktykanci czy osoby wykonujące prace na podstawie innej niż umowa o pracę.

6.2. Wymagania dla systemów informatycznych służących do przetwarzania danych osobowych

Rozporządzenie ustala trzy poziomy ochrony danych osobowych, pokazane w tabeli 4. Kryteriami podziału jest przetwarzanie danych wrażliwych oraz podłączenie urządzeń wchodzących w skład systemu informatycznego do sieci publicznej, czyli sieci telekomunikacyjnej wykorzystywanej głównie do świadczenia publicznie dostępnych usług telekomunikacyjnych[75].

Wszystkie systemy informatyczne służące do przetwarzania danych, które zostały dopuszczone przez właściwą służbę ochrony państwa do przetwarzania informacji niejawnych, spełniają wymogi omawianego rozporządzenia pod względem bezpieczeństwa na poziomie wysokim.

Rozporządzenie wprowadza również dla systemu informatycznego przetwarzającego dane osobowe wymaganie odnośnie do rejestracji dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, następujących danych:

- daty pierwszego wprowadzenia danych do systemu,
- identyfikatora użytkownika wprowadzającego dane osobowe do systemu, chyba że dostęp do systemu informatycznego i przetwarzanych w nim danych posiada wyłącznie jedna osoba,

[75] Ustawa z 16 lipca 2004 r., Prawo telekomunikacyjne, Dz.U. z 2004 r. Nr 171, poz. 1800.

- źródła danych w przypadku zbierania ich nie od osoby, której dotyczą,
- informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych,
- sprzeciwu wobec przetwarzania danych osobowych.

Tabela 4. Poziomy ochrony danych osobowych

Nazwa	Warunki stosowania	Środki bezpieczeństwa
Podstawowy	Brak danych wrażliwych Urządzenie niepodłączone do sieci publicznej	Ochrona obszaru przetwarzania danych osobowych Kontrola dostępu Zabezpieczenie przed oprogramowaniem uzyskującym nieuprawniony dostęp Ochrona przed awarią i zakłóceniami zasilania Nieprzydzielanie identyfikatora, który utracił ważność innemu użytkownikowi Zmiana hasła co 30 dni Minimalna długość hasła – 6 znaków Zabezpieczone kopie zapasowe usuwane po okresie ich użyteczności Środki kryptograficzne w urządzeniach przenośnych Pozbawianie zapisu nośników informacji likwidowanych lub przekazywanych podmiotom nieuprawnionym
Podwyższony	Przetwarzane są dane wrażliwe Urządzenie niepodłączone do sieci publicznej	Środki bezpieczeństwa poziomu podstawowego Hasła składające się co najmniej z 8 znaków, zawierające małe i wielkie litery oraz cyfry lub znaki specjalne Urządzenia i nośniki zabezpieczone w sposób zapewniający poufność i integralność danych ujęte w instrukcji zarządzania systemem informatycznym
Wysoki	Przynajmniej jedno z urządzeń podłączone do sieci publicznej	Środki bezpieczeństwa poziomu podstawowego Środki bezpieczeństwa poziomu podwyższonego Fizyczne lub logiczne zabezpieczenia chroniące przed nieuprawnionym dostępem poprzez sieć publiczną Środki kryptograficznej ochrony danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej

Źródło: opracowanie własne.

Dane te zapisywane są automatycznie w systemie przy operacji wprowadzania danych osobowych. W systemie powinna tez być możliwość sporządzenie

i wydrukowania raportu prezentującego je w powszechnie zrozumiałej formie. Powyższe przepisy nie dotyczą systemów służących do przetwarzania danych osobowych ograniczonych wyłącznie do edycji tekstu w celu udostępnienia go na piśmie.

Omawiany wymóg rejestracji jest niemożliwy do spełnienia dla systemów, które zostały opracowane przed wejściem w życie UODO, a które utraciły wsparcie techniczne. Pewne rozwiązanie nasuwa się po analizie kolejnego przepisu rozporządzenia mówiącego o przypadku przetwarzania danych osobowych w co najmniej dwóch systemach informatycznych. Automatyczna rejestracja przedstawionych powyżej danych może być realizowana w jednym z nich lub w odrębnym systemie informatycznym przeznaczonym do tego celu.

Rozdział 7. Techniczne środki bezpieczeństwa

Budowa systemu zarządzania bezpieczeństwem informacji opiera się między innymi na doborze odpowiednich środków technicznych. Do dyspozycji jest ich szeroki wachlarz, zróżnicowany pod względem cenowym, jakościowym i wydajnościowym. Zapoznanie się z funkcjonującymi na rynku rozwiązaniami oraz poznanie trendów rozwojowych niezbędne jest do opracowania projektu systemu, który spełni wymagania organizacji.

Różnorodność oraz dostępność technologii, choć korzystna z punktu widzenia projektantów, stanowi jednak problem dla kadry zarządzającej, która zwraca szczególną uwagę na koszty funkcjonowania przedsiębiorstwa. Znając jedynie hasłowo pojęcia związane z informatyką, kierownictwo powinno uzyskać jasno sprecyzowane dane na temat parametrów doboru technologii, którymi kierowali się projektanci i ich wpływ na bezpieczeństwo, stabilność, wydajność i niezawodność systemu. Z tego też względu poniżej skrótowo przedstawiono podstawowe informacje o wykorzystywanych w systemach bezpieczeństwa informacji technologiach. Są to zamieszczone w poszczególnych podrozdziałach:

- kopie bezpieczeństwa,
- identyfikacja, uwierzytelnianie i autoryzacja,
- techniki kryptograficzne,
- zasilanie awaryjne,
- nadmiarowość,
- fizyczna ochrona informacji.

W tej kolejności omówiono w dalszych podrozdziałach istotne aspekty bezpieczeństwa systemów informatycznych, w tym tych służących do przetwarzania danych osobowych.

7.1. Kopie bezpieczeństwa

Pojęcie *backup* jest często mylone z archiwizacją i kopią bezpieczeństwa. Obejmuje zespół czynności mających na celu zapis i przechowywanie informacji na nośniku innym niż macierzysty. W odróżnieniu od archiwizacji, kopia bezpieczeństwa obejmuje, oprócz danych, także oprogramowanie pozwalające na ich interpretację. Zazwyczaj pozwala na szybkie odtworzenie systemu informatycznego w przypadku jego uszkodzenia.

Analitycy szacują, że całkowita liczba wytworzonych danych przekracza 3 ZB (zettabajtów), a tempo ich przyrostu zwiększa się z roku na rok. Koszty nośników są więc ważnym elementem wpływającym na metody składowania danych. Równie istotnymi czynnikami są: czas potrzebny na wykonanie kopii, czas niezbędny do ich odtworzenia oraz niezawodność nośników, na jakich są one zapisane.

Ze względu na technologię zapisu możemy wyszczególnić 5 rodzajów nośników:

- taśmy magnetyczne,
- dyski magnetyczne,
- dyski magnetooptyczne,
- dyski optyczne,
- pamięci typu „flash".

Taśmy magnetyczne stosowane są już od 50 lat. Te najbardziej popularne w profesjonalnych zastosowaniach nośniki wykorzystują właściwości materiałów ferromagnetycznych pokrywających taśmy z tworzywa sztucznego.

Taśmowe nośniki danych są obecnie powszechnie stosowane, ale daje się zauważyć tendencję do wypierania ich przez rozwiązania bazujące na dyskach magnetycznych. Potentat w dziedzinie oprogramowania systemowego już od wersji Windows Server 2008 zaprzestał wspierania *backupu* opartego na taśmach. Ich przyszłość rysuje się więc niepewnie.

Najbardziej popularne standardy taśm magnetycznych zostały zaprezentowane w tabeli 5.

Dyski magnetyczne to urządzenia składające się z wirującego talerza (ang. *plate*) lub zespołu talerzy, pokrytego nośnikiem magnetycznym. Rozróżniamy dyski magnetyczne w hermetycznej obudowie – HDD (ang. *Hard Disk Drive*) oraz napędy nośników zewnętrznych FDD (ang. *Floppy Disk Drive*), ZIP, JAZ, LS-120, które straciły na popularności ze względu na zbyt

niskie pojemności i duże czasy dostępu do danych. Od roku 1956, w którym to powstał pierwszy dysk twardy, technologia przeżywa burzliwy rozwój. Rosną pojemności i transfery, postępuje miniaturyzacja[76]. Obecnie na rynku dostępne są dyski o pojemnościach rzędu terabajtów o transferach kilkuset MB/s.

Tabela 5. Parametry taśmowych nośników danych

Nazwa	Najnowszy format	Maksymalna pojemność	Maksymalny transfer
DDS	DDS-8	320 GB	16MB/s
SLR	SLR400	200 GB	32MB/s
DLT	DLT S-4	800 GB	60 MB/s
AIT	SAIT-3	1 TB	120 MB/s
LTO	Ultrium-4	800 GB	160 MB/s

Źródło: opracowanie własne na podstawie: J. Luther, *Napędy taśmowe*, „PC World" 2003, nr 10; *DLT-S4 Buffer Management – Speed matching White Paper*, Quantum Corporation, 5 kwietnia 2006 r.; *8 mm Wide Magnetic Tape Cartridge for Information Interchange – Helical Scan Recording – AIT-3 Format*, ECMA, 12/2001; *LTO Ultrium 2 Tape Drive Introducing Next Generation Tape Technology*, Fujitsu White Paper, lipiec 2003 r.

Dyski magnetooptyczne MO (ang. *Magneto-Optical disk*) to także urządzenia składające się z czytnika i wymiennego nośnika. Nośnikiem tym jest talerz z tworzywa sztucznego, pokryty materiałem magnetycznym i zabezpieczony powłoką ze szkła lub plastiku. Odczyt wykorzystuje efekt Kerra – polaryzacja promienia lasera ulega skręceniu, odbijając się od namagnesowanej powierzchni. Dyski MO, pomimo iż uważane są za rozwiązanie zapewniające najbardziej trwały zapis, to ze względu na małą pojemność (do 9,1 GB) nie są już powszechnie stosowane.

Dyski optyczne składają się z krążka poliwęglanowego, warstwy metalu i powłoki lakierowej lub plastikowej. Dane przechowywane są na warstwie metalicznej, w formie mikroskopijnych rowków (ang. *pits*) i miejsc płaskich (ang. *lands*). Standard CD-ROM (ang. *Compact Disc – Read Only Memory*),

[76] E. Grochowski, R.D. Halem, *Technological impact of magnetic hard disk drives on storage systems*, "IBM Systems Journal" 2003, Vol. 42, No. 2.

powstały pod koniec lat 80. zeszłego wieku, umożliwił jednokrotny zapis 700 MB danych[77]. Nowy, powstały w roku 1995 standard CD-RW (ang. *Compact Disc – Rewritable*) pozwolił na operacje zapisu, odczytu i kasowania[78]. Dzięki zastosowaniu promienia lasera o krótszej długości fali możliwym stało się gęstsze rozmieszczenie ścieżek na nośniku tej samej wielkości. Opracowano standard DVD (pierwotnie ang. *Digital Video Disc*, następnie ang. *Digital Versatile Disc*). Najbardziej popularne na rynku dyski DVD mają pojemność 4,7 GB. Dostępne jednakże są płyty dwustronne, posiadające cztery warstwy nośnika, o łącznej pojemności 17 GB[79].

Najnowszym rozwiązaniem, które pojawiło się na rynku jest dysk BD (ang. *Blue-ray Disc*). W celu zwiększenia pojemności zastosowano niebieski laser zamiast czerwonego, stosowanego w DVD. Ze względu na znacznie mniejszą długość fali możliwe stało się większe zagęszczenie rowków. Jednowarstwowy nośnik umożliwia zapis 25 GB danych. Dostępne są płyty 2-, 4- i 8-warstwowe, o pojemnościach odpowiednio 50 GB, 100 GB i 400 GB.

Pamięć typu „flash" to odmiana pamięci EPROM (ang. *Electrically-Erasable Programmable Read-Only Memory*). Pozwalają na jednoczesną operację na wielu komórkach. Są tzw. pamięcią nieulotną, zatem nie wymagają zasilania do podtrzymywania zawartości. Cykl zapisywania jest ściśle powiązany z wcześniejszym kasowaniem zawartości komórek. O ile można zapisać zawartość pojedynczej komórki, o tyle kasowanie polega na usunięciu zawartości bloku komórek, co ma niebagatelny wpływ na szybkość operacji. Dodatkowym mankamentem pamięci flash jest ograniczona liczba cykli kasowania, po przekroczeniu których ulega ona uszkodzeniu. Obecnie na rynku funkcjonują następujące standardy pamięci flash:

- CF (ang. *CompactFlash*) pojemność do 100 GB, transfer do 100 MB/s,
- MS (ang. *Memory Stick*) pojemność do 32 GB, transfer do 20 MB/s,
- MMC (ang. *MultiMedia Card*) pojemność do 8 GB, transfer do 15 MB/s,
- SD (ang. *Secure Digital*) pojemność 2 TB i transfer 104 MB/s,

[77] *Data interchange on read-only 120 mm optical data disks (CD-ROM)*, ECMA 6/1996, Ecma International, Geneva 1996.

[78] H. Bennett, *Understanding CD-R & CD-RW*, Optical Storage Technology Association, Rev 1.00 1/2003

[79] *Information technology — 120 mm (8,54 Gbytes per side) and 80 mm (2,66 Gbytes per side) DVD recordable disk for dual layer (DVD-R for DL)*, ISO/IEC12862 2009(E), International Organization for Standardization, Geneva 2009.

- SM (ang. *SmartMedia*) pojemność do 128 MB, transfer do 3,5 MB/s,
- xD (ang. *xD Picture Card*) pojemność do 2 GB, transfer do 15 MB/s[80].

Każdy z nośników ma określoną żywotność. Charakteryzuje ją parametr MTBF (ang. *Mean Time Between Failures*), który dla taśm magnetycznych przyjmuje wartość kilku tysięcy godzin, dla dysków magnetycznych – miliony godzin, a dla dysków optycznych oraz magnetooptycznych osiąga nawet 100 lat. Parametru MTBF nie stosuje się dla pamięci flash. Jak już było wspominane powyżej, istotna jest też liczba cykli kasowania i zapisu. Pamiętać należy, że podawane wysokie wartości MTBF obwarowane są licznymi warunkami – np. optymalną temperaturą i wilgotnością pracy. Przyczynami występowania licznych uszkodzeń nośników są także pola magnetyczne czy elektromagnetyczne. Dodatkowo taśmy magnetyczne oraz dyskietki narażone są na uszkodzenia mechaniczne, ze względu na bezpośredni kontakt warstwy magnetycznej z otoczeniem.

Wydawałoby się, że dyski optyczne i magnetooptyczne zabezpieczone warstwą ochronną powinny być odporne na większość opisanych zagrożeń. Warstwa ta jest jednak niezwykle cienka i nawet nieuważne umieszczenie nośnika w czytniku może doprowadzić do powstania rys uniemożliwiających odczyt danych. Na trwałość nośników optycznych i magnetooptycznych wpływ mają również procesy korozyjne zachodzące w warstwach metalizowanych. Łączenie warstw plastiku i metalu, które mają różne współczynniki rozszerzalności cieplnej, może doprowadzić także do termicznego odkształcenia dysku. Producenci nośników optycznych przeprowadzają doświadczenia z przechowywaniem płyt w ekstremalnych warunkach, ekstrapolując ich wyniki na dłuższy czas. Ponieważ jednak najstarsze tego typu produkty funkcjonują na rynku od zaledwie dwudziestu kilku lat, trudno wyniki te zweryfikować[81].

Od stosowania współczynnika MTBF producenci twardych dysków zaczynają odchodzić, ponieważ awarie są zależne nie tylko od środowiska, w jakim pracują. Twardy dysk, oprócz magnetycznego nośnika danych, który od środowiska jest oddzielony hermetyczną obudową, zawiera również mechanizmy odczytu i zapisu. Mechanizmy te są zarówno elektroniczne, jak

[80] M. Łukaj, *Fleszowa wieża Babel*, „CHIP" 2004, nr 8.

[81] K. Daszkiewicz, A. Arnold, R. Vogt, *Jak archiwizować dane na lata*, „PC World" 2009, nr 11.

i mechaniczne. Trwałość zależy więc także od liczby przepracowanych godzin. Uwzględnia to współczynnik AFR (ang. *Annual Failure Rate*). Jest to procentowo określone prawdopodobieństwo wystąpienia awarii w ciągu roku. Wyliczony jest na podstawie liczby awarii w ciągu miesiąca i pomnożony przez 12. Typowa wartość AFR to 0,9%.

Zależność pomiędzy MTBF a AFR określa następujący wzór:

$$AFR = \frac{1}{MTBF} \times POH \times 100$$

gdzie POH (ang. *Power-On Hours*) jest liczbą godzin pracy w miesiącu[82].

Wybór odpowiedniego nośnika nie zawsze determinuje dobór właściwego urządzenia. Często *backup* wykonywany jest na nośnikach i to poza godzinami pracy. Stąd powstało wiele urządzeń zapewniających automatyzacje wykonywania operacji *backupu*. Możemy wyróżnić następujące ich rodzaje:

- napędy taśmowe,
- zmieniacze taśmowe,
- biblioteki nośników (taśmowe, optyczne lub magnetooptyczne),
- macierze dyskowe,
- NAS,
- wirtualne biblioteki taśmowe.

Napęd taśmowy (ang. *Streamer*) to urządzenia zapisujące i odczytujące dane na taśmie magnetycznej. Zapisywane dane są kompresowane, zwykle ze współczynnikiem kompresji 2:1, wraz z informacjami nadmiarowymi zapewniającymi korekcję błędów.

Zmieniacz taśmowy (ang. *Autoloader*) to napęd taśmowy wraz z magazynkiem taśm i mechanizmem ich zmieniania. Pozwala na zautomatyzowanie procesu wykonywania *backupu*. Stosowany jest najczęściej, gdy wielkość danych przekracza pojemność pojedynczej taśmy. Charakteryzuje się dużym transferem, ale także długim czasem dostępu.

Biblioteka nośników (ang. *Juke-box*) zawiera przynajmniej jeden napęd nośników oraz przynajmniej jeden magazynek nośników. W przeciwieństwie do zmieniacza taśmowego jest to zestaw nadający się do rozbudowy, który można uzupełniać o dodatkowe napędy i magazynki. Posiada też zaawansowane mechanizmy wyszukiwania danych.

[82] C. Vilsbeck, *Twarde dyski IDE, a praca ciągła*, „PC World" 2003, wyd. specjalne *Sprzęt – podzespoły*.

Macierz dyskowa (ang. *Disk array*, *disk matrix*) to zestaw dysków twardych umieszczonych we wspólnej obudowie. Macierze dyskowe mają zaimplementowane mechanizmy zabezpieczające dane przed zniszczeniem w przypadku awarii jednego z dysków i/ lub przyśpieszającego odczyt i zapis danych w stosunku do zapisu i odczytu dokonywanego na pojedynczym dysku.

NAS (ang. *Network Attached Storage*) jest urządzeniem, jak również nazwą technologii umożliwiającej podłączenie pamięci bezpośrednio do sieci komputerowej. Pozwala na zautomatyzowanie procesu *backupu*. Częściej używane jest jednak do replikacji danych lub jako archiwum danych rzadziej wykorzystywanych.

Wirtualna biblioteka taśmowa (ang. V*irtual tape library*) jest rozwiązaniem programowym oraz sprzętowym pozwalającym symulować bibliotekę taśmową, wykorzystując w rzeczywistości macierz dyskową. Technologia ta operuje na zaimplementowanych już w systemie rozwiązaniach związanych z *backupem* na taśmach magnetycznych, jednocześnie zmniejsza czas dostępu do danych dzięki magazynowaniu ich na dyskach twardych.

Problem wyboru nośników i napędów jest zupełnie nieistotny przy usłudze *online-backup*. Polega ona na dzierżawieniu przestrzeni dyskowej i oprogramowania automatyzującego proces. Zapewnia także synchronizację danych, szyfrowanie oraz nadawanie praw dostępu. Jest alternatywą dla przedsiębiorstw, które nie mogą sobie pozwolić ze względów ekonomicznych czy organizacyjnych na utrzymywanie własnej infrastruktury.

Należy zwrócić uwagę na różnice pomiędzy *backupem online*, a popularnymi dyskami internetowymi, tzw. e-dyskami. E-dyski zazwyczaj nie mają zaimplementowanego szyfrowania danych ani automatyzacji *backupu*. Nie gwarantują także ciągłego dostępu do danych.

Dobór odpowiednich nośników oraz obsługującego ich sprzętu należy uzupełnić o właściwe procedury określające typy oraz strategie *backupu*. Mogą one być różne dla poszczególnych zakresów danych. Wyróżniamy cztery typy *backupów*:

- pełny,
- przyrostowy,
- różnicowy,

- delta[83].

Backup pełny (ang. *Full backup*) polega na całościowym zarchiwizowaniu danych. Choć jest najłatwiejszy w wykonaniu oraz pozwala na bardzo szybkie wyszukanie danych lub odtworzenie systemu, to jednocześnie zajmuje najwięcej przestrzeni na nośnikach danych. Wykonywany jest najczęściej jednorazowo, zaraz po uruchomieniu systemu lub okazjonalnie, np. przed przeprowadzeniem operacji o krytycznym znaczeniu.

Backup przyrostowy (ang. *Incremental backup*) archiwizuje jedynie pliki, które powstały lub uległy modyfikacji od czasu wykonania ostatniego *backupu*. Krótki czas wykonywania oraz oszczędniejsze podejście do wykorzystania nośników danych okupione jest dłuższym czasem wyszukiwania danych lub czasem odtwarzania systemu. Do przeprowadzenia tych operacji wymagane jest użycie nośnika z *backupem* pełnym oraz wszystkich następnych.

Backup różnicowy (ang. *Differential backup*) archiwizuje pliki utworzone lub zmienione po ostatnim *backupie* pełnym. Do odzyskania zarchiwizowanych danych wymagany jest zatem nośnik z ostatnim pełnym *backupem* oraz ostatni z *backupem* różnicowym. Charakteryzuje się oszczędniejszym wykorzystaniem nośników w stosunku do *backupów* pełnych, lecz znacznie większym niż w *backupie* przyrostowym. Sprawniej przebiega jednak proces wyszukiwania i odtwarzania niż w *backupie* przyrostowym.

Backup typu delta (ang. *Delta backup*) jest właściwie podtypem *backupu* różnicowego lub przyrostowego. Archiwizowane są nie całe modyfikowane pliki, a jedynie ich fragmenty. Wady i zalety poszczególnych typów kopii zapasowych pokazano w tabeli 6.

Tabela 6. Wady i zalety różnych typów kopii zapasowych

Typ *backupu*	Czas wykonywania	Czas odtwarzania	Wykorzystanie nośników
Backup pełny	Długi	Krótki	Duże
Backup przyrostowy	Krótki	Długi	Małe
Backup różnicowy	Średni	Średni	Średnie

Źródło: opracowanie własne.

[83] W.C. Preston, *Archiwizacja i odzyskiwanie danych*, Helion, Gliwice 2008.

Strategie *backupu* określają odpowiednią rotację nośników, która pozwala na efektywne nimi zarządzanie, tak aby nie uległy nadmiernemu zużyciu. Należy pamiętać, że nie zawsze jesteśmy w stanie uzyskać natychmiastową informację o uszkodzeniu danych. Czasem zachodzi konieczność odzyskania stanu informacji sprzed tygodnia, miesiąca lub kwartału. Dlatego też odpowiednio dobrana rotacja powinna zapewnić odtworzenie nie tylko najświeższych danych, ale też danych z okresów wcześniejszych[84].

Najczęściej stosowana jest rotacja typu Dziadek-Ojciec-Syn – G/F/S (ang. *Grandfather*/*Father*/*Son*). Cykl trwa jeden rok i wymaga 19 nośników. Pozwala odzyskać zapisane dane z każdego dnia poprzedniego tygodnia oraz na ostatni dzień 4 poprzednich tygodni, a także ostatni dzień miesiąca w roku.

Wieża Hanoi (ang. *Towers of Hanoi*) to mało popularna strategia, ze względu na trudną implementację. Stosunkowo nieliczne oprogramowanie wspomaga ten proces. Pozwala jednak najefektywniej wykorzystywać nośniki oraz elastycznie określać długość cyklu, co zostało zaprezentowane w tabeli 7.

Tabela 7. Schemat rotacji wieża Hanoi z 5 nośnikami

	Dzień															
Nośnik	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	A		A		A		A		A		A		A		A	
		B				B				B				B		
				C								C				
								D								
																E

Źródło: opracowanie własne.

Strategia wieży Hanoi zakłada użycie pierwszego nośnika nazwanego „A" w dwudniowym cyklu, zaś każdego następnego w dwukrotnie dłuższym cyklu. Tak więc nośnik „B" będzie używany co 4 dni, nośnik „C" co 8 itd.

Długość całego cyklu określa wzór:

[84] K. Jakubik, *Jak przechowywać więcej za mniej*, „Computerworld" 2008, nr 5.

$$L = 2^{N-1}$$

gdzie:

L – długość cyklu w dniach,

N – liczba nośników.

7.2. Identyfikacja, uwierzytelnianie i autoryzacja

Identyfikacja, uwierzytelnianie i autoryzacja to elementy systemu bezpieczeństwa informacji, z którymi najczęściej spotyka się przeciętny użytkownik. Pomimo wielu technik oraz procedur mających na celu narzucenie im reguł postępowania, nadal stanowią najczęstsze źródło nadużyć. Nie znaczy to, że nie należy poszukiwać rozwiązań, które pozwolą na satysfakcjonujący kompromis pomiędzy wygodą użytkowników, a zapewnieniem bezpieczeństwa systemu.

W celu ochrony systemów informatycznych przed niebezpieczeństwem związanym z dostępem osób niepowołanych, stosowane są techniki:

- identyfikacji (ang. *Identification*),
- uwierzytelniania (ang. *Authentication*),
- autoryzacji (ang. *Authorization*).

Identyfikacja, zwana także autentykacją, to proces umożliwiający rozpoznanie użytkownika w systemie. Uwierzytelnianie pozwala na weryfikację tożsamości użytkownika z danymi zawartymi w systemie. Ma to na celu przyznanie mu odpowiednich uprawnień, czyli autoryzację.

Schemat uwierzytelniania przedstawiono na rysunku 10.

Podstawowe kategorie informacji uwierzytelniającej to:

- „Coś, o czym wiesz" (ang. *Something you know*),
- „Kim jesteś" (ang. *Something you are*),
- „Coś, co posiadasz" (ang. *Something you have*)[85].

Kategoria „Coś, o czym wiesz" obejmuje przede wszystkim zestaw składający się z nazwy użytkownika (ang. *Login* lub *User name*) oraz odpowiadającego mu hasła (ang. *Password*). W stosunku do nazwy użytkownika nie ma żadnych rygorystycznych wymagań oprócz unikalności. Często jednak administratorzy – dla wygody – konstruują je w taki sposób, aby pozwalały na wstępne rozpoznanie użytkownika. Przy tworzeniu i użytkowaniu haseł należy kierować się następującą zasadą: hasło powinno być długie, co najmniej

[85] M. Bieńkowski, *Odcisk palca zamiast hasła*, „IT w administracji" 2009, nr 4.

ośmioznakowe, o dużym stopniu skomplikowania oraz nie mieć znaczenia w żadnym języku. Powinno składać się co najmniej z 3 spośród 4 grup znaków – litery wielkie, litery małe, cyfry oraz znaki specjalne.

Rys. 10. Schematy uwierzytelniania

Źródło: opracowanie firmy Symantec Corporation, 2010.

Skomplikowane hasła są jednak trudne do zapamiętania przez użytkowników systemu. Konieczność ich okresowej zmiany dodatkowo prowokuje do czynności naruszających bezpieczeństwo, takich jak zapisywanie.

Hasła najczęściej łamane są metodą słownikową lub dzięki tzw. *brute force*. Obie metody polegają na sprawdzaniu kolejnych haseł, przy czym metoda słownikowa pobiera je ze zdefiniowanych słowników, zaś *brute force* generuje je poprzez kombinacje wszystkich dostępnych znaków. Choć są one nieoptymalne, to zarazem najbardziej skuteczne[86].

Najsłabszym ogniwem tego typu uwierzytelniania jest więc człowiek. Jego ograniczona pamięć, dążenie do wygody oraz podatność na hakerskie metody socjotechniczne powodują, że staje się on potencjalnym źródłem informacji o sposobie dostępu do systemu.

Rozwój technologiczny pozwolił na identyfikację i autoryzację przy pomocy technik biometrycznych. Należą one do kategorii „Kim jesteś" i opierają się na pomiarach unikatowych cech organizmów żywych. Pierwsze naukowe podejście do tematu zaprezentował w roku 1879 francuski urzędnik, Alphonse Bertillon. Opracował metodę identyfikacji przestępców na podstawie pomiarów kilkunastu cech, takich jak wzrost, obwód głowy, długość palców itp.[87].

Najbardziej znane techniki biometryczne oparte są na pomiarach:

- odcisku palca,
- siatkówki oka,
- tęczówki oka,
- charakterystycznych cech głosu,
- geometrii twarzy,
- wzorców żył,
- DNA[88].

Przy doborze technologii biometrycznej należy zwrócić uwagę na następujące wskaźniki: wskaźnik[89] FRR (ang. *False rejection rate*) – współczynnik fałszywych odrzuceń zwanych błędami typu pierwszego (*Type I*), czyli procentowy współczynnik błędnych odrzuceń prawidłowych prób zalogowania, jak również FAR (ang. *False acceptance rate*) – współczynnik fałszywych akceptacji zwanych błędami typu drugiego (*Type II*), czyli procentowy

[86] P. Jaroszewski, *Dobre praktyki: Hasło*, CERT Polska 02/2005.

[87] T. Witczak, *Początki identyfikacji*, „Detektyw" 2007, nr 3, wydanie specjalne.

[88] D. Gutkowska, L. Stolc, *Techniki identyfikacji osób z wykorzystaniem indywidualnych cech biometrycznych*, Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej, nr 20, Gdańsk 2004.

[89] E. Cole, R.L. Krutz, J. Conley, *Bezpieczeństwo sieci. Biblia*, Helion, Gliwice 2005.

współczynnik błędnych akceptacji nieprawidłowych prób logowania. Istotny jest też CER (ang. *Crossover error rate*) – skrzyżowany współczynnik błędu, czyli procent przypadków, w których FRR jest równy FAR. Skala wspomnianych wskaźników dla poszczególnych technologii biometrycznych została pokazana w tabeli 8.

Tabela 8. Zestawienie porównawcze wybranych technologii biometrycznych

Cecha biometryczna	Przyczyny błędów	FAR	FRR	Poziom bezpieczeństwa	Stabilność w czasie
Odcisk palca	Uszkodzenia skóry, wiek użytkownika	Mały	Mały	Duży	Średnia
Twarz	Uszkodzenia, wiek, zarost, fryzura, mimika, oświetlenie	Mały	Duży	Mały	Mała
Tęczówka	Oświetlenie	Mały	Mały	Duży	Duża
Głos	Wiek, choroby, tło dźwiękowe	Średni	Duży	Mały	Mała

Źródło: P. Niedziejko, I. Krysowaty, *Biometria. Charakterystyka danych człowieka i ich wykorzystanie w bezpieczeństwie*, „Zabezpieczenia" 2007, nr 1.

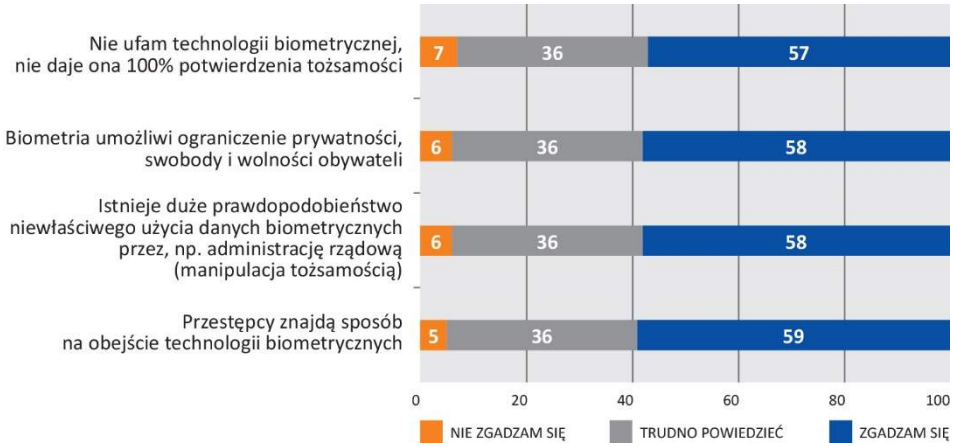
Przed podjęciem decyzji o wdrażaniu technologii biometrycznej należy uwzględnić niejasności prawne, których efektem są liczne spory prowadzone pomiędzy przedsiębiorcami a Generalnym Inspektorem Ochrony Danych Osobowych (GIODO). Przykładowo, 28 lutego 2008 roku GIODO wydał decyzję[90], nakazującą usunięcie danych osobowych obejmujących przetworzone do postaci cyfrowej informacje o charakterystycznych punktach linii papilarnych palców pracowników pewnej spółki oraz zaprzestanie zbierania tego typu danych. Podtrzymał ją 24 kwietnia tego samego roku, pomimo że spółka wykazała, iż wszyscy pracownicy, od których pobrano linie papilarne, wyrazili na to zgodę, wskazując ściśle, w jakim zakresie godzą się na przetwarzanie danych[91].

[90] Decyzja GIODO z 28 lutego 2008 r., DIS/DEC-134/4605/08 GIODO 28.02.2008.
[91] Decyzja GIODO z 24 kwietnia 2008 r., DIS/DEC-254/10616/08 GIODO 24.04.2008.

Naczelny Sąd Administracyjny w wyroku z 1 grudnia 2009 roku o sygn. akt I OSK 249/09 w sprawie Spółka LG Electronics z Mławy vs. GIODO, orzekał, że wykorzystanie danych biometrycznych w postaci linii papilarnych pracownika w systemie elektronicznego rozliczania czasu pracy nie stanowi wykroczenia przeciw obowiązującym przepisom prawnym, jeśli pracownik wyrazi na to zgodę[92].

O dobrowolną zgodę pracowników może być jednak niezmiernie trudno, o czym świadczą badania przeprowadzone przez Instytut Inżynierii Systemów Bezpieczeństwa w roku 2007. Potwierdziły one postawioną tezę, że istnieje duża obawa społeczna co do ograniczenia swobód poprzez wprowadzenie biometrycznych systemów kontroli tożsamości[93].

Poziom zaufania do technologii biometrycznych został pokazany na rysunku 11.



Rys. 11. Poziom zaufania do technologii biometrycznych

Źródło: A. Krysowaty, I. Krysowaty, P. Niedziejko, *Nie bójmy się biometrii!*, „Zabezpieczenia" 2007, nr. 6.

Techniki behawioralne różnią się od technik wykorzystujących cechy anatomii tym, że nie mierzą cech wrodzonych, a wyuczone sposoby zachowania. Weryfikacja tożsamości oparta na badaniu dynamiki podpisu odręcznego

[92] Wyrok Naczelnego Sądu Administracyjnego w Warszawie z 1 grudnia 2009 r., I OSK 249/09.
[93] A. Krysowaty, I. Krysowaty, P. Nadziejko, *Biometria w systemie bezpieczeństwa człowieka – metoda czy konieczność*, Instytut Inżynierii Systemów Bezpieczeństwa, Warszawa 2007.

jest najbardziej naturalną, przez co także i akceptowalną metodą identyfikacji lub weryfikacji. Cyfrowa reprezentacja podpisu zawiera zarówno charakterystykę wizualną, jak i dynamikę ruchu pióra, siłę nacisku, kąt elewacji i azymutu oraz nachylenie. Liczba dodatkowo pobieranych parametrów jest uzależniona od urządzenia służącego do składania podpisu (tablet graficzny), jak również algorytmu. Najbardziej zaawansowany algorytm Muramatsu łączy podejście statystyczne oraz dynamiczne, cechuje się niskimi współczynnikami FAR 0,86%, FRR 0,8% i ERR 0,86%[94].

Podejście statyczne to analiza graficzna zeskanowanych podpisów. Zastosowana przez Giovanniego Dimauro i współpracowników polega na wyodrębnieniu cech charakterystycznych obrazu po uniezależnieniu od skali i orientacji oraz podziale na części[95]. Podejście dynamiczne zajmuje się czasową analizą składników podpisu w czasie. Przykładem jest algorytm opracowany przez Thomasa Wesselsa i Christiana Omlina, wykorzystujący pięciowymiarowe obserwacje Markowa[96].

Opisane wcześniej techniki wymagają odpowiednich urządzeń, od jakości których uzależniony jest stopień bezpieczeństwa systemu. Stąd metoda bazująca na dynamice pisania na klawiaturze oraz ruchu myszy jest atrakcyjną alternatywą. Wykorzystuje się w nich klasyfikatory regułowe lub sztuczną inteligencję opartą na sieciach neuronowych, które pozwalają na stworzenie profilu osoby piszącej lub używającej myszy na podstawie analizy odstępów pomiędzy przyciskaniem poszczególnych klawiszy, rytmu pisania na klawiaturze czy prędkości ruchu kursora myszy lub nieskoordynowanych, a charakterystycznych jego ruchów.

Metoda jest tym bardziej skuteczna, im więcej zarejestrowanych jest próbek, co z kolei angażuje sporą moc obliczeniową potrzebną do utworzenia wzorca. Osiągane wskaźniki błędów są zadowalające (FAR 1,8%, FRR 3%) i dają podstawy do dalszych prac. Zazwyczaj badanie dynamiki pisania na

[94] A. Czajka, A. Pacut, *Biometria podpisu odręcznego*, w: *Automatyczna identyfikacja w systemach logistycznych*, (red.) P. Zając, S. Kwaśniowski, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2004.

[95] G. Dimauro, S. Impedevo, G. Pirlo, A. Salzo, *A Multi-Expert Signature Verification System for Bankcheck Processing*, "International Journal of Pattern Recognition and Artificial Intelligence" 1996/97, Vol. 11, Iss. 2.

[96] T. Wessels, C. Omlin, *A hybrid system for signature verification*, Neural Networks, 2000. IJCNN 2000, Proceedings of the IEEE-INNS-ENNS International Joint Conference, Vol. 5.

klawiaturze stosowane jest najczęściej w połączeniu z uwierzytelnianiem na podstawie haseł. Badana jest wtedy nie tylko zgodność hasła, ale też sposób jego wprowadzania. Ogranicza to w istotny sposób liczbę próbek potrzebnych do wygenerowania wzorca[97].

Token (pol. *symbol, znacznik lub żeton*) jest urządzeniem kryptograficznym generującym jednorazowe hasła. Z tego też względu w literaturze spotyka się także nazwę Token OTP (ang. *One Time Password*). Działanie tokena opiera się na algorytmach oraz kluczach kryptograficznych. Generuje on ciąg cyfr przy użyciu prywatnego klucza, bazując na czasie lub wprowadzonym wcześniej ciągu cyfr stanowiących hasło. System uwierzytelniający na podstawie kluczy i wygenerowanego przez token ciągu, identyfikuje i uwierzytelnia użytkownika[98].

Tokeny występują w wersji sprzętowej oraz programowej. Tokeny programowe (ang. *Soft-token*), inaczej zwane wirtualnymi, posiadają taką samą funkcjonalność, jak sprzętowe. Emulują praktycznie działanie sprzętu, są jednak znacznie mniej bezpieczne, gdyż ich kradzież może pozostać nieujawniona. Bezpieczeństwo wirtualnego tokena jest tak silne, jak silna jest ochrona komputera, na którym został zainstalowany. Dlatego też są rzadko stosowane[99].

Współczesne systemy identyfikacji oparte są na kartach mikroprocesorowych, które cechuje możliwość weryfikacji dostępu do ich pamięci poprzez numer PIN (ang. *Personal Identification Number*) oraz zastosowanie silnych algorytmów kryptograficznych. Oprogramowanie kart mikroprocesorowych tworzone jest w specjalnej implementacji języka JAVA, tzw. JAVA CARD. W pamięci karty umieszczona jest także maszyna wirtualna, obsługującą napisane w niej oprogramowanie[100].

Komunikację pomiędzy kartami a systemami uwierzytelniania zapewniają odpowiednie czytniki. Ze względu na sposób przesyłania danych wyróżnić można karty stykowe, przy których zachodzi konieczność umieszczenia karty w urządzeniu oraz karty bezstykowe, przesyłające informacje

[97] T. Długosz, P. Wujczyk, *Behawioralne metody biometryczne – dynamika pisania na klawiaturze*, „Wiadomości Telekomunikacyjne" 2009, nr 10.

[98] S. Bakalarczyk, *Innowacje bankowe: bankowość elektroniczna, bankowość inwestycyjna i inżynieria finansowa*, Wydawnictwo Politechniki Łódzkiej, Łódź 2006.

[99] B. Królikowski, *Silne uwierzytelnianie z użyciem tokenów kryptograficznych*, „Networld" 2008, nr 9.

[100] M. Kubas, M. Molski, *Karta elektroniczna. Bezpieczny nośnik informacji*, Mikom, Warszawa 2002.

drogą radiową. Kluczowym problemem związanym z kartami procesorowymi jest ich strona sprzętowa. Zachodzi potrzeba ujednolicenia sposobu działania kart i czytników. Głównym standardem jest norma ISO 7816, opisująca właściwości fizyczne i charakterystyki komunikacyjne stosowanych układów. Jest na tyle ogólna, iż większość producentów ją akceptuje[101].

Infrastruktura klucza publicznego, w skrócie PKI (ang. *Public Key Infrastructure*), jest najbardziej kompleksowym rozwiązaniem problemów związanych z bezpieczeństwem sieci. Polega na szyfrowaniu asymetrycznym oraz kluczach kryptograficznych, wydawanych przez zaufaną, trzecią stronę, którą jest Główny Urząd Certyfikacji (ang. *Root Certification Authority*). Kluczem o najwyższym poziomie zaufania jest w Polsce tzw. certyfikat kwalifikowany, wydawany przez podmioty świadczące usługi certyfikacyjne, zarejestrowane w Rejestrze podmiotów kwalifikowanych, prowadzonym przez Narodowe Centrum Certyfikacji. W tabeli 9 pokazano zawartość tego rejestru. Podmioty wpisane pod nr 4, 7 i 8 zaprzestały już działalności związanej z usługami certyfikacyjnymi.

Tabela 9. Wpisy Rejestru podmiotów kwalifikowanych Narodowego Centrum Certyfikacji

Nr wpisu	Nazwa podmiotu	Rodzaj świadczonych usług	Czas dokonania wpisu
1.	UNIZETO TECHNOLOGIES SA	Wydawanie kwalifikowanych certyfikatów	31 grudnia 2002 r., godz. 12:00:00
		Wydawanie kwalifikowanych certyfikatów atrybutów	13 września 2007 r., godz. 10:00:00
2.	UNIZETO TECHNOLOGIES SA	Znakowanie czasem	24 stycznia 2003 r., godz. 12:00:00
		Weryfikowanie statusu certyfikatów w trybie *on-line*	17 października 2006 r., godz. 12:00:00
		Walidacja danych	17 października 2006 r., godz. 12:00:00
		Poświadczenie odbioru i przedłożenia	17 października 2006 r., godz. 12:00:00
		Poświadczenie depozytowe	5 stycznia 2007 r., godz. 10:00:00
		Poświadczenie rejestrowe i repozytoryjne	5 stycznia 2007 r., godz. 10:00:00

[101] P. Leszek, *Smart cards – krzemowa inteligencja*, „Chip", wyd. specjalne *Security*, 2003.

3.	POLSKA WYTWÓRNIA PAPIERÓW WARTOŚCIOWYCH SA	Wydawanie kwalifikowanych certyfikatów	14 lutego 2003 r., godz. 15:00:00
4.	TP INTERNET Sp z o.o.	Wydawanie kwalifikowanych certyfikatów	14 lutego 2003 r., godz. 15:30:00
5.	POLSKA WYTWÓRNIA PAPIERÓW WARTOŚCIOWYCH SA	Znakowanie czasem	14 marca 2003 r., godz. 15:00:00
6.	KRAJOWA IZBA ROZLICZENIOWA SA	Wydawanie kwalifikowanych certyfikatów	21 marca 2003 r., godz. 13:00:00
		Znakowanie czasem	13 września 2005 r., godz. 1:16:00
7.	TP INTERNET Sp. z o.o.	Znakowanie czasem	17 sierpnia 2004 r., godz. 13:30:00
8.	MOBICERT Sp. z o.o.	Wydawanie kwalifikowanych certyfikatów	21 września 2009 r., godz. 11:30:00
9.	SAFE TECHNOLOGIES SA	Wydawanie kwalifikowanych certyfikatów	21 września 2009 r., godz. 11:30:00
10.	SAFE TECHNOLOGIES SA	Poświadczanie ważności certyfikatów	21 września 2009 r., godz. 11:30:00
		Znakowanie czasem	21 września 2009 r., godz. 11:30:00
11.	ENIGMA SOI Sp z o.o.	Wydawanie kwalifikowanych certyfikatów	04 kwietnia 2011 r., godz. 15:30:00
12.	ENIGMA SOI Sp z o.o.	Poświadczanie ważności certyfikatów	04 kwietnia 2011 r., godz. 15:30:00
		Znakowanie czasem	04 kwietnia 2011 r., godz. 15:30:00
13.	EUROCERT Sp z o.o.	Wydawanie kwalifikowanych certyfikatów	30 grudnia 2013 r., godz. 15:30:00

Źródło: Rejestr podmiotów kwalifikowanych NCC 2015, http://www.nccert.pl/podmioty.htm.

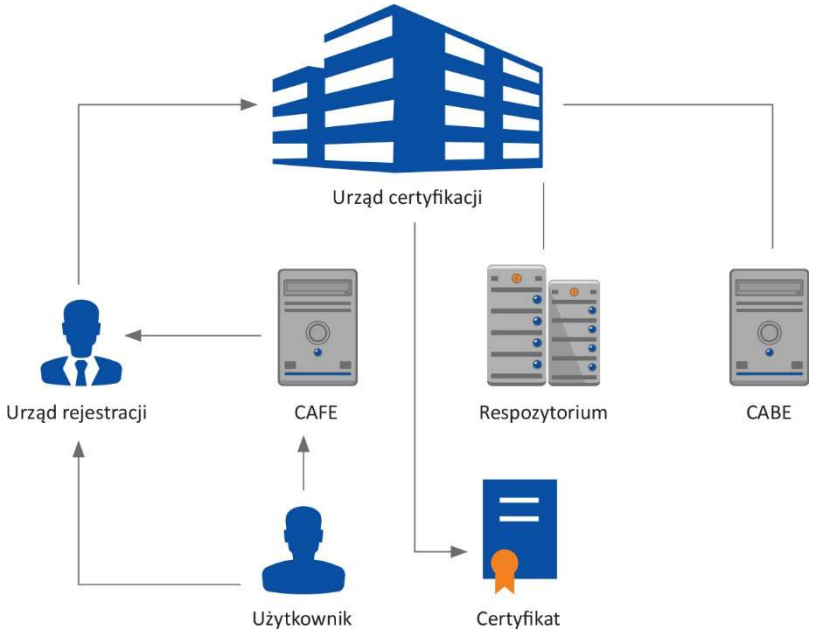
Głównemu Urzędowi Certyfikacji podlegają pośrednie urzędy certyfikacji, wydające certyfikaty użytkownikom końcowym, których tożsamość jest weryfikowana przez urząd rejestracji (ang. *Registration authority*). Certyfikaty te, a właściwie ich część publiczna, umieszczone są w repozytorium oraz publikowane na stronach internetowych danych instytucji lub poprzez usługę katalogową LDAP (ang. *Lightweight Directory Access Protocol*). Pozwala to na weryfikację każdemu zainteresowanemu tożsamości osoby korzystającej z danego certyfikatu[102].

[102] C. Adams, S. Lloyd, *PKI. Podstawy i zasady działania. Koncepcje, standardy i wdrażanie infrastruktury kluczy publicznych*, WN PWN, Warszawa 2007.

Uzyskanie certyfikatu, zaprezentowane na rysunku 12, rozpoczyna się od wyboru jego rodzaju:

- certyfikatu indywidualnego,
- certyfikatu serwera,
- certyfikatu pośredniego urzędu certyfikacji.

Żądanie wydania certyfikatu składane jest na serwerze dostępowym CAFE (ang. *Certification Authority Front End*), skąd zostaje przesłane do urzędu rejestracji. Weryfikuje on dane zawarte we wniosku ze stanem faktycznym, na podstawie dostarczonych przez użytkownika dokumentów. Urząd certyfikacji, po otrzymaniu zweryfikowanego wniosku, generuje certyfikat przy pomocy bezpiecznej jednostki do generowania certyfikatów CABE (ang. *Certification Authority Back End*), umieszcza go w repozytorium oraz publikuje poprzez CABE[103].



Rys. 12. Proces certyfikacji

Źródło: opracowanie własne.

[103] C. Adams, S. Lloyd, *Podpis elektroniczny klucz publiczny*, ROBOMATIC, Wrocław 2002.

Wygenerowane klucze kryptograficzne mają zastosowanie nie tylko w procesach związanych z uzyskaniem dostępu do zasobów informatycznych. Dzięki nim można ustanowić bezpieczny kanał komunikacyjny pomiędzy parami użytkowników, w którym informacja będzie zaszyfrowana oraz sygnowana elektronicznym podpisem. Podpisem tym mogą być również sygnowane, niezaszyfrowane, ogólnie dostępne dokumenty o postaci cyfrowej, co uwiarygodnia ich autorstwo i może być równoznaczne z opatrzeniem podpisem odręcznym tradycyjnego papierowego dokumentu.

7.3. Techniki kryptograficzne

Kryptologia to według jednych autorów, dział matematyki, według innych samodzielna dziedzina wiedzy. Wszyscy są jednak zgodni, że dotyczy bezpiecznych sposobów przekazywania informacji. Zazwyczaj w kryptologii wyróżnia się kryptografię jako naukę o tworzeniu szyfrów i kryptoanalizę, zajmującą się oceną ich skuteczności.

Pierwsze wzmianki o kryptografii możemy znaleźć już w *Kamasutrze*, która wymieniając 64 umiejętności ważne dla kobiety, wspomina o sztuce sekretnego pisania (*mlecchita-vikalpa*)[104].

Najstarszym znanym sposobem szyfrowania informacji jest kod Juliusza Cezara, którym się posługiwał w korespondencji z Cyceronem. Historycy nie są jednak zgodni co do rzeczywistego autorstwa tego szyfru. Polega on na zastępowaniu poszczególnych znaków alfabetu znakami przesuniętymi co do pozycji w alfabecie o określoną liczbę[105]. Udoskonalony został przez arabskich matematyków, którzy zamiast stałego przesunięcia stosowali tablicę podstawieniową. Szyfry takie zwane są monoalfabetycznymi szyframi podstawieniowymi, gdyż każdemu znakowi alfabetu odpowiada pojedynczy znak alfabetu tajnego.

Zarówno do kodowania, jak i dekodowania zaszyfrowanej informacji, niezbędny jest tzw. klucz. Dla różnych rodzajów szyfrów może on przyjmować inną postać, dlatego też definicja klucza w kryptologii jest dosyć ogólna. Klucz (w kryptologii) to ogół informacji niezbędnych w procesie szyfrowania i deszyfrowania informacji przy użyciu danego szyfru. Kluczem dla

[104] W. Foryś, *W kręgu idei kryptologii*, „Alma Mater – miesięcznik Uniwersytetu Jagiellońskiego" 2005, nr 69.
[105] S. Singh, *Księga Szyfrów*, Wydawnictwo Albatros, Szczecin 2001.

szyfru Cezara jest więc liczba, o którą przesuwany jest znak w alfabecie, a dla jego arabskiej modyfikacji – tablica podstawieniowa.

W szyfrach polialfabetycznych jedna litera alfabetu może być zaszyfrowana na wiele różnych sposobów, co skutecznie utrudnia ich łamanie. Jednym z najbardziej znanych szyfrów polialfabetycznych jest szyfr Vigenèra, dyplomaty w służbie króla Karola IX. Blaise de Vigenèr założył, że każdą literę alfabetu można zaszyfrować na 25 sposobów (liczba liter w alfabecie). Kluczem jest dowolny ciąg liter alfabetu. Do szyfrowania opracował tablicę nazwaną później jego imieniem. Składa się ona z wierszy zawierających kolejne litery alfabetu, przy czym każdy następny wiersz przesunięty jest w lewo o jedną pozycję. Szyfrowanie przy jej użyciu polega na odnajdywaniu litery położonej na przecięciu wiersza rozpoczynającego się od litery tekstu jawnego oraz odpowiadającej jej w kolejności litery klucza. Jeśli długość klucza jest krótsza niż długość tekstu jawnego, ciąg liter klucza zostaje powielony odpowiednią ilość razy.

Jak można zauważyć, odporność na złamanie szyfru wzrasta wraz z długością klucza oraz losowym wyborem liter go tworzących. Podczas I wojny światowej Gilbert Vernam zaproponował, aby stosować klucze o tej samej długości, co szyfrowany tekst jawny[106]. Wszystkie wyliczone teksty jawne, w takim przypadku są równie prawdopodobne.

W latach 40. zeszłego wieku, amerykański matematyk Claude Elwood Shannon udowodnił, że szyfr jest doskonale bezpieczny, jeśli jest tyle możliwych kluczy, co tekstów jawnych, oraz każdy z kluczy jest równie prawdopodobny[107]. Jedynym absolutnie bezpiecznym szyfrem jest więc szyfr z kluczem jednorazowym. Do dnia dzisiejszego szyfry tego typu są używane w dyplomacji, jednak ze względu na uciążliwość ich stosowania mają marginalne znaczenie.

W przeciwieństwie do opisywanych powyżej, szyfry blokowe nie zajmują się kodowaniem pojedynczych znaków alfabetu, lecz ich bloków o określonej długości. Najbardziej znanym, wczesnym szyfrem blokowym, jest szyfr Playfaira, opracowany w roku 1854 przez brytyjskiego wynalazcę, sir Charles'a Wheatstone'a, a spopularyzowany przez barona Lyona Playfaira. Operuje on

[106] M. Karbowski, *Podstawy kryptografii*, Helion, Gliwice 2007.

[107] C.E. Shannon, *Communication Theory of Secrecy Systems*, "The Bell System Technical Journal" 1948, Vol. 27.

na 2-znakowych blokach i wykorzystuje do szyfrowania i deszyfrowania tablicę 5 x 5 zawierającą 25 różnych znaków z alfabetu łacińskiego oraz zakłada zamianę brakującego znaku z alfabetu na inny, występujący w tablicy. Szyfr Playfaira był stosowany podczas obu dwudziestowiecznych wojen światowych przez Brytyjczyków, Amerykanów i Niemców.

W stosunku do szyfrów polialfabetycznych, jest on trudniejszy do złamania, gdyż konieczne jest zbadanie statystyki występowania bloków liter, a nie pojedynczych liter, do czego niezbędna jest większa liczba zaszyfrowanego tekstu[108].

Współcześnie wykorzystywane szyfry blokowe to przede wszystkim:

- DES,
- DESX,
- 3DES,
- AES,
- Blowfish,
- IDEA,
- Serpent.

DES (ang. *Data Encryption Standard*) został stworzony przez firmę IBM, a zmodyfikowany przez amerykańską NSA (*National Security Agency*). W roku 1977 zaakceptowano go jako standard amerykański[109]. Jest krytykowany ze względu na słabości klucza. Istnieje podejrzenie, że NSA umieściło w nim tzw. tylną furtkę (ang. *back door*), pozwalającą na odszyfrowanie danych bez znajomości klucza.

DESX (ang. *Data Encryption Standard XORed*) to najprostsza modyfikacja DES-a. Wykorzystuje klucz o długości 184 bitów. Wydzielane są z niego trzy podklucze, stosowane do operacji XOR, szyfrowania DES i ponownego XOR[110]. DESX jest bardziej bezpieczny niż DES ze względu na zwiększoną długość przy nieznacznym zwiększeniu czasu kodowania. 3DES (ang. *Triple Data Encryption Standard*) trzykrotnie koduje wiadomości DES-em[111].

[108] R. Anderson, *Inżynieria zabezpieczeń*, WNT, Warszawa 2005.

[109] *Announcing the Standard for DATA ENCRYPTION STANDARD (DES)*, Federal Information Processing Standards Publication 46-2 1988, National Institute of Standards and Technology, Gaithersburg 1988.

[110] F.L. Bauer, *Sekrety kryptografii*, Helion, Gliwice 2003.

[111] D.R. Stinson, *Kryptografia w teorii i praktyce*, WNT, Warszawa 2005.

AES (ang. *Advanced Encryption Standard*), znany również jako *Rijndael*, jest następcą DES przyjętym przez National Institute of Standards and Technology, w wyniku rozstrzygnięcia ogłoszonego w roku 1997 konkursu[112]. Wykorzystuje klucze o długościach 128, 196 i 256 bitów i operuje na blokach danych o długości 128 bitów, wykonując 10, 12 lub 14 rund szyfrujących. AES wykazuje się dużą odpornością na większość znanych ataków kryptograficznych, za wyjątkiem ataku XSL[113].

Blowfish jest szyfrem blokowym opracowanym w roku 1993 przez amerykańskiego kryptografa, Bruce'a Schneiera. Operuje na 64-bitowych blokach danych, szyfrując je kluczem o długości od 32 do 448 bitów[114]. Nie istnieją przesłanki o udanych atakach na szyfr Blowfish. Ponieważ jest on dostępny bezpłatnie, stanowi atrakcyjną alternatywę dla innych, komercyjnych rozwiązań.

IDEA (ang. *International Data Encryption Algorithm*) został opracowany w ramach projektu prowadzonego przez ETHZ (*Eidgenössische Technische Hochschule Zürich*) oraz firmę Ascom Systec AG[115]. Algorytm IDEA operuje na 64-bitowych blokach danych i używa 128-bitowego klucza. Na jego podstawie generowanych jest 52 podkluczy. Pierwsze 8 tworzonych jest poprzez podział klucza głównego na osiem 16-bitowych bloków. Kolejne uzyskiwane są w wyniku cyklicznych przesunięć o 25 bitów w lewo i ponownych podziałów[116]. Pomimo zalet, jakie posiada IDEA w stosunku do innych algorytmów, tzn. szybkości działania oraz bezpieczeństwa (nie odnotowano przypadków złamania szyfru), nie zyskał szerokiej aprobaty w świecie biznesu ze względu na koszty związane z opłatami licencyjnymi.

---

[112] R. Wobst, *Kryptologia. Budowa i łamanie zabezpieczeń*, Grupa Wydawnicza READ ME, Warszawa 2002.

[113] N. Courtois, J. Pieprzyk, *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations*, Cryptology ePrint Archive: Report 2002/044. 2002, https://eprint.iacr.org/2002/044.

[114] B. Schneier, *Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)*, Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer-Verlag, 1994, https://www.schneier.com/paper-blowfish-fse.html.

[115] J. Daemen, R. Govaerts, J. Vandewalle, *Weak Keys For IDEA*, w: *Advances in Cryptology – CRYPTO 1993*, Lecture Notes in Computer Science 773, (ed.) D.R. Stinson, Springer-Verlag, Berlin 1994.

[116] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton 1996.

Serpent (pol. *wąż*) to jeden z algorytmów szyfrujących, które znalazły się w finale wspominanego powyżej konkursu ogłoszonego przez National Institute of Standards and Technology. Choć uważany jest za bezpieczny, to duży stopień skomplikowania oraz konieczne do jego zaimplementowania zasoby sprzętowe ograniczają znacznie jego popularyzację. Wykorzystuje klucz o maksymalnej długości 256 bitów. W przypadku mniejszej długości, uzupełniany jest do postaci 256-bitowej liczby i dzielony na osiem 32-bitowych bloków[117].

Wszystkie przedstawione powyżej algorytmy stanowią przykłady szyfrowania symetrycznego (ang. *Symmetric encryption),* w którym ten sam klucz potrzebny jest zarówno w procesie szyfrowania, jak i deszyfrowania.

Ciągle rozwijane algorytmy mają na celu uczynienie ich obliczeniowo-bezpiecznymi[118], czyli takimi, których złamanie przy obecnym stanie techniki jest nieopłacalne. Koszt uwzględniający zasoby sprzętowe, zapewniające odpowiednią moc obliczeniową oraz poświęcony łamaniu czas powinien znacznie przewyższać wartość uzyskiwanych w ten sposób informacji lub przekroczyć czas ich użyteczności. Uzyskiwane jest to poprzez złożoność samych algorytmów, jak i wydłużanie klucza szyfrującego.

Współczesne algorytmy oparte na co najmniej 128-bitowych kluczach zapewniają poufność i integralność danych na bardzo wysokim poziomie, o czym świadczy fakt nacisków NSA na producentów oprogramowania kryptograficznego, aby umieszczali w nim funkcje pozwalające instytucjom rządowym na wgląd do zaszyfrowanych danych[119]. Ze względu na szybkość ich działania stosowane są zazwyczaj do szyfrowania dużych bloków informacji.

Wadami szyfrowania symetrycznego są:

- konieczność wymiany tajnego klucza,
- problem efektu skali,
- komunikacja pomiędzy obcymi jednostkami.

[117] R. Anderson, E. Biham, L. Knudsen, *Serpent: A Flexible Block Cipher With Maximum Assurance*, First AES Candidate Conference (AES1), California 1998.

[118] K. Maćkowiak, *Złam szyfr i odkryj tajemnicę*, „Software 2.0" 2004, nr 9.

[119] *Świat zaszyfrowany, Marcin Bójko rozmawia z wiceprezesem RSA Security*, „Komputer" nr 7, dodatek do „Komputer" 2002, nr 36.

Poza technicznymi aspektami związanymi z zastosowaniem algorytmu symetrycznego, na bezpieczeństwo wymiany informacji duży wpływ ma tajność klucza. Ponieważ opisywany rodzaj szyfrowania wymaga przekazania odbiorcy wiadomości klucza, który jest używany zarówno w procesie szyfrowania, jak i deszyfrowania, istotną rolę ma ustanowienie bezpiecznego kanału łączności. Najbardziej bezpiecznym sposobem byłoby przekazywanie klucza przez nadawcę bezpośrednio odbiorcy. Często jest to jednak niemożliwe lub trudne ze względu na czas i odległość.

Efekt skali występuje, gdy jest wielu uczestników procesu komunikacji. Każda ich para potrzebuje klucza na wyłączność. Liczba niezbędnych kluczy rośnie więc w postępie geometrycznym i wynosi $\frac{n*(n-1)}{2}$, gdzie n oznacza liczbę uczestników[120].

Problem komunikacji pomiędzy obcymi sobie jednostkami jest bezpośrednio związany z koniecznością ustalenia bezpiecznego kanału informacji i ma wpływ na dwa ważne zadania stawiane kryptografii, tzn. uwierzytelnianie i niezaprzeczalność. Ustalenie kanału wymiany informacji pomiędzy osobami, które się nie znają, a nawet mogą nie wiedzieć o swoim istnieniu, jest w praktyce niemożliwe, co powoduje niemożność rozszyfrowania.

W roku 1976 opublikowana została przełomowa praca Martina Hellmana i Whitfielda Diffiego, obalająca tezę, iż wymiana klucza poprzez kanał publiczny jest niemożliwa. Zaproponowali oni stosowanie pary powiązanych ze sobą kluczy – publicznego i prywatnego[121]. Klucz publiczny, służący do szyfrowania wiadomości, może być swobodnie rozpowszechniany, zaś klucz prywatny, używany do deszyfrowania, musi pozostawać tajny. Zaprezentowali również protokół uzgadniania kluczy, zwany protokołem Diffiego-Hellmana. Polega on na wykonaniu odpowiednich działań matematycznych na względnie dużych liczbach pierwszych, w wyniku których dwie strony otrzymują taką samą liczbę. Liczba ta nie jest możliwa do otrzymania na podstawie treści wiadomości wymienionych między stronami i może być używana jako klucz szyfrujący.

Kryptografia asymetryczna znana była jednakże już wcześniej, za sprawą Jamesa H. Ellisa z brytyjskiej agencji wywiadowczej GCHQ (ang. *Government*

[120] A. Sikora, *Przegląd zagadnień kryptografii*, „PC World", wyd. specjalne *Security*, 2003.
[121] W. Diffie, M.E. Hellman, *New Directions in Cryptography*, "IEEE Transactions on Information Theory" 1976, Vol. IT-22, No. 6.

Communications Headquarters), a algorytm Diffiego-Hellmana opracował wcześniej Malcolm Williamson[122].

W roku 1978 Ronald Rivest, Adi Shamir i Leonard Adleman opracowali alternatywny system asymetryczny, nazwany od pierwszych liter nazwisk twórców – RSA[123]. Prawa do tego algorytmu posiada firma RSA Security Inc. Siła RSA wynika z trudności rozbicia dużych liczb na czynniki pierwsze. Wysoki poziom bezpieczeństwa zapewniają klucze o długości 2048 bitów, które najczęściej stosowane są obecnie w praktyce. Wadą algorytmu RSA jest jego wolne działanie.

Drugim co do popularności systemem kryptografii asymetrycznej jest algorytm ElGamal, opracowany w latach 80. XX wieku przez Tahere ElGamala. Oparty jest na trudności problemu logarytmu dyskretnego w ciele liczb całkowitych[124].

Coraz większą popularność zdobywa technika kryptografii asymetrycznej, zwana kryptografią krzywych eliptycznych ECC (ang. *Elliptic Curve Cryptography*). Bezpieczeństwo ECC jest oparte na złożoności obliczeniowej dyskretnych logarytmów na krzywych eliptycznych *ECDLP (ang. Elliptic Curve Discrete Logarithm Problem)*[125]. Algorytmy ECC oferują porównywalne bezpieczeństwo co RSA przy mniej złożonych kluczach. Klucz ECC o długości 160 bitów jest równie bezpieczny jak 1024-bitowy RSA. Zapewnia to znacznie wydajniejsze szyfrowanie w stosunku do RSA, który jest uważany za wolny i wymagający sporych mocy obliczeniowych.

7.4. Zasilanie awaryjne

W literaturze można się natknąć na bardzo zróżnicowane dane na temat rozkładu przyczyn utraty danych i awarii systemów informatycznych. Określają one, że awarie zasilania mają od 4% do 40% udziału w ogólnej liczbie

[122] *NSA Releases Top Secret Crypto Papers*, Cryptome, 3 marca 2007, http://cryptome.org/nsa-nse/nsa-nse-01.htm.

[123] R. Rivest, A. Shamir, L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, "Communications of the ACM" 1978, Vol. 21, No. 2.

[124] T. ElGamal, *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, "IEEE Transactions on Information Theory" 1985, Vol. IT-31, No. 4.

[125] *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, ANSI X9.62 Standard, American National Standards Institute, New York 1998.

awarii. Tak duża rozbieżność wyników badań przeprowadzanych w stosunkowo krótkim odstępie czasu (2000-2004) wzbudza określone wątpliwości. Badania te przeprowadzane były w krajach bardziej uprzemysłowionych niż Polska, trudno więc odnieść je do naszego kraju. Nie można jednak zaprzeczyć, że problem istnieje i nie należy go bagatelizować.

Podstawowym warunkiem poprawnej pracy każdego systemu informatycznego jest ciągłe i stabilne zasilanie wszystkich urządzeń wchodzących w jego skład. Tymczasem, jak prognozuje Ernst & Young Polska, w najbliższych latach wskutek braku remontów i inwestycji w energetyce czekają nas przerwy w dostawach energii elektrycznej[126]. Zazwyczaj przedsiębiorstwo ma dość marginalny wpływ na dostawy energii elektrycznej, ale może się zabezpieczyć przed przerwami i awariami zasilania.

Podstawowymi urządzeniami, które podnoszą bezpieczeństwo energetyczne, są zasilacze awaryjne UPS (ang. *Uninterruptable Power Supply*). Możemy wyróżnić trzy podstawowe ich typy:

- zasilacze awaryjne *off-line*,
- zasilacze awaryjne *line-interactive*,
- zasilacze awaryjne *on-line*[127].

Zasilacze awaryjne *off-line*, pracując z siecią zasilającą o prawidłowych parametrach, bezpośrednio z niej zasilają podłączone urządzenia. Prowadzą jednocześnie pomiary parametrów zasilania i ładują wewnętrzne akumulatory. Gdy wykryją anomalie w zasilaniu lub jego zanik, przechodzą na pracę awaryjną, uruchamiając swój wewnętrzny falownik, generujący na wyjściu napięcie przemienne, odłączając jednocześnie urządzenia od wadliwej sieci zasilającej.

W UPS-ie typu *line-interactive* regulowana i ciągła moc dostarczana jest do krytycznego obciążenia poprzez inwerter, współpracujący z elementami indukcyjnymi, takimi jak cewka, dławik, liniowy transformator lub transformator ferrorezonansowy. Inwerter eliminuje przepięcia, spadki i zaniki napięcia z sieci zasilającej. Ten UPS umożliwia szybkie przejście na pracę

[126] A. Jadczak, *Jak zarządzać ryzykiem braku prądu*, „Computerworld" 2008, nr 8.

[127] S. Januszewski, C. Kosut, M. Pietranik, M. Pyter, *Systemy bezprzerwowego zasilania (UPS). Komentarz do norm serii PN-EN 62040*, SEP Centralny Ośrodek Szkolenia i Wydawnictw, Warszawa 2002.

awaryjną i z powrotem, przy stosunkowo małych zaburzeniach w przebiegu zasilającym w momencie przełączania[128].

UPS *on-line* separuje całkowicie podłączone do niego urządzenia od linii zasilającej. Zmienne napięcie wejściowe jest przetwarzane na napięcie stałe, które ładuje także akumulatory, a następnie ponownie przetwarzane na napięcie zmienne. Awaria linii zasilającej nie ma więc wpływu na parametry napięcia wyjściowego.

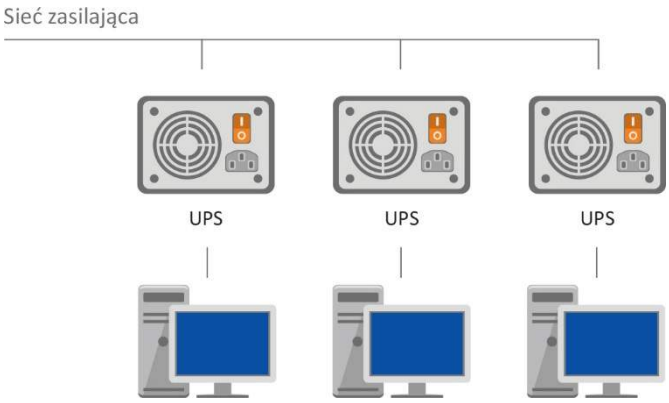
Zasilacze awaryjne pracować mogą w konfiguracjach centralnego (rys. 13) lub rozproszonego (rys. 14) systemu zasilania. Centralny system zasilania awaryjnego jest rozwiązaniem kosztownym, projektowanym zazwyczaj już na etapie budowy budynku. Wymaga wydzielenia osobnych linii zasilających przeznaczonych wyłącznie dla sprzętu informatycznego. UPS zasila całą wydzieloną linię. Położony w osobnym pomieszczeniu lub serwerowni pracuje w kontrolowanym środowisku i jest łatwy do monitorowania. Ze względu na koszty takiego rozwiązania stosuje się je jedynie dla systemów o koniecznej, bardzo dużej niezawodności.

Rys. 13. Centralny system zasilania awaryjnego

Źródło: opracowanie własne.

Rozproszony system zasilania awaryjnego stosowany jest ze względu na niewielkie koszty oraz łatwość wdrożenia. Każdy z UPS-ów zasila pojedyncze urządzenie. Często w celu optymalizacji kosztów, gdy urządzenia położone są w niewielkiej odległości, UPS zasila kilka urządzeń. System ten nie wymaga budowania dedykowanej linii zasilającej. Jest dość trudny do zarządzania i monitorowania. Dużo większą podatność na awarię rekompensuje niewielki wpływ uszkodzenia pojedynczego zasilacza awaryjnego na pracę całego systemu informatycznego.

[128] B. Mężyk, *UPS Line-Interactive – co to naprawdę jest*, „Computerworld" 1994, nr 5.



Rys. 14. Rozproszony system zasilania

Źródło: opracowanie własne.

W dużych przedsiębiorstwach najczęściej spotykany jest system mieszany. Centralny UPS zasila wydzieloną linię, do której podłączone są urządzenia o znaczeniu krytycznym – serwery i aktywne elementy sieci. W systemach centralnego zasilania słabym ogniwem może być sam UPS. Jest to urządzenie dość skomplikowane, w którym, jak w każdym innym urządzeniu, może wystąpić usterka. Niezależnie od konfiguracji w jakiej pracują poszczególne UPS-y, należy zwrócić uwagę na następujące parametry:

- moc wyjściowa,
- współczynnik mocy wyjściowej,
- tolerancja napięcia wejściowego,
- tolerancja częstotliwości napięcia wejściowego,
- tolerancja szybkości zmian częstotliwości,
- przeciążalność,
- współczynnik szczytu,
- miękki start,
- czas podtrzymania[129].

7.5. Nadmiarowość

Nadmiarowość (ang. *Redundancy*) jest wprowadzeniem do systemu informatycznego dodatkowych zasobów sprzętowych i programowych, mających

[129] J. Wiatr, M. Miegoń, *Zasilacze UPS oraz baterie akumulatorów w układzie zasilania gwarantowanego*, Dom Wydawniczy MEDIUM, Warszawa 2008.

na celu zwiększenie jego niezawodności[130]. Zapewnia poprawną pracę systemów pomimo awarii jednego z jego składników, gdyż funkcję uszkodzonego elementu zastępuje element nadmiarowy.

Nadmiarowość serwerów polega na tworzeniu tzw. klastrów (ang. *Cluster*) serwerów. Klaster to niezależne, połączone ze sobą komputery działające razem jako jeden zasób obliczeniowy. Technologia ta stosowana jest w przetwarzaniu równoległym, równoważeniu obciążenia i w rozwiązaniach odpornych na uszkodzenia. Wyróżniamy następujące rodzaje klastrów[131]:

- HPC,
- LBC,
- HA.

HPC (ang. *High Performance Computing*) to klastry wydajnościowe, inaczej zwane klastrami przetwarzania równoległego. Zwiększają szybkość przetwarzania danych. Wymagają jednak specjalnie przygotowanego oprogramowania.

LBC (ang. *Load Balancing Cluster*) to klastry równoważące obciążenie, inaczej zwane klastrami serwerowymi. Dzielą one żądania dostępu do usług pomiędzy serwerami wchodzącymi w skład klastra, tak aby były one równomiernie obciążone.

HA (ang. *High Availability*) to klastry niezawodnościowe. Mają za zadanie eliminację pojedynczych punktów awarii (ang. *Single Point of Failure*). Serwer, zwany w klastrze węzłem (ang. *Node*), może być w sposób dynamiczny usuwany w przypadku awarii oraz dynamicznie dodawany po odzyskaniu sprawności. Procesy rozpoczynające się w uszkodzonym węźle zostają zapisane i podjęte przez następny sprawny węzeł.

Niższym poziomem redundancji jest nadmiarowość poszczególnych podzespołów komputerów i serwerów. Firmy Acorp Electronics Corporation oraz Gigabyte Technology Co., Ltd. niezależnie opatentowały rozwiązania uodparniające płyty główne na uszkodzenia BIOS (ang. *Basic Input/Output System*). Uszkodzenia te zazwyczaj są następstwem działania wirusów lub nieprawidłowego przeprowadzenia aktualizacji. Technologia Gigabyte, znana pod nazwą DualBios, polega na zastosowaniu dwóch

[130] P. Adamczewski, *Słownik informatyczny*, Helion, Gliwice 2005.
[131] K. Lal, T. Rak, *Linux a technologie klastrowe*, Mikom, Warszawa 2005.

niezależnych układów scalonych (kości). W przypadku awarii jednej, system automatycznie przechodzi na pracę z zapasową. Rozwiązanie Acorp, nazwane Die Hard BIOS II, wymaga interwencji użytkownika, który poprzez przełącznik wybiera odpowiednią kość, z jaką pracować będzie płyta główna[132].

Nadmiarowość pozostałych elementów często połączona jest z technologią HOT-SWAP, czyli wymianą elementów bez konieczności wyłączania jednostki komputerowej. Zwykle jest implementowana w rozwiązaniach serwerowych i obejmuje zasilacze, napędy dysków i wentylatory. W najnowszych urządzeniach wysokiej klasy objęte są nim także pamięci, urządzenia podłączone do szyny komunikacyjnej PCIe (ang. *Peripheral Component Interconnect Express*) oraz procesory, a właściwie karty procesorowe.

Współczesne systemy informatyczne składają się z wielu jednostek połączonych siecią. Sprawne i niezawodne działanie sieci wpływa nie tylko na komfort i wydajność pracy. Uszkodzenie jej elementów może całkowicie uniemożliwić funkcjonowanie systemu. Z tego też względu należy uwzględnić możliwość zastosowania nadmiarowości nie tylko urządzeń i zasilania, ale również aktywnych i pasywnych elementów sieci. Poziom redundancji zależy przede wszystkim od wymagań co do czasu pracy sieci.

Redundancja niskiego poziomu stosowana jest, gdy przerwy w pracy sieci wymagane na konserwację można planować po godzinach pracy przedsiębiorstwa, a jej uszkodzenia mają minimalny wpływ na wydajność pracowników i powodują minimalne straty.

Średni poziom redundancji wymagany jest, gdy konserwację wykonywać można jedynie w dniach wolnych od pracy, gdyż normalnie pracuje przez 24 godziny na dobę. Awarie sieci przynoszą straty i zmniejsza się wydajność pracowników.

Redundancja wysokiego poziomu ma zapewnić 24 godziny pracy sieci, przez 7 dni w tygodniu. Przerwy na konserwację muszą być planowane z wyprzedzeniem i prowadzone z gwarancją terminowego powrotu do normalnej pracy. Awarie mają wydatny wpływ na straty i wydajność użytkowników[133].

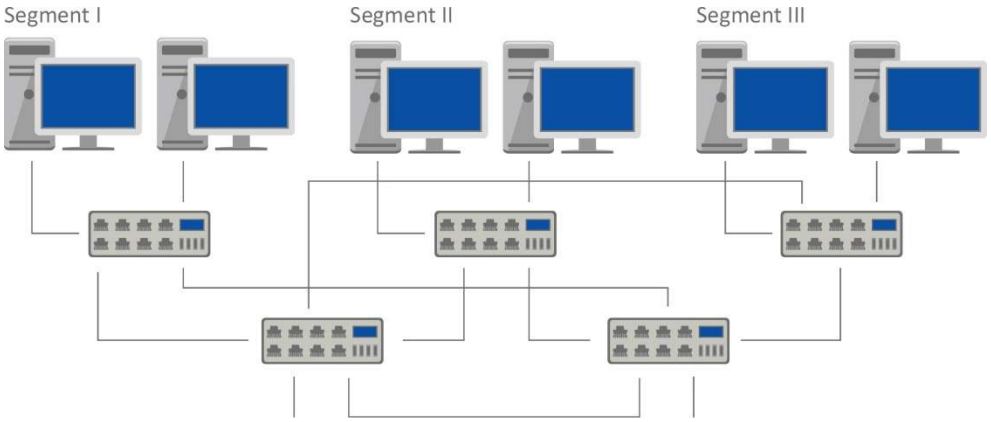
Wyróżniamy redundancję:

[132] A. Pyrchla, B. Danowski, *BIOS. Przewodnik*, wyd. III, Helion, Gliwice 2007.
[133] B. Sosinsky, *Sieci komputerowe. Biblia*, Helion, Gliwice 2011.

- sprzętową,
- połączeń,
- programową.

Redundancja sprzętowa polega głównie na dublowaniu aktywnych elementów sieci, jakimi są przełączniki i routery, a także układy ich zasilania.

O redundancji połączeń (rys. 15) mówimy, gdy pomiędzy dwoma punktami sieci istnieją co najmniej dwie trasy. Stosowana jest zazwyczaj w sieciach wielosegmentowych, w celu zapewnienia ciągłości połączeń pomiędzy segmentami sieci[134].



Rys. 15. Przykład redundancji połączeń w sieci wielosegmentowej

Źródło: opracowanie własne.

Redundancja połączeń metodą samonaprawialnych pierścieni polega na utworzeniu sieci o topologii pierścienia, składającej się ze specjalnie skonstruowanych urządzeń (przełączników). Węzły połączone są dwoma pierścieniami transportującymi dane w przeciwnych kierunkach. W przypadku awarii węzła lub odcinka pierścienia, przepływ danych zostaje przekierowany do drugiego pierścienia[135].

Redundancję programową realizują protokoły:

- STP (ang. *Spanning Tree Protocol*),

[134] S. Mueller, T.W. Ogletree, M.E. Soper, *Rozbudowa i naprawa sieci*, wyd. V, Helion, Gliwice 2006.
[135] W. Pawełczyk, *Redundancja komunikacji w sieci Ethernet – JETNet Ring*, „Biuletyn Automatyki" 2006, nr 1, tom nr 47.

- HSRP (ang. *Hot Standby Router Protocol*),
- VRRP (ang. *Virtual Router Redundancy Protocol*),
- protokoły routingu.

STP obsługiwany jest przez przełączniki (ang. *Network switch*) oraz mosty sieciowe (ang. *Bridge*). Zapobiega powstawaniu pętli, gdyż tworzy graf jedynie aktywnych połączeń, ustalając jednak połączenia rezerwowe. Blokuje je podczas normalnej pracy i aktywuje w przypadku zaniku awarii. Przełączniki i mosty posiadają indywidualne identyfikatory MAC (ang. *Media Access Control*), różne dla każdego egzemplarza aktywnego urządzenia sieciowego, a także komunikują się ze sobą, rozgłaszając ramki BPDU (ang. *Bridge Protocol Data Unit*)[136].

Protokół HSRP[137], opracowany przez firmę CISCO, oraz protokół VRPP[138] mają na celu ochronę domyślnej bramy (ang. *default gateway*) koniecznej w komunikacji sieciowej. Dwa routery współdzielą adres IP oraz adres MAC, tworząc w ten sposób wirtualny router (ang. *Phantom Router*). Awaria jednego fizycznego routera nie ma wpływu na pracę routera wirtualnego.

7.6. Pamięci masowe

Klastry, jak również samodzielne serwery, korzystają z magazynów danych (pamięci masowe). Połączenia takie muszą odbywać się przy pomocy interfejsów zapewniających dużą niezawodność, szybki transfer, możliwość podłączenia większej ilości urządzeń. Pierwszym tego typu interfejsem był SCSI (ang. *Small Computer Systems Interface*), czyli magistrala równoległa, w której każde urządzenie traktowane jest równorzędnie. Posiada własny identyfikator. Może zarówno inicjować operację, jak i być jej wykonawcą. W obrębie jednego urządzenia fizycznego może być wyodrębnionych kilka urządzeń logicznych o własnych identyfikatorach LUN (ang. *Logical Unit Number*)[139].

SCSI umożliwia między innymi podłączenie kilku dysków do kilku różnych komputerów, a także wyminę danych pomiędzy urządzeniami (dyski,

[136] *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*, Institute of Electrical and Electronics Engineers, Inc., Carol Stream 2012.
[137] T. Li, B. Cole, P. Morton, D. Li, *Cisco Hot Standby Router Protocol (HSRP)*, CISCO Systems, RFC 2281, marzec 1998.
[138] R. Hinden, *Virtual Router Redundancy Protocol (VRRP)*, Nokia RFC3768, kwiecień 2004.
[139] P. Metzger, *Anatomia PC. Kompendium*, wyd. IV, Helion, Gliwice 2008.

napędy taśmowe) bez pośrednictwa komputera. Obecnie wykorzystywane najnowsze, Ultra 640 SCSI, przesyłają dane z prędkością 320 MB/s na maksymalną odległość 12 m i obsługują do 16 urządzeń. Planowany standard Ultra 640 SCSI nie wszedł już w życie, zastąpiony przez nowszy SAS (ang. *Serial Attached* SCSI). Równoległa magistrala zmieniona została w szeregową. Każde z urządzeń wykorzystuje niezależne połączenia, nie dzieląc wspólnego pasma. Dzięki temu zwiększyła się też odporność układu na awarie. Uszkodzenie jednego urządzenia pozostaje bez wpływu na pozostałe. SAS zapewnia transfer do 600 MB/s urządzeniom oddalonym o nie więcej niż 10 m od kontrolera. Umożliwia podłączenie większej liczby urządzeń, niż liczba portów kontrolera, poprzez dodatkowe urządzenia, tzw. edge expander. Ich maksymalna liczba to 128, przy czym można podłączyć do nich kolejne urządzenia rozszerzające – „fanout expander", uzyskując w ten sposób potencjalną możliwość zastosowania ponad 16 tysięcy urządzeń końcowych[140].

Obecnie SAS konkuruje z technologią FC (ang. *Fibre Channel*) i iSCSI (ang. *Internet SCSI*). Zaletą obu jest możliwość pracy przy dużej odległości pomiędzy urządzeniami. FC zapewnia transfer danych na odległość 100 km z prędkością 4 GB/s, zaś iSCSI – 1 GB/s przy nieograniczonej, poprzez stosowanie switchy, odległości. FC wykorzystuje kable miedziane oraz światłowody, a także kosztowne kontrolery HBA.

Choć na razie iSCSI nie może równać się z SAS czy FC pod względem prędkości, to w miarę rozwoju łącz Ethernet będzie zyskiwał na znaczeniu. Jest też rozwiązaniem znacznie tańszym oraz łatwiejszym do wdrożenia[141].

Same pamięci masowe, a nawet twarde dyski, mają zaimplementowane technologie redundancji. Nowoczesne twarde dyski w swoim oprogramowaniu systemowym (ang. *firmware*) zawierają oprogramowanie monitorujące stan techniczny dysku – HDD S.M.A.R.T (ang. *Self Monitoring, Analysis and Reporting Technology*). Potrafi ono przenosić dane z sektorów, w których napotyka na błędy odczytu, zapisu lub weryfikacji, do sprawnych sektorów

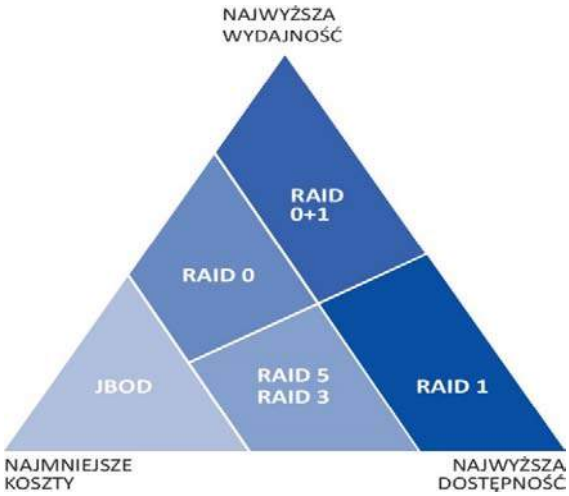
[140] *Serial Attached SCSI: Meeting the Growing Needs of Enterprise Storage*, White Papers, Adaptec, Inc., Singapore 2004.
[141] K. Jakubik, *Fibre channel kontra ISCSI*, „Networld" 2006, nr 1.

z zapasowej puli i ukrywać błędne sektory (ang. *bad blocks*), wyłączając je tym samym z pracy[142].

W przypadku nagłych awarii, np. układów mechanicznych lub elektronicznych, technologia HD S.M.A.R.T często okazuje się zawodna. Dlatego też stosuje się nadmiarowość na wyższym poziomie, łącząc dyski w tzw. macierze RAID (ang. *Redundant Array of Independent Disks*). Oprócz wzrostu odporności na awarie, zwiększają prędkość transmisji danych oraz przestrzeń dyskową widzianą jako całość[143]. Wyróżniamy poziomy RAID od 0 do 7 oraz ich modyfikacje:

- RAID 0+1,
- RAID 1+0,
- MATRIX RAID,
- RAID 0+5,
- RAID ADG.

Wybór odpowiedniej macierzy wiąże się ze znalezieniem właściwej proporcji pomiędzy dostępnością, wydajnością i kosztem, co pokazuje graf na rys. 16.



Rys. 16. Graf wyboru RAID

Źródło: J. Luther, *Macierze RAID*, op. cit.

[142] E. Pinheiro, W.D. Weber, L.A. Barroso, *Failure Trends in a Large Disk Drive Population*, 5th USENIX Conference on File and Storage Technologies (FAST'07), San Jose, luty 2007.

[143] J. Luther, *Macierze RAID*, „PC World" 2003, nr 10, wyd. specjalne *Sprzęt – urządzenia peryferyjne*.

Tabela 10. Podstawowe parametry macierzy RAID

RAID	Minimalna liczba dysków	Dostępna przestrzeń	Liczba dysków, które mogą ulec awarii bez utraty danych
RAID 0	2	N	0
RAID 1	2	1	N – 1
RAID 2	3	N – logN	1
RAID 3	3	N-1	1
RAID 4	3	N-1	1
RAID 5	3	N-1	1
RAID 6	4	N-2	2
RAID 7	3	N-1	1

Źródło: opracowanie własne.

Istnieje jeszcze wiele innych egzotycznych odmian macierzy, promowanych przez poszczególne firmy. Parametry podstawowych konfiguracji zostały pokazane w tabeli 10.

Tabela 11. Różnice w sprzętowej i programowej realizacji RAID

	RAID sprzętowy	RAID programowy
Koszt implementacji	Wysoki	Niski
Wydajność	Duża	Mała
Zależność od systemu operacyjnego	Niezależny	Zależny
Czas odbudowy	Krótki	Długi
Obciążenie procesora	Małe	Duże

Źródło: opracowanie własne.

Macierze RAID mogą być budowane na podstawie rozwiązań sprzętowych oraz programowych. Wiele systemów operacyjnych ma wbudowane mechanizmy tworzenia i obsługi RAID. W tabeli 11 powyżej przedstawiono podstawowe różnice pomiędzy obydwoma rozwiązaniami.

7.7. Rozpraszanie zasobów

Klastry oraz stabilna i niezawodna sieć dają możliwość stosowania rozproszonego systemu plików DSF (ang. *Distributed File System*). Pozwala on umieścić dane w wielu lokalizacjach fizycznych. Przy czym pliki znajdujące się na licznych serwerach dla użytkownika wyglądają tak, jak gdyby znajdowały się w jednym miejscu w sieci. Wyróżniamy Stand-Alone DFS, w którym schemat powiązań pomiędzy lokalizacjami jest przechowywany na jednym serwerze, oraz Fault-tolerant DFS, replikujący go pomiędzy różnymi serwerami.

Sieciowe systemy plików to zagadnienie węższe. Dzięki nim także uzyskać można dostęp do danych poprzez sieć, jednakże brak jest możliwości połączenia danych pochodzących z wielu lokalizacji w jedną, spójną jednostkę logiczną. Dopiero łączne stosowanie obu rozwiązań daje pełną niezależność od fizycznego położenia danych.

Najczęściej spotykane sieciowe i rozproszone systemy plików to:

- NFS,
- AFS,
- Coda,
- SMB.

NFS (ang. *Network File System*) został opracowany przez firmę Sun Microsystems. Obecnie jest protokołem otwartym. Umożliwia współdzielenie systemów plików pomiędzy dowolną liczbą komputerów, z których każdy może pełnić rolę zarówno klienta, jak i serwera. Pozwala udostępniać katalogi lokalnego systemu plików na jednym komputerze oraz mapować go na innych. Obsługa zamapowanego udziału nie różni się od obsługi lokalnego systemu plików[144].

AFS (ang. *Andrew File System*) stworzono na Carnegie Mellon University. Najważniejszą logiczną jednostką jest w AFS, tzw. wolumin, czyli zbiór powiązanych ze sobą plików i katalogów. Woluminy mogą być przenoszone do innych lokalizacji bez konieczności powiadamiania użytkowników. Czynność ta może być wykonywana także, gdy wolumin jest zajęty. Pracę na plikach obsługują dwa procesy, proces klienta – Venus oraz proces serwera – Vice. Venus, na żądanie, otrzymuje od Vice plik wraz z obietnicą

[144] R. Scrimger, P. LaSalle, C. Leitzke, M. Parihar, M. Gupta, *TCP/IP. Biblia*, Helion, Gliwice 2002.

zawiadomienia o zmianie pliku przez innego użytkownika (ang. *callback promise*). Korzystać z niego może do chwili otrzymania takiego zawiadomienia. AFS jest odporny na chwilowe zerwanie połączenia, gdyż faktycznie praca odbywa się na lokalnej kopii plików[145].

Protokół Coda również opracowano na uniwersytecie Carnegie Mellon i jest on następcą AFS. Charakteryzuje się zwielokrotnianiem woluminów dostępnych do czytania i zapisywania w celu zwiększenia prędkości operacji. Grupa serwerów przechowujących kopie wolumenów VSG (ang. *Volume Storage Group*) umożliwia dostęp klientowi do swojego podzbioru AVSG (ang. *Available Volume Storage Group*). Klient dostaje również obietnicę powiadomienia o zmianach. W przypadku odłączenia od sieci, praca odbywa się na kopiach lokalnych, które synchronizowane są z AVSG po ponownym uzyskaniu połączenia[146].

SMB (ang. *Server Message Block*) został opracowany przez firmy Intel, Microsoft i IBM na potrzeby wymiany plików oraz wspólnej pracy z drukarkami. Charakteryzuje się specyficznym mechanizmem blokowania plików przez klienta, tzw. *opportunistic locks*. Poprzez *opportunistic locks* klient informuje serwer SMB o lokalnym wykonywaniu operacji na pliku. Żądanie dostępu do zajętego pliku przez innego użytkownika zrywa blokadę, wymuszając wcześniej zapis uaktualniający.

Nadmiarowość w komputerach stanowiących końcówki sieci jest zbyt kosztowna. Dąży się więc do tego, by każdy komputer można było zastąpić inną jednostką. Wymaga to oczywiście unifikacji stanowisk komputerowych, zarówno w zakresie sprzętu, jak i zainstalowanego na nim oprogramowania. Należy jednak zadbać o dane tworzone przez użytkowników. Trudno wdrożyć techniki *backupu* w tak rozproszonym środowisku. Można jednak zaimplementować mechanizmy takie jak kopie migawkowe (ang. *snapshot*), ciągłą ochronę danych CDP (ang. *Continuous Data Protection*) czy synchronizację danych pomiędzy końcówką sieci a serwerem. CDP jest w stanie wychwycić każdą zmianę pliku, katalogu czy bazy danych oraz zapisać stan poprzedni. To rozwiązanie wydaje się być idealnym sposobem

[145] A.S. Tanenbaum, M. van Steen, *Systemy rozproszone. Zasady i paradygmaty*, WNT, Warszawa 2005.
[146] M. Satyanarayanan, M.R. Ebling, J. Raiff, P.J. Braam, J. Harkes, *Coda File System User and System Administrators Manual*, Coda Team 2000, http://coda.cs.cmu.edu/doc/html/manual/index.html.

ochrony danych. Jednakże w rozbudowanych systemach informatycznych zmian jest tak dużo, że zapisy generowane przez CDP mogą w wydatny sposób wpłynąć niekorzystnie na wydajność systemu. Lepszym rozwiązaniem wydają się być kopie migawkowe. Wykonywane co określoną jednostkę czasu, pozwalają nie tylko zapisać dane przed ich zmianą, lecz także zawartość buforów[147].

Odtworzenie stanowiska komputerowego przy pomocy omówionych powyżej technologii wymaga jednak czasu. Innym rozwiązaniem jest zastosowanie tzw. profili mobilnych. Pozwalają one użytkownikom systemów Windows używać wszystkich indywidualnych ustawień systemu, oprogramowania, a także osobistych plików i folderów na różnych komputerach w ramach tej samej sieci. Ustawienia te oraz dane przechowywane są na serwerze i kopiowane na jednostkę, na którą loguje się ich właściciel. Po wylogowaniu następuje synchronizacja danych lokalnych i zapisanych na serwerze. Zastosowanie profili mobilnych wiąże się więc z wydłużonym czasem logowania i wylogowywania się z systemu[148].

Coraz bardziej powszechna staje się praca terminalowa, czyli obsługa programu zainstalowanego i uruchomionego na innym komputerze. Polecenia przetwarzania danych wydawane przez końcówkę, którą jest najczęściej tzw. cienki klient (ang. *Thin Client*), realizowane są po stronie serwera. Cienki klient to komputer lub urządzenie, zwane też terminalem, wyposażony w odpowiednie oprogramowanie do łączenia się z serwerem. Wyniki przetwarzania przesyłane są na ekran terminala. Obsługiwane w ten sposób może być jedynie oprogramowanie o architekturze klient–serwer. Jest to, obok uzależnienia od protokołów, podstawowa wada tego rozwiązania.

Najczęściej spotykanymi rozwiązaniami stosowanymi w pracy terminalowej są:

- Telnet – obsługujący jedynie terminale alfanumeryczne,
- SSH (ang. *Secure Shell*) – pozwalający także na pracę w trybie znakowym, zapewniający jednak na szyfrowanie przesyłanych informacji,
- X Window System – zapewniający połączenie w trybie graficznym z systemami UNIX/LINUX,

[147] K. Jakubik, *Ochrona danych przed błędami ludzkimi*, „Networld" 2007, nr 9.

[148] D. Holme, *Efektywne rozwiązania dla specjalistów IT. Resource Kit*, Microsoft Press, Warszawa 2008.

- VNC (ang. *Virtual Network Computing*) – obsługujący także tryb graficzny, dostępny dla większości systemów operacyjnych,
- RDP (ang. *Remote Desktop Protocol*) – zapewniający wsparcie dla usług terminalowych firmy Microsoft[149].

Każdy terminal może więc być zastąpiony innym, a czas rozpoczęcia pracy na nowym stanowisku jest minimalny. Zastosowanie cienkiego klienta przynosi też korzyści ekonomiczne, gdyż urządzenie to jest znacznie tańsze od jednostki komputerowej ze względu na swoją niską złożoność technologiczną. W minimalnej konfiguracji składa się z klawiatury, monitora i jednostki centralnej, zawierającej interfejs sieciowy oraz oprogramowanie klienckie. Nie jest wymagana duża moc obliczeniowa oraz nośniki danych o dużej objętości. Cienki klient nie wymaga również tak częstej wymiany, ze względu na proces tzw. starzenia się moralnego, jak klasyczne jednostki komputerowe.

Należy się jednak liczyć z opóźnieniami reakcji systemu na polecenia. Związane są one przede wszystkim z prędkością sieci. Osiągane transfery są nieporównywalne z tymi, jakie zapewniają nośniki danych. Dlatego też niezwykle istotnym jest, aby w wymianie danych pomiędzy klientem a serwerem stosowane były zaawansowane algorytmy kompresji, a graficzne interfejsy użytkownika charakteryzowały się prostotą.

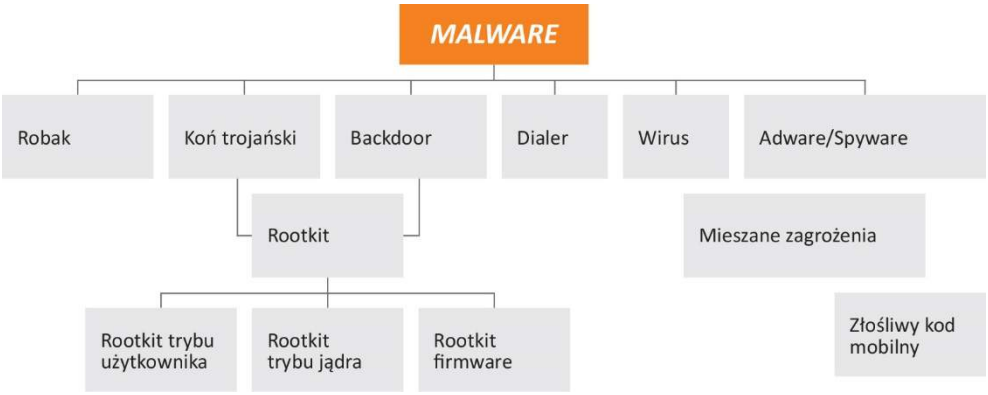
7.8. Ochrona antywirusowa

Od lat 80. zeszłego wieku wirusy ewoluowały, obecnie to jedynie jeden z kilku rodzajów złośliwego oprogramowania. Pojawił się nowy termin – *malware* czyli złośliwe oprogramowanie – obejmujący wszystkie typy programów (rys. 17), które zostały stworzone specjalnie do infiltracji, uszkadzania systemów komputerowych lub innych niepożądanych czynności bez wiedzy i zezwolenia ich użytkowników.

Ochronę przed *malware* zapewnia oprogramowanie antywirusowe. Zastosowane w rozwiniętych organizacjach, oprócz podstawowej funkcji, jaką jest ochrona przed wszystkimi jego rodzajami, powinno cechować się możliwością zdalnej, centralnej administracji. Należy zwrócić uwagę na fakt, iż nieliczne z oferowanych na polskim rynku antywirusów chronią systemy przed rootkitami oraz spamem. Prostota instalacji i konfiguracji to cecha

[149] R. Chyra, *Usługi terminalowe Windows 2000*, Helion, Gliwice 2003.

drugorzędna, gdyż zazwyczaj zajmuje się tym wykwalifikowana kadra. Inną, rzadko braną pod uwagę przy zakupie cechą, jest wpływ, jaki działający w tle antywirus ma na wydajność systemu oraz zużywane przez niego zasoby (pamięci operacyjnej i mocy obliczeniowej procesora) przy skanowaniu, a w szczególności podczas monitorowania.



Rys. 17. Kategorie *malware*
Źródło: *10 Faces of Computer Malware*, portal Techrepublic, http://www.techrepublic.com/blog/10-things/the-10-faces-of-computer-malware/.

Należy również zasięgnąć informacji, jak często producent dostarcza aktualizacje sygnatur wirusów i samej aplikacji. Pomocne w wyborze są publikowane w czasopismach fachowych testy i rankingi. Warto jednak zwrócić uwagę na kryteria, którymi kierują się ich autorzy.

Skuteczność oprogramowania antywirusowego jest obecnie podważana. Antywirusy wykrywają i usuwają złośliwe oprogramowanie. Zazwyczaj składają się z modułu skanera, który na żądanie sprawdza wybiórczo dane, oraz monitora nadzorującego pamięć operacyjną i system plików.

Szkodliwe oprogramowanie wykrywane jest przy pomocy metody opartej na sygnaturach, czyli wzorcach zagrożeń, lub metody heurystycznej. Wzorzec (ang. *pattern*) jest ciągiem bajtów wyekstrahowanym ze szkodliwego oprogramowania. Musi on jednoznacznie je identyfikować i nie występować w innych, nieszkodliwych plikach. Poprawny wzorzec nie może być zbyt krótki, gdyż wywoływać będzie fałszywe alarmy, ani zbyt długi,

ponieważ jego wyszukiwanie powodowałoby zbyt duże obciążenie procesora i zużycie pamięci operacyjnej. Metoda wykorzystująca wzorce zagrożeń ma jedną podstawową wadę. Jest skuteczna jedynie wobec znanych wirusów, dla których opracowano już odpowiednie sygnatury. Czynione są wprawdzie próby opracowania wzorców uogólnionych, jednakże znacznie skuteczniejszą metodą wykrywania nowych nieznanych, złośliwych programów, jest metoda heurystyczna.

Działanie metody na bazie sygnatur, zaimplementowanej w eksploatowanym programie antywirusowym, możemy sprawdzić w sposób bezpieczny, tworząc testowego wirusa EICAR Test Virus, opracowanego przez European Institute for Computer Anti-Virus Research (EICAR). Tworzymy plik tekstowy zawierający następujący ciąg znaków:

X5O!P%@AP[4PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Następnie zmieniamy jego rozszerzenie z domyślnego *.txt na *.com lub *.exe, tak aby udawał plik wykonywalny. Tak utworzony plik powinien wywołać alarm programu wirusowego.

Metodę heurystyczną podzielić można na statyczną i dynamiczną. Heurystyka statyczna opiera się na analizie pliku traktowanego jako ciąg bajtów, w których wyszukuje się fragmenty znane z innych niebezpiecznych programów, a odróżniające je od bezpiecznych. Heurystyka dynamiczna jest analizą zachowania podejrzanego programu w bezpiecznym środowisku.

7.9. Włamania do systemu informatycznego

Od wynalezienia tranzystora, który otworzył drogę do budowy komputerów, do momentu pierwszego głośnego włamania, minęły zaledwie 24 lata. W roku 1971 John T. Draper przełamał zabezpieczenia firmy telekomunikacyjnej AT&T, uzyskując dostęp do ukrytych funkcji centrali telefonicznej[150]. Tym samym stał się pierwszym znanym hakerem, czyli osobą zajmującą się łamaniem zabezpieczeń systemów informatycznych. Działalność hakerów, choć niezgodna z prawem, nie zawsze jest szkodliwa. Czasem prowadzona jest w ramach hobby, nie pociąga za sobą zniszczeń, a wytyka błędy i źródła zagrożeń. Częściej jednak jest źródłem wycieku danych i utraty kontroli nad działaniem systemu. Nie można jednak dopuścić do nieautoryzowanego

[150] G.D. Robson, *The Origins of Phreaking*, "Blacklisted! 411" 2004, Vol. 6, Iss. 2.

dostępu, bez względu na intencje. Najbardziej znane fakty związane z włamaniami zawarto w tabeli 12.

Tabela 12. Najsłynniejsze fakty związane z włamaniami komputerowymi

Rok	Haker	Opis
1971	John Draper, znany jako „Cap'n Crunch”	Włamanie zabezpieczeń w systemach telefonicznych
1983	Kevin Poulsen, znany jako „Dark Dante”	Włamanie do sieci ARPANET
1984	Bill Landreth, znany jako „Cracker”	Włamanie do systemów NASA i Departamentu Obrony
1986	Loyda Blankenship, znany jako „The Mentor”, członek grupy „Legion of Doom”	Aresztowanie autora słynnego manifestu *Hacker's Manifesto*
1990	Kevin Poulsen	Włamanie do systemu telefonicznego w Los Angeles
1992	grupa „Masters of Deception’	Aresztowanie grupy hakerów, która w nielegalny sposób nawiązywała połączenia telefoniczne
1994	Richard Pryce, znany jako „Datastream Cowboy”	Włamanie do komputerów bazy lotniczej w Rzymie, włamanie do koreańskiego Instytutu Badań Atomowych
1994	Vladimir Levin, matematyk rosyjski	Włamanie się do systemu komputerowego Citibanku i kradzież 10 milionów dolarów
1995	Kevin Mitnick	Aresztowanie hakera znanego z licznych włamań do systemów największych koncernów komputerowych i telekomunikacyjnych dokonywanych od lat 70. XX wieku
1998	Hao Jinglong i Hao Jingwen	Włamanie do sieci komputerowej banku i kradzież 87 tysięcy dolarów
1998	Ehud Tenebaum, znany jako „Analyzer’	Włamanie do ponad tysiąca znanych serwerów w Stanach Zjednoczonych
2000	haker znany jako „Mafiaboy”	Przeprowadzenie ataku dos, w wyniku którego nieczynne były strony Yahoo, ebay, Amazon, CNN
2000	Alexei V. Ivanov i Vasiliy Gorshkov	Włamania do Central National Bank of Waco w Teksasie, Nara Bank NA w Los Angeles
2002	Nieznany	Masowy atak na 13 internetowych serwerów DNS
2003	Lynn Htun	Włamanie do Symantec i SecurityFocus
2009	chińscy hakerzy	Włamanie do komputerów Dalajlamy i wielu tybetańskich uchodźców
2010	Hacker Croll (pseudonim)	Włamanie do konta Baracka Obamy na Twitterze

Źródło: opracowanie własne.

Najprostszym, a zarazem najskuteczniejszym sposobem nielegalnego dostania się do systemu, jest odgadnięcie lub zdobycie hasła i nazwy użytkownika. W dużych organizacjach, zatrudniających licznych pracowników użytkujących komputery, nazwy użytkowników przyznawane są według określonych zasad, np. pierwsza litera imienia, znak kropki i nazwisko. Informacja o sposobie ich generowania jest powszechnie znana wśród kadry pracowniczej i nie uznawana jest za szczególnie chronioną. Do rzadkości należy również usuwanie standardowych nazw użytkowników administrujących systemem, takich jak „admin", „administrator" czy „manager". Stąd odgadnięcie ich nie jest zadaniem trudnym, szczególnie w jednostkach publicznych, w których nazwiska urzędników są jawne i często wypisane na drzwiach biur.

Każdy administrator spotkał się również z problemem zapisywania haseł przez pracowników i pozostawiania ich w dostępnym dla innych miejscu. Ponieważ pamięć ludzka jest zawodna, poza zapisywaniem panuje też tendencja do konstruowania najprostszych i najkrótszych haseł.

Oprócz pozyskania informacji o sposobie dostania się do systemu pośrednio lub bezpośrednio od pracowników lub próbie ich odgadnięcia, popularną techniką jest tzw. *sniffing*. Technika ta polega na podsłuchiwaniu wszystkich pakietów krążących w sieci. Ich analiza może doprowadzić do ujawnienia informacji o sposobie logowania. Służące do tego aplikacje – *sniffery* – nie są jednak tylko narzędziami hakerskimi. Użytkowane są też przez administratorów diagnozujących sieć. Zabezpieczeniem przeciwko *sniffingowi* jest stosowanie szyfrowanych połączeń np. SSL (ang. *Secure Socket Layer*).

Atak na system informatyczny zaczyna się zwykle od skanowania otwartych portów na serwerze ofiary. Choć nie jest to działanie karalne, to środowisko informatyków uznaje je za nieetyczne. Skanowanie portów pozwala na uzyskanie informacji o dostępnych usługach sieciowych oraz wersjach oprogramowania, które je udostępnia. Najczęściej używane porty zostały wyszczególnione w tabeli 13.

Pełna lista wykorzystywanych portów przez ogólnie znane oprogramowanie oraz protokoły publikowana jest przez Internet Assigned Numbers Authority (IANA) – organizację zajmującą się zarządzaniem domenami

najwyższego poziomu oraz ogólnym nadzorem nad działaniem mechanizmu DNS.

Tabela 13. Wykaz najczęściej wykorzystywanych portów sieciowych

Nr portu	Nazwa usługi	Nr portu	Nazwa usługi
20	FTP	80	http
21	FTP	109	POP2
22	SSH	110	POP3
23	Telnet	119	NNTP
25	SMTP	143	IMAP
53	DNS	443	HTTPS

Źródło: opracowanie własne.

Najczęściej stosowaną metodą ataku jest *spoofing*. Polega on na fałszowaniu podstawowych usług oraz protokołów sieciowych tak, aby ofiara ataku rozpoznała atakującego jako uprawnionego do dostępu do określonych zasobów sieci. Wyróżniamy następujące kategorie *spoofingu*:

- ARP *spoofing*,
- IP *spoofing*,
- DNS *spoofing*,
- Web *spoofing*,
- E-mail *spoofing*[151].

Poważne zagrożenie stanowi przepełnienie bufora (ang. *Buffer overflow*). Do określonego obszaru pamięci wprowadza się większą ilość danych niż została zarezerwowana przez autorów oprogramowania. Skutkować to może przejęciem kontroli nad działaniem programu. Programy wykorzystujące błędy aplikacji umożliwiające przepełnienie bufora zwane są exploitami. Microsoft w poprawce Service Pack 2 zaimplementował metodę blokowania prób uruchomienia nieautoryzowanego kodu DEP (ang. *Data Execution Prevention*). Jednakże Berend-Jan Wever, specjalista ds. bezpieczeństwa z koncernu Google, zaprezentował technikę obchodzenia go, zamieszczając exploita na swoim prywatnym blogu[152].

[151] K. Folga, *Spoofing: sztuka ataku i obrony*, „Networld" 2005, nr 10.

[152] G. Keizer, *New exploit technique nullifies major Windows defense*, "Computerworld" 2010, No. 3.

Najbardziej narażone na ataki są portale internetowe organizacji, ogólnie dostępne z racji swojej funkcjonalności. Charakteryzują się podatnością na „wstrzyknięcie" (ang. *injection*) kodu np. SQL, który wykonuje serwer WWW. Zamiast oczekiwanych danych otrzymuje polecenia. Innym równie groźnym atakiem jest XSS (ang. *Cross Site Scripting*). Polega on na wyświetleniu danych pochodzących od użytkownika, bez wcześniejszej ich walidacji. Skutkować to może przejęciem sesji ofiary i wykonaniem skryptu korzystającego z jej uprawnień.

Ranking zagrożeń stron internetowych prowadzony jest w ramach projektu OWASP (ang. *The Open Web Application Security Project*)[153].

Atakujący systemy informatyczne nie zawsze mają na celu uzyskanie do niego dostępu. Ataki typu DoS (ang. *Denial of Service*) powodują przeciążenie systemu. Zwykle polegają na wysyłaniu dużej liczby zleceń, których realizacja zajmuje całe zasoby. Odmianą DoS jest DDoS (ang. *Distributed Denial of Service*), gdzie atak następuje z wielu źródeł jednocześnie, a także DRDoS (ang. *Distributed Reflection Denial of Service*), co polega na sfałszowaniu adresu ofiary tak, aby zalewana ona była odpowiedziami z sieci.

Podstawowymi środkami technicznymi stosowanymi w celu zabezpieczenia systemów informatycznych przed atakami są systemy IDS/IPS. IDS (ang. *Intrusion Detection Systems*) to sprzętowe bądź programowe rozwiązania przeznaczone do wykrywania intruzów, czyli uzyskania nieautoryzowanego dostępu do chronionego nimi systemu. Wraz z zaporą sieciową tworzą systemy IPS (ang. *Intrusion Prevention Systems*), które oprócz informowania o ataku podejmują także próby jego zablokowania.

Podstawowymi zadaniami systemów IDS/IPS są:

- monitorowanie systemu,
- detekcja ataków,
- podejmowanie odpowiednich działań w zależności od zagrożenia.

Podział systemów IDS/IPS ze względu na metody analizy oraz typy odpowiedzi przedstawiony jest w tabeli 14.

[153] *The Ten Most Critical Web Application Security Risks*, OWASP Foundation 2010, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

Tabela 14. Podział systemów IDS/IPS

Klasyfikacja IDS/IPS według źródeł informacji	Klasyfikacja IDS/IPS według metod analizy	Klasyfikacja IDS/IPS według typów odpowiedzi
IDS hostowy (*Host IDS*)	Metoda ta inaczej zwana sygnaturową (*signature-based detection*) polega na wykrywaniu zachowań charakterystycznych dla poznanych już metod ataku	Odpowiedzi aktywne (*Active Responses*) Automatyczne działania, podejmowane w wyniku wykrytych anomalii lub nadużyć
IDS Aplikacyjny (*Application-Based IDS*)	Detekcja anomalii (*Anomaly Detection*) Detekcja anomalii polega na wykrywaniu niezwyczajnych zachowań (anomalii) odbiegających od przyjętych dla normalnej aktywności chronionego systemu	Zbieranie dodatkowych informacji
IDS sieciowy (*Network IDS*)		Zmiana środowiska
IDS węzłowy		Podjęcie akcji przeciwko intruzowi
		Alarmy i powiadomienia w postaci okien pop-up, e-maili, SMS'ów lub pułapki SNMP (*Simple Network Management Protocol*) kierujące wiadomości do centralnej kontroli zarządzającej

Źródło: opracowanie własne.

7.10. Fizyczna ochrona informacji

Ochrona fizyczna w postaci drzwi, zamków, sejfów, krat oraz systemów alarmowych stanowi podstawowe elementy systemu bezpieczeństwa informacji. Ogranicza możliwość kradzieży dokumentów, blokuje bezpośredni dostęp do urządzeń przetwarzających informacje oraz nośników je przechowujących. Trudno jednak okratować całą firmę. Z tego też względu przedsiębiorstwo winno być podzielone na obszary o zbliżonych poziomach wymagań bezpieczeństwa oraz poziomach ryzyka jego naruszenia. Obszarami o najwyższym poziomie bezpieczeństwa są tereny obejmujące kancelarię

tajną oraz serwerownię[154]. Dla każdego typu obszaru można dobrać odpowiednie zabezpieczenia techniczne.

Niestety, nie istnieją normy uwzględniające specyfikę ochrony informacji. Można się kierować klasyfikacją zagrożeń znajdującą się w już nieaktualnej polskiej normie PN-93/E-08390/14: 1993, co przedstawiono w tabeli 15.

Tabela 15. Klasyfikacja zagrożeń wg PN-93/E-08390/14: 1993

Symbol	Zagrożone elementy
Z1a	Mienie o małej wartości, które można wymienić lub zastąpić
Z2a	Mienie średniej wartości, które można wymienić lub zastąpić
Z2b	Dokumenty lub przedmioty o wartości zabytkowej lub muzealnej, występujące w powtarzalnych egzemplarzach lub które można odtworzyć
Z2c	Dokumenty zawierające tajemnicę służbową
Z3a	Mienie dużej wartości
Z3b	Dokumenty lub przedmioty mające zabytkową wartość, niepowtarzalne w kraju
Z3c	Dokumenty o dużej wartości, których uszkodzenie, zniszczenie lub kradzież jak również poznanie może prowadzić do dużych szkód
Z3d	Życie ludzi związanych z wartościami wymienionymi w punktach a, b, c
Z4a	Mienie bardzo dużej wartości
Z4b	Przedmioty zabytkowe stanowiące dziedzictwo kultury światowej
Z4c	Dokumenty, których kradzież jak również poznanie lub podejrzenie przez osoby niepowołane może zagrażać porządkowi społecznemu, osłabieniu obronności lub egzystencji państwa
Z4d	Życie wielu ludzi

Źródło: Polska Norma PN-93/E-08390/14: 1993 Systemy alarmowe – Wymagania ogólne – Zasady stosowania, PKN, Warszawa 1993.

Przy stosowaniu powyższej klasyfikacji napotkać można problem z rozróżnieniem mienia dużej i bardzo dużej wartości. Rodzi się też pytanie natury moralnej, dlaczego zagrożenie życia ludzi (Z3d) jest klasyfikowane niżej niż

[154] E. Studzińska, *Bezpieczeństwo techniczne. Więcej niż ochrona*, Raport specjalny *Bezpieczeństwo techniczne*, „Computerworld" 2009.

utrata mienia bardzo dużej wartości. Jeśli możliwe jest finansowe określenie skutków utraty informacji, to pomocna może być klasyfikacja zawarta w załączniku do uchylonego już Rozporządzenia MSWiA z 14 października 1998 roku w sprawie szczegółowych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych przez przedsiębiorców i inne jednostki organizacyjne[155].

W tabeli 16 każdej klasie odporności przyporządkowano limit wartości pieniężnych wyrażony w jednostkach przeliczeniowych. Jedna jednostka przeliczeniowa wynosi 120-krotność przeciętnego miesięcznego wynagrodzenia za ubiegły kwartał, ogłaszanego przez prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski". Minimalna wartość odporności na włamania RU (ang. *Resistance Units*) jest określana na podstawie dwóch parametrów: czasu trwania włamania oraz rodzaju użytego narzędzia. Testy sprawdzające, ile czasu zajmuje włamywaczowi dostanie się do sejfu, bez uwzględniania natężenia hałasu lub dymu, przeprowadzane są w Polsce przez Instytut Mechaniki Precyzyjnej w Warszawie.

Podział pomieszczeń przedsiębiorstwa na strefy bezpieczeństwa umożliwia dobór odpowiednich zabezpieczeń technicznych. Dla informacji niejawnych są one określone w Rozporządzeniu Rady Ministrów z 29 maja 2012 roku w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych[156]. Serwerownie w jednostkach rządowych i samorządowych powinny spełniać równie ostre kryteria mające na względzie:

- fizyczne umiejscowienie pomieszczenia,
- budowę ścian,
- sposoby zabezpieczeń otworów drzwiowych i okiennych,
- rodzaje szaf do przechowywania dokumentacji,
- systemy alarmowe,
    - system sygnalizacji pożarowej,
    - system sygnalizacji włamania i napadu,

[155] Rozporządzenie MSWiA z 14 października 1998 r. w sprawie szczegółowych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych przez przedsiębiorców i inne jednostki organizacyjne, Dz.U. Nr 129, poz. 858.

[156] Rozporządzenie Rady Ministrów z 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych, Dz.U. 2012 r., poz. 683.

- systemy nadzoru wizyjnego,
- sposób niszczenia dokumentów.

Tabela 16. Klasyfikacja odporności na włamania pomieszczeń i urządzeń

Klasa odporności na włamanie pomieszczeń i urządzeń	Minimalna wartość odporności na włamania (RU)		Klasa zamka	Dopuszczalny limit wartości pieniężnych (w jednostkach obliczeniowych) przechowywanych w pomieszczeniach i urządzeniach			
				Pomieszczenia i urządzenia nie chronione systemem alarmowym lub chronione systemem alarmowym klasy niższej od SA3		Pomieszczenia i urządzenia chronione systemem alarmowym klasy co najmniej SA3	
	Dostęp częściowy	Dostęp całkowity		Pomieszczenia	Urządzenia	Pomieszczenia	Urządzenia
0	Poniżej 30	Poniżej 50	1 x A	–	–	–	–
I	30	50	1 x A	–	0,5	–	1,3
II	50	80	1 x A	–	1,5	–	3
III	80	120	1 x B	–	3	–	6
IV	120	180	2 x B	–	5	–	10
V	180	270	2 x B	8	8	15	15
VI	270	400	2 x C	12	12	20	20
VII	400	600	2 x C	16	16	30	30
VIII	550	825	2 x C	20	20	40	40
IX	700	1050	2 x C	30	–	60	60
X	900	1350	2 x C	40	–	100	100
XI	–	2000	3 x C lub 2 x D	60	–	Bez ograniczenia	–
XII	–	3000	3 x C lub 2 x D	–	–	Bez ograniczenia	–
XIII	–	4500	2 x D	–	–	Bez ograniczenia	–

Źródło: opracowanie własne.

Systemy alarmowe powinny odpowiadać zagrożeniom Z3 (tabela 15), czyli należeć do klasy S3. Oznacza to, że wyposażone być muszą w czujki wykrywające próby przedostania się, bądź obecność osób niepowołanych, które nie mogą być zneutralizowane nawet za pomocą specjalnie konstruowanych narzędzi. Próba manipulowania przy nich wywołuje stan alarmowania. Monitorowane jest także występowanie przerw i zwarć w torach kablowych nie rzadziej niż co sekundę, a uszkodzenia sygnalizowane po nie więcej niż 20 sekundach. Systemy muszą posiadać podwyższoną odporność na zakłócenia elektromagnetyczne. Centrum odbiorcze powinno odbierać sygnały poprzez tory monitorowane. Gwarantują też ochronę przed osobami niepowołanymi przez całodobową, przeciwsabotażową kontrolę urządzeń systemu. Dostęp do sterowania systemami jest zróżnicowany w zakresie funkcjonalnym dla różnych służb i zapewniony poprzez manipulatory szyfrowe, wyposażone w systemy zapobiegania symulowaniu sygnałów kontrolnych.

Kontrola działania systemów alarmowych klasy S3 musi być dokonywana corocznie w pełnym zakresie, a naprawy podjęte w czasie nie dłuższym niż 4 godziny.

Istotnym aspektem ochrony fizycznej jest zabezpieczenie przed pożarem. Choć każde przedsiębiorstwo zobligowane jest prawnie do przestrzegania przepisów BHP i przeciwpożarowych, to szczególną uwagę zwrócić należy na serwerownie, które z racji gęstego upakowania dużej liczby urządzeń zasilanych energią elektryczną na stosunkowo małej powierzchni są wyjątkowo mocno zagrożone pożarem. Ze względu na wartość danych, a także samego sprzętu, warto wyposażyć ją w dodatkowy, zaawansowany system przeciwpożarowy.

Systemy przeciwpożarowe można podzielić na trzy grupy:

- systemy odcięcia ognia,
- bierne zabezpieczenia antypożarowe,
- systemy detekcji i gaszenia pożaru[157].

Systemy odcięć ogniowych to stosunkowo drogie rozwiązania stosowane w dużych budynkach, polegające na podziale pomieszczeń na strefy, które można w sposób automatyczny odizolować od siebie za pomocą przegród ognioodpornych i dymoszczelnych.

[157] R. Pawlak, *Okablowanie strukturalne sieci. Teoria i praktyka*, Helion, Gliwice 2008.

W skład biernych zabezpieczeń antypożarowych wchodzą ognioodporne ściany i drzwi, pozwalające powstrzymać przez pewien czas rozprzestrzenianie się ognia.

Systemy detekcji i gaszenia pożaru składają się z czujek reagujących na dym, temperaturę lub płomień, przekazujących informację do centrali alarmowej, która sygnalizuje wystąpienie pożaru oraz załącza urządzenia gaśnicze. Ze względu na występujące w serwerowniach urządzenia elektryczne i mechaniczne, jako czynniki gaśnicze zastosowane mogą być jedynie gazy. Są to zazwyczaj gazy obojętne, mające za zadanie obniżenie stężenia tlenu podtrzymującego spalanie, lub gazy halogenopodobne, absorbujące ciepło. Obecnie najczęściej wykorzystywany jest gaz HFC-227ea, uważany za w pełni obojętny dla środowiska i bezpieczny dla elektroniki.

O tym, jak ważne jest niszczenie danych, świadczą badania przeprowadzone w roku 2005 przez Uniwersytet Wrocławski, na zlecenie firmy Fellowes Polska. Badaniami objęto 146 firm, spośród których 95% odpowiedziało, że niszczy lub archiwizuje dokumenty zawierające poufne dane. Tymczasem 44% przeszukanych worków ze śmieciami zawierało dokumenty, które w 52% przypadków zawierały możliwe do odczytania dane i poufne informacje[158].

Wspomniane już Rozporządzenie Rady Ministrów z 18 października 2005 roku szczegółowo określa sposób postępowania z dokumentacją papierową. Można ją zniszczyć przekazując wyspecjalizowanym firmom posiadającym odpowiednie uprawnienia lub stosując odpowiednie niszczarki, rozdrabniające dokumenty zgodnie z normą DIN 32757 (tabela 17).

„W październiku 2012 roku Deutsches Institut für Normung opublikował nową normę dotyczącą niszczenia, DIN 66399:2012. W stosunku do swej poprzedniczki DIN 32757, nowa norma reguluje zarówno proces niszczenia dokumentów, jak i nośników danych. Projekt standardu opracował niemiecki komitet techniczny Standards Committee for Information Technology and Applications. Normę tę wykorzystują producenci urządzeń i systemów niszczących”[159].

[158] M. Engelmann, *Bezpieczeństwo informacji – bezpieczeństwo fizyczne*, „Boston IT Security Review” 2007, nr 3, tom 4.

[159] A. Guzik, *Nowy standard niszczenia dokumentów i nośników danych – DIN 66399*, „Człowiek i dokumenty” 2015, nr 37, http://www.pwpw.pl/kwartalnik_biezacy_numer.html?print=1&id=45&magCid=227.

Tabela 17. Wymagany sposób niszczenia dokumentów wg normy DIN 32757

Klasa tajności	Dokumenty	Wymagania
I	Materiały ogólne, korespondencja	długość nielimitowana, powierzchnia ogółem ≤ 2000 mm *szatkowanie paskowe max 12 mm*
II	Korespondencja wewnętrzna	długość nielimitowana, powierzchnia ogółem ≤ 800 mm *szatkowanie paskowe max 6 mm*
II	Materiały poufne	powierzchnia ogółem ≤ 594 mm, szerokość paska ≤ 4 mm, długość ≤ 80 mm powierzchnia ogółem ≤ 320 mm *szatkowanie paskowe max 2 mm,* *szatkowanie paskowo-odcinkowe max 4* x *60 mm*
IV	Materiały tajne	szerokość paska ≤ 2 mm, długość ≤ 15 mm powierzchnia ogółem ≤ 30 mm *szatkowanie paskowo-odcinkowe max 2* x *15 mm*
V	Materiały ściśle tajne, najwyższego utajnienia	długość ≤ 13 mm, powierzchnia ogółem ≤ 10 mm *szatkowanie paskowo-odcinkowe max 0,8* x *12 mm*

Źródło: DIN 32757-2, Office machines; destruction of information media; machines and devices; minimum informations, Deutsches Institut für Normung, Berlin 1985.

Dane zapisane w postaci cyfrowej niszczyć można programowo lub mechanicznie. Niszczenie programowe polega na wielokrotnym nadpisaniu wszystkich bitów danych na nośniku przypadkowymi ciągami znaków. Skuteczność metody rośnie wraz z liczbą zapisów. Metoda jest więc bardzo czasochłonna, ale nośniki nadają się do ponownego użycia. Nie jest możliwa do zastosowania w przypadku częściowo uszkodzonego nośnika (np. układów elektronicznych lub mechanicznych twardych dysków)[160].

Czynniki pozwalające na mechaniczne usunięcie danych to:

- temperatura – wyższa od temperatury Curie, powyżej której ferromagnetyk traci właściwości magnetyczne, stając się paramagnetykiem,
- silne pole magnetyczne – generowane przez urządzenie zwane degausserem,
- fizyczne zniszczenie powierzchni nośnika – mechaniczne lub za pomocą kwasu.

[160] P. Odor, *Nieodwracalne niszczenie danych*, „NEXT" 2009, nr 1.

Rozdział 8. Rejestracja zbiorów danych osobowych

Obowiązek rejestracji zbiorów danych osobowych w ogólnopolskim, jawnym rejestrze prowadzonym przez GIODO, spoczywa na administratorze danych. Dotyczy wszystkich zbiorów, za wyjątkiem ściśle zdefiniowanych w art. 43 ust. 1 i 1a. UODO zbiorów, które:

- zawierają informacje niejawne,
- obejmują informacje uzyskane w wyniku czynności operacyjno-rozpoznawczych przez funkcjonariuszy organów uprawnionych do tych czynności,
- przetwarzane są przez właściwe organy dla potrzeb postępowania sądowego oraz na podstawie przepisów o Krajowym Rejestrze Karnym,
- przetwarzane są przez Generalnego Inspektora Informacji Finansowej,
- przetwarzane są przez właściwe organy na potrzeby udziału Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym,
- przetwarzane są przez właściwe organy na podstawie przepisów o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej,
- dotyczą osób należących do kościoła lub innego związku wyznaniowego o uregulowanej sytuacji prawnej, przetwarzanych na potrzeby tego kościoła lub związku wyznaniowego,
- przetwarzane są w związku z zatrudnieniem u administratora danych osobowych, świadczeniem na jego rzecz usług, a także u niego zrzeszonych,
- dotyczą osób korzystających z usług medycznych świadczonych przez administratora danych osobowych, obsługi notarialnej, adwokackiej, radcy prawnego, rzecznika patentowego, doradcy podatkowego lub biegłego rewidenta,

- tworzone są na podstawie przepisów dotyczących wyborów do Sejmu, Senatu, Parlamentu Europejskiego, rad gmin, rad powiatów i sejmików województw, wyborów na urząd Prezydenta Rzeczypospolitej Polskiej, na wójta, burmistrza, prezydenta miasta oraz dotyczące referendum ogólnokrajowego i referendum lokalnego,
- dotyczą osób pozbawionych wolności na podstawie ustawy, w zakresie niezbędnym do wykonania tymczasowego aresztowania lub kary pozbawienia wolności,
- przetwarzane są wyłącznie w celu wystawienia faktury, rachunku lub prowadzenia sprawozdawczości finansowej,
- są powszechnie dostępne,
- przetwarzane są w celu przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego,
- przetwarzane są w zakresie drobnych bieżących spraw życia codziennego,
- przetwarzane są w zbiorach prowadzonych bez wykorzystania systemów informatycznych, z wyjątkiem zbiorów zawierających dane wrażliwe.

Zgłoszenie zbioru do rejestracji odbywa się poprzez złożenie lub przesłanie wypełnionego formularza opatrzonego podpisem osoby uprawnionej, którego wzór został opublikowany w Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 11 grudnia 2008 roku w sprawie wzoru zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych[161] (załącznik nr 4). Osoba reprezentująca administratora winna być wpisana do właściwego rejestru albo upoważniona treścią pełnomocnictwa, które należy dołączyć do zgłoszenia.

Wniosek o wpisanie zbioru do rejestru zbiorów danych osobowych zawiera przede wszystkim dane administratora danych, opis wymaganych i stosowanych środków technicznych i organizacyjnych służących ochronie przetwarzanych danych osobowych oraz informacje o:

- celu i zakresie przetwarzania danych,
- kategorii osób, których dane dotyczą,

[161] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, Dz.U. z 2008 r., Nr 229, poz. 1536.

- sposobie zbierania oraz udostępniania danych,
- odbiorcach lub kategoriach odbiorców, którym dane mogą być przekazywane,
- ewentualnym przekazywaniu danych do państwa trzeciego.

Wypełnienie wspomnianego formularza wspomagane jest poprzez odpowiednią funkcjonalność serwisu e-GIODO, dostępną pod adresem internetowym: https://egiodo.giodo.gov.pl/formular_step0.dhtml (rys. 18). Serwis ten umożliwia również elektroniczną rejestrację, pod warunkiem iż wypełniony w systemie wiosek zostanie podpisany podpisem elektronicznym lub profilem zaufanym. Niezwłocznie po zarejestrowaniu oraz na żądanie GIODO wydaje administratorowi danych zaświadczenie o zarejestrowaniu zbioru.

Rys. 18. Rejestracja zbioru danych w serwisie e-GIODO

Źródło: portal e-GIODO.

Administrator danych może rozpocząć ich przetwarzanie bezpośrednio po zgłoszeniu zbioru do rejestracji. Wyjątkiem są zbiory zawierające dane wrażliwe. Administrator wstrzymuje się z ich przetwarzaniem do chwili zarejestrowania zbioru.

Rejestracji podlegają także zmiany informacji zawartych we wniosku. Należy je zgłosić w terminie 30 dni od daty ich wystąpienia. Przepis ten zawiera pewne niebezpieczeństwo, na które ustawodawca zwrócił uwagę w art. 41 ust. 3. Jeżeli zmiana dotyczy rozszerzenia zakresu przetwarzanych danych o dane wrażliwe, konieczne jest powiadomienie GIODO przed jej dokonaniem i oczekiwanie na decyzję o rejestracji. Decyzja ta może zapaść nawet po kilku miesiącach po przesłaniu wniosku.

GIODO może odmówić rejestracji zbioru, która to czynność jest decyzją administracyjną, nakazując ograniczenie przetwarzania wszystkich albo niektórych kategorii danych wyłącznie do ich przechowywania lub przywrócenie stanu zgodnego z prawem. Przyczyny odmowy rejestracji to:

- nieprawidłowe wypełnienie formularza wniosku,
- przetwarzanie danych niezgodne z zasadami,
- niespełnienie podstawowych warunków technicznych i organizacyjnych przez urządzenia i systemy informatyczne służące do przetwarzania zbioru danych zgłoszonego do rejestracji.

Administrator danych, po usunięciu wad, może ponownie zgłosić zbiór do rejestracji, jednakże musi się wstrzymać z przetwarzaniem zawartych w nim danych do chwili pozytywnej decyzji GIODO.

Z obowiązku rejestracji zbiorów danych osobowych zwolnieni są administratorzy danych, którzy wyznaczyli i zgłosili do GIODO administratorów bezpieczeństwa informacji. Nadal jednak muszą rejestrować zbiory zawierające informacje wrażliwe. Pozostałe zbiory administrator bezpieczeństwa informacji, zgodnie z Rozporządzeniem Ministra Administracji i Cyfryzacji z 11 maja 2015 roku[162], ewidencjonuje w prowadzonym przez siebie rejestrze. Rejestr ten, formie papierowej lub elektronicznej, stanowi wykaz prowadzonych zbiorów, wraz z następującymi informacjami dotyczącymi każdego z nich:

[162] Rozporządzenie Ministra Administracji i Cyfryzacji z 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych, Dz.U. z 2015 r., poz. 719.

- nazwa zbioru danych,
- oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania,
- numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został administratorowi danych nadany,
- oznaczenie przedstawiciela administratora danych wyznaczonego dla podmiotów mających siedzibę albo miejsce zamieszkania w państwie trzecim, adres jego siedziby lub miejsca zamieszkania,
- oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi,
- podstawa prawna upoważniająca do prowadzenia zbioru danych,
- cel przetwarzania danych w zbiorze,
- opis kategorii osób, których dane są przetwarzane w zbiorze,
- zakres danych przetwarzanych w zbiorze,
- sposób zbierania danych do zbioru,
- sposób udostępniania danych ze zbioru,
- oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane,
- informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego.

Dodatkowo dla każdego zbioru w rejestrze umieszcza się datę wpisu oraz datę ostatniej aktualizacji. Prowadzona jest też historia zmian w rejestrze, zawierająca informację o rodzaju zmiany (nowy wpis, aktualizacja, wykreślenie), datę dokonania oraz informację o jej zakresie. W przypadku zaprzestania przetwarzania danych ze zbioru, administrator wykreśla ją ze zbioru, pozostawiając jedynie nazwę, datę wpisania do rejestru oraz datę ostatniej aktualizacji, z adnotacją, że jest to data wykreślenia.

Administrator danych może rozpocząć przetwarzanie danych ze zbioru bezpośrednio po rejestracji w prowadzonym przez ABI rejestrze. Fakt dokonania zmian danych podlegających rejestracji skutkuje ich aktualizacją w rejestrze bezpośrednio po ich zaistnieniu.

Administrator bezpieczeństwa informacji udostępnia treść rejestru do przeglądania każdemu zainteresowanemu. Jeśli rejestr prowadzony jest

w postaci papierowej, udostępnienie następuje w siedzibie lub miejscu zamieszkania administratora danych.

Rejestr prowadzony w sposób elektroniczny należy udostępnić na stronie internetowej administratora danych, przy czym na stronie głównej umieszcza się odwołanie umożliwiające bezpośredni dostęp do rejestru. Jako alternatywa, przewidywana jest możliwość udostępniania, na stanowisku dostępowym w systemie informatycznym administratora, danych znajdującym się w siedzibie lub miejscu zamieszkania tego administratora lub przez sporządzenie wydruku rejestru z systemu informatycznego administratora danych.

W stosunku do rejestrów prowadzonych jedynie w sposób elektroniczny, jak również rejestrów prowadzonych w sposób mieszany – papierowo i elektronicznie – administrator bezpieczeństwa może podjąć decyzję o ograniczeniu udostępnienia informacji związanej z powierzeniem przetwarzania zbioru innemu podmiotowi. W sposób elektroniczny udostępnia się wtedy jedynie nazwę podmiotu zaś pozostałe dane – adres jego siedziby lub miejsca zamieszkania – dostępne są do przeglądania każdemu zainteresowanemu w siedzibie lub miejscu zamieszkania administratora danych.

Należy zwrócić uwagę na dość istotną wadę wprowadzanych przepisów. Nie przewidują one szczegółowych rozwiązań dla zbiorów zarejestrowanych wcześniej w rejestrze prowadzonym przez Generalnego Inspektora Danych Osobowych. Nie mogą one być z niego wykreślone, gdyż według przepisów ustawy o ochronie danych osobowych, wykreślenie z rejestru zbiorów danych osobowych jest dokonywane w drodze decyzji administracyjnej, jeżeli zaprzestano przetwarzania danych w zarejestrowanym zbiorze lub rejestracji dokonano z naruszeniem prawa. Możliwe jest więc, że ten sam zbiór będzie zarejestrowany w zbiorze GIODO oraz w zbiorze prowadzonym przez administratora danych osobowych. Ponieważ problem jest znany, co przyznali pracownicy GIODO podczas konferencji „Ochrona danych osobowych – najnowsze krajowe i europejskie regulacje prawne" 28 stycznia 2015 roku, należy spodziewać się następnych zmian prawnych.

Prawidłowe prowadzenie i udostępnianie rejestru w przypadku większej liczby zmieniających się zbiorów to czynność kłopotliwa dla administratora. Powstaje już oprogramowanie, tworzone przez autora niniejszej pracy, które wspomoże ABI w prowadzeniu pełnej dokumentacji zgodnie z ustawą

o ochronie danych osobowych oraz aktów wykonawczych. Obecnie posiada ono pełną funkcjonalność rejestru zbiorów danych osobowych. System RejestrABI dostępny jest pod adresem internetowym https://rejestrabi.pl/.

Wygląd jednego z ekranów przedstawiony został na rysunku 19.

Rys. 19. Wygląd systemu RejestrABI

Źródło: portal RejestrABI, https://rejestrabi.pl/.

Rozdział 9. Nowe trendy w przetwarzaniu danych osobowych

9.1. Projektowane rozwiązania

Niezależnie od zmian prawnych wprowadzonych do UODO na początku 2015 roku oraz kontynuowanych w rozporządzeniach Ministerstwa Administracji i Cyfryzacji, przepisy i zalecenia dotyczące przetwarzania danych osobowych muszą sprostać nowym wyzwaniom. Jednym z nich jest ochrona przed omawianym na wstępie zjawiskiem spamu. W kwietniu 2015 roku Polskie Stowarzyszenie Marketingu SMB, we współpracy z UOKiK i GIODO, umożliwiło w prowadzonym przez siebie systemie, zwanym Listą Robinsonów, zastrzeżenie swojego adresu zamieszkania, adresu e-mail czy numeru telefonu stacjonarnego i komórkowego przed wykorzystaniem ich do działalności marketingowej. Pomysł nie jest nowatorski, gdyż podobne systemy, zwane także Mailing Preference Service, Telephone Preference Service czy Do-not-call lists, funkcjonują na całym świecie, a w niektórych krajach wymóg ich stosowania przez przedsiębiorców przy realizacji kampanii marketingowych jest obligatoryjny.

Poważne zaniepokojenie, wyrażone także w opinii wspominanej już Grupy Roboczej Art. 29, wzbudza zjawisko profilowania[163]. Jest to zbieranie i kategoryzowanie informacji odnoszących się do poszczególnych osób oraz generowanie na ich podstawie uzupełniających danych, tworząc tym samym tzw. profil osobowościowy. Wykorzystywane jest między innymi do podejmowania decyzji w kwestii udzielania kredytów czy ustalania stawek ubezpieczenia. Profilowanie oparte jest na metodach statystycznych, które z definicji obarczone są pewnym błędem. Trwające prace i dyskusje mają na celu opracowanie definicji profilowania, zagwarantowania obywatelom

[163] Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, ARTICLE 29 Data Protection Working Party, Brussels, 13 maja 2013 r.

dostępu do informacji składających się na ich profil i możliwości ich korygowania oraz odwoływania się od automatycznie podejmowanych na jego podstawie decyzji. Grupa Robocza Art. 29 naciska, wbrew opinii Komisji Europejskiej, aby nowo opracowane przepisy odnosiły się do samego zjawiska profilowania, a nie do jego skutków.

Szerzący się na świecie terroryzm i związany z walką z nim dostęp służb specjalnych do danych osobowych rodzi pytanie o granicę pomiędzy poczuciem bezpieczeństwa a prywatnością. Jednym z ważnych podejmowanych tematów jest wykorzystywanie danych pasażerów lotów. Zdaniem doktora Wojciecha Wiewiórowskiego:

> „Rzecznicy ochrony danych osobowych nie są przeciwni PNR jako samemu systemowi czy zbieraniu tych danych, bo one i tak są zbierane. Natomiast jeżeli chodzi o gromadzenie ich w bazach, które miałyby być powszechnie przetwarzane przez służby i przez policję, to należy wykazać dużą ostrożność"[164].

Ministerstwo Spraw Wewnętrznych opracowało projekt rozporządzenia Ministra Spraw Wewnętrznych w sprawie przetwarzania informacji przez policję[165]. Jest on w dużej mierze zgodny z przepisami UODO. Dodatkowo wskazuje na konieczność i sposób usuwania danych ze zbiorów.

W przyszłości wszystkie ustawy o ochronie danych osobowych państw członkowskich UE mają być zastąpione przez rozporządzenie. Wszelkie odmienności w zakresie ochrony danych w policji i wymiarze sprawiedliwości uregulowane zostaną uzupełniającą dyrektywą. Ujednolicenie przepisów ochrony danych osobowych pozwoli między innymi na wprowadzenie zasady „*one stop shop*", która zapewnia, iż spełnienie wymagań w jednym z krajów członkowskich jest wystarczające dla administratora działającego na terenie UE.

Projektowane przepisy mają zmienić fakt mówiący o tym, iż „Internet nigdy nie zapomina". Trybunał Sprawiedliwości Unii Europejskiej orzekł,

[164] W. Wiewiórowski, wypowiedź na forum GoldenLine w temacie Zbiór danych w elektronicznym obiegu, op. cit.

[165] Projekt rozporządzenia Ministra Spraw Wewnętrznych w sprawie przetwarzania informacji przez Policję z 18 listopada 2014 r., http://bip.msw.gov.pl/bip/projekty-aktow-prawnyc/2014/23298,Projekt-rozporzadzenia-Ministra-Spraw-Wewnetrznych-w-sprawie-przetwarzania-infor.html.

że prawa osoby, której dotyczą dane, są co do zasady nadrzędne wobec interesu internautów[166]. Przyznał, iż operator wyszukiwarki internetowej przetwarza dane osobowe i jest ich administratorem. Powinien więc w określonych sytuacjach usuwać z wyników odnośniki do stron internetowych zawierających informacje o osobie, której imię i nazwisko zostało użyte jako parametr wyszukiwania. Ponieważ definicja danych osobowych jest dużo szersza niż imię i nazwisko, wyrok Trybunału nie odnosi się w sposób holistyczny do ochrony danych osobowych w Internecie. Stawia jednak pod znakiem zapytania przyszłe funkcjonowanie wyszukiwarek internetowych.

Rozporządzenie wprowadzić ma również konieczność zgłaszania incydentów związanych z naruszeniem danych osobowych. Pozwoli on ugruntować pozycję na rynku solidnych, dbających o bezpieczeństwo administratorów danych, jak również podjąć niezbędne działania ograniczające skutki incydentu.

Szczególnie wymagający obowiązek, który spadnie na administratorów danych, to przeprowadzenie analiz szczególnego ryzyka wraz z oceną skutków w zakresie ochrony danych osobowych.

9.2. Analiza ryzyka

Analiza ryzyka jest istotną częścią modelowania systemu zarządzania bezpieczeństwem informacji. Opiera się na określeniu oraz oszacowaniu prawdopodobieństwa, a także skutków wystąpienia niepożądanego zdarzenia. Pozwala ustalić jakościowy i ilościowy poziom ryzyka, a także dobrać odpowiednie działania zapobiegawcze, które umożliwią eliminację ryzyka, jego kontrolowanie i minimalizację efektów. Analiza ryzyka przewiduje podział ryzyka na kategorie i odpowiadające im czynności przeciwdziałania.

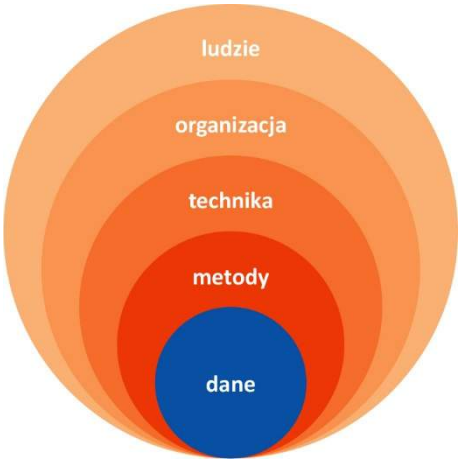
Terminologia używana w analizie ryzyka bezpieczeństwa systemów informacyjnych wywodzi się z wielu gałęzi wiedzy, począwszy od psychologii, poprzez naukę o zarządzaniu, a na informatyce kończąc. Często zachodzi więc mylna interpretacja pojęć związanych z tym tematem.

Klasycznym tego przykładem jest „system informacyjny", utożsamiany nieprawidłowo z systemem informatycznym. System to zbiór elementów

[166] Orzeczenie Trybunału Sprawiedliwości Unii Europejskiej z 13 maja 2014 roku w sprawie C-131/12, ECLI:EU:C:2014:317.

i zachodzących między nimi relacji[167]. Informacja jest tymczasem abstrakcyjnym pojęciem, które oznacza czynnik zmniejszający entropię[168]. Czy można więc przyjąć definicję systemu informacyjnego jako posiadającą wiele poziomów strukturę pozwalającą użytkownikowi na przetwarzanie, za pomocą procedur i modeli, informacji wejściowych w wyjściowe[169]? Przetwarzanie informacji jest związane z procesami myślowymi, tymczasem definicja nie obejmuje czynnika ludzkiego. Systemy sztuczne (ang. *artefact*) przetwarzają dane, czyli fizyczną reprezentację informacji[170].

Pełniejszą definicję zaproponował w 1977 roku Wilhelm Steinmüller[171], według której system informacyjny to system społeczny (ang. *Human activity*), który współtworzą elementy przynależne do pięciu klas, pokazanych na rysunku 20.



Rys. 20. Elementy systemu informacyjnego

Źródło: opracowanie własne.

[167] M. Mazur, *Pojęcie systemu i rygory jego stosowania*, „Postępy Cybernetyki" 1987, z. 2.
[168] S. Alter, *A General, yet Useful Theory of Information Systems*, "Communications of the Association for Information Systems" 1999, Vol. 1., Article 13.
[169] J. Kisielnicki, H. Sroka, *Systemy informacyjne biznesu. Informatyka dla zarządzania*, Placet, Warszawa 2005.
[170] B. Langefors, *Theoretical Analysis of Information Systems*, 4th ed., Auerbach Publishers, Lund–Philadelphia 1973.
[171] W. Steinmüller, *Zautomatyzowane systemy informacyjne w administracji prywatnej i publicznej*, „Organizacja – Metoda – Technika" 1977, nr 9.

Często spotyka się również stwierdzenie, iż system informacyjny jest wielopoziomową strukturą, pozwalającą użytkownikowi na przetwarzanie – za pomocą procedur i modeli – informacji wejściowych w wyjściowe. System informatyczny jest wydzieloną, skomputeryzowaną, jego częścią. Cechy odróżniające system informacyjny od informatycznego zostały pokazane w tabeli 18.

Tabela 18. Cechy systemów informacyjnych i informatycznych

Cecha	SI – system informacyjny	SIT – system informatyczny
Dziedzina	Informacja jako istotny czynnik Układy przetwarzające i przesyłające	Dane rejestrowane, przesyłane, przechowywane, wyszukiwane, przetwarzane, prezentowane, (...) dostarczane odbiorcom
Cele działania, tworzone wyjścia	Informacja dla każdego członka organizacji, cele operacyjne w oparciu o potrzeby zarządzających	Struktury danych wynikowych, przyjętych dotychczas raportów
Klasa systemu	System działalności ludzkiej (*Human activity system*) – system społeczny	System sztuczny (artefakt)
Składniki	Ludzie, systemy sztuczne (dane, środki techniczne) i systemy abstrakcyjne (metody, organizacja)	Systemy sztuczne (artefakty) – dane, metody i systemy abstrakcyjne
Klasa rozwiązywanych problemów	Typowe problemy zarządzania, problemy organizacyjne	Dobrze ustrukturyzowane, problemy informatyków sformułowane według potrzeb odbiorców danych
Metoda badania, analizy i tworzenia systemu	Różnorodność metod, dotychczas przewaga metod twardych, wzrastająca świadomość potrzeby stosowania miękkiego podejścia	Twarde metody
Właściciel systemu	Najwyższe kierownictwo	Szef SIT i kierownicy liniowi
Potrzeby	Potrzeba zapewnienia informacji	Potrzeba wykonania przypisanych zadań
Dane	Wszystkie dane przydatne dla odbiorcy	Dane zidentyfikowane wg wzorca starej organizacji
Techniki	Wszelkie techniki odpowiednie do przystosowania danych do ich spożytkowania przez odbiorców	TI czyli technika komputerowa
Metody	Wszelkie metody przydatne do zapewniania informacji	Metody ilościowe wspomagane przez technikę komputerową

Technologia	Wszelkie techniki, okablowanie / systemy / komputery / …, przystosowane do potrzeb osi	Techniki komputerowe i jako uzupełnienie dostępne techniki obliczeniowe
Organizacja	Nowa organizacja podporządkowana celom wynikającym z celów organizacji jako całości	Organizacja odziedziczona, do której dostosowuje się Organizacyjny System Informatyczny
Ludzie	Ludzie przystosowujący się do nowych celów / potrzeb / wymagań adaptującej się organizacji	Ludzie przyuczający się nowych rozwiązań technicznych
Rola człowieka	Człowiek jako część składowa SI jest świadomym i odpowiedzialnym jego czynnikiem	Człowiek traktowany jako element techniczny

Źródło: M. Kuraś, *System informacyjny – system informatyczny. Co poza nazwą różni te dwa obiekty?*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2005, nr 770, http://www.uci.agh.edu.pl/uczelnia/tad/PSI11/art/SI-vs-SIT.pdf.

Kolejnym wartym sprecyzowania terminem jest bezpieczeństwo. Według słownika nauk społecznych pojęcie to jest tożsame z pewnością braku zagrożenia fizycznego albo ochroną przed nim[172]. Definicja ta, ze względu na swą szczegółowość, jest mało użyteczna dla potrzeb niniejszej pracy.

Bardziej ogólną podaje politolog, Jerzy Stańczyk: „Bezpieczeństwo to stan pewności, spokoju, zabezpieczenia oraz jego poczucia, jak również brak zagrożenia oraz ochrona przed niebezpieczeństwami"[173]. Według filozofa Janusza Świniarskiego istota bezpieczeństwa tkwi w takich formach istnienia, które zapewniają trwanie, przetrwanie i rozwój oraz doskonalenie[174].

Tak rozbieżne definicje świadczą o tym, że bezpieczeństwo jest pojęciem polisemantycznym. Wykorzystywane jest współcześnie w wielu dyscyplinach naukowych, posiada różne znaczenia w zależności od kontekstu użycia. Wiele pozycji encyklopedycznych czy słownikowych uważa bezpieczeństwo za antonim zagrożenia lub odnosi się jedynie do poszczególnych rodzajów bezpieczeństwa.

Przydatną w dalszych rozważaniach okazuje się definicja bezpieczeństwa teleinformatycznego, która określa je jako stopień uzasadnionego zaufania

[172] *A Dictionary of the social sciences*, (eds.) J. Gould, W.L. Kolb, Free Press, London 1964.
[173] J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, ISP PAN, Warszawa 1996, s. 15.
[174] J. Świniarski, *Filozoficzne podstawy edukacji dla bezpieczeństwa*, Egros, Warszawa 1999.

co do tego, że nie zostaną poniesione potencjalne straty wynikające z niepożądanego ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej, przetwarzanej i przesyłanej za pomocą systemu teleinformatycznego[175]. Definicję tę można śmiało uogólnić i stosować do systemów informacyjnych.

Wspomniane zaufanie może być uzasadnione analizą ryzyka. Ryzyko powszechnie utożsamiane jest z niepewnością. Na odmienność tych pojęć zwrócił uwagę Irving Pfeffer:

> „Ryzyko jest kombinacją hazardu i jest mierzone prawdopodobieństwem; niepewność jest mierzona przez poziom wiary. Ryzyko jest stanem świata; niepewność jest stanem umysłu"[176].

Odmiennego zdania jest Allan Willett, twierdząc, że jest ono zobiektywizowaną niepewnością wystąpienia niepożądanego zdarzenia i zmienia się wraz z niepewnością, a nie ze stopniem prawdopodobieństwa[177].

Nowsze definicje powracają jednak do koncepcji powiązania ryzyka i prawdopodobieństwa. Ministerstwo Finansów w standardach dotyczących przeprowadzania audytów określa ryzyko jako prawdopodobieństwo wystąpienia dowolnego zdarzenia, działania lub zaniechania działania, którego skutkiem może być szkoda w majątku lub wizerunku danej jednostki organizacyjnej lub które może przeszkodzić w osiągnięciu wyznaczonych celów lub zadań[178].

Analiza ryzyka to badanie ryzyka obejmujące określenie charakterystyki obiektu, identyfikację zagrożeń i szacowanie ryzyka[179]. Szersze ujęcie tego terminu znaleźć można w opracowaniu Najwyższej Izby Kontroli. Definiuje ono analizę ryzyka jako proces, którego elementami są:

- identyfikacja,
- oszacowanie,

[175] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Mikom, Warszawa 2008.

[176] I. Pfeffer, *Insurance and economic theory. Pub. for SS Huebner Foundation for Insurance Education*, University of Pennsylvania, Philadelphia 1956, s. 42.

[177] A.H. Willet, *The Economic Theory of Risk Insurance*, Columbia University Press, New York 1951.

[178] K. Czerwiński, *Analiza ryzyka w audycie wewnętrznym*, LINK, Szczecin 2003.

[179] I. Romanowska-Słomka, A. Słomka, *Zarządzanie ryzykiem zawodowym*, wyd. 3, Tarbonus, Tarnobrzeg 2003.

- hierarchizacja pojedynczych zdarzeń (wydarzeń, okoliczności) mogących niekorzystnie wpływać na osiągnięcie określonego celu[180].

W literaturze przedmiotu napotkać można na wiele różnych klasyfikacji zagrożeń bezpieczeństwa informacji. Zagrożenia można podzielić ze względu na lokalizację ich źródła na:

- wewnętrzne (powstające wewnątrz organizacji), obejmujące zagrożenie utratą, uszkodzeniem lub brakiem dostępu do danych spowodowane błędem, przypadkowym albo celowym działaniem nieuczciwych użytkowników,
- zewnętrzne (powstające poza organizacją), które obejmują zagrożenie utratą, uszkodzeniem danych lub pozbawieniem możliwości obsługi przez celowe lub przypadkowe działanie ze strony osób trzecich w stosunku do sieci lub systemu,
- fizyczne, w których utrata, uszkodzenie danych lub brak możliwości obsługi następuje z powodu wypadku, awarii, katastrofy lub innego nieprzewidzianego zdarzenia, wpływającego na system informacyjny, bądź urządzenie sieciowe[181].

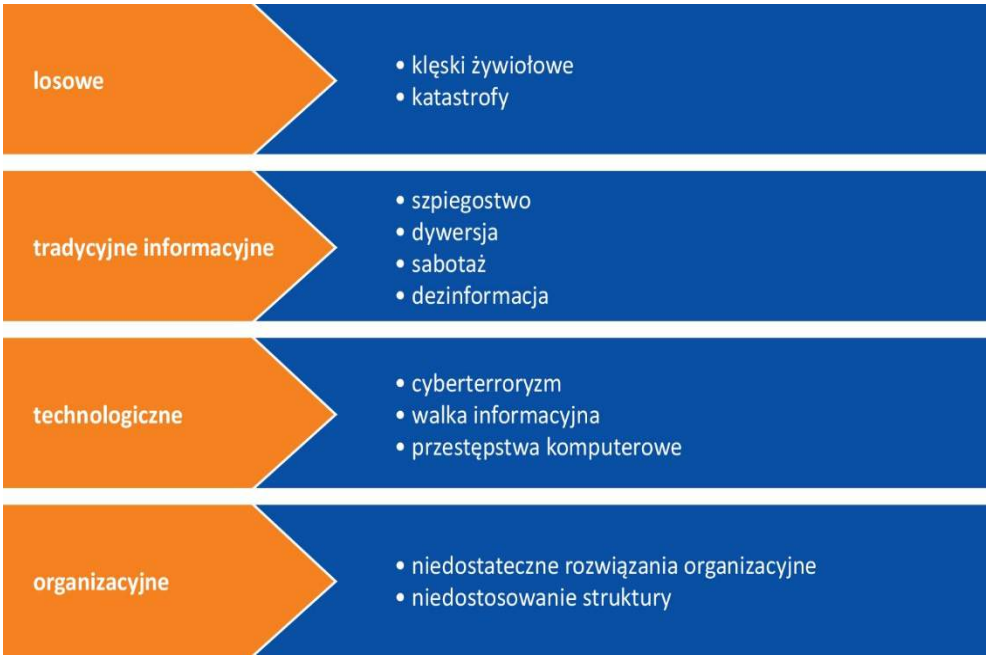
Powyższa klasyfikacja jest obecnie coraz trudniejsza do utrzymania. Współczesne systemy informacyjne, a w szczególności systemy instytucji publicznych, obsługiwane są często przez szeroką rzeszę użytkowników, niezatrudnionych przez organizację, której system jest własnością. Jednakże ze względu na jego przeznaczenie (publiczne) nie można ich nazwać osobami trzecimi. Niesłusznym wydaje się również wydzielenie zagrożenia fizycznego. Jest ono skutkiem działania lub częściej zaniechania działania osób odpowiedzialnych za eksploatację i nadzór nad systemami informacyjnymi. Należy także zwrócić uwagę, iż bezzasadnie dokonano rozdziału systemu informacyjnego oraz urządzeń sieciowych.

Bardziej użyteczna klasyfikacja obejmuje obszary zagrożeń pokazane na rysunku 21. Na jej podstawie trudno jest jednak określić rodzaj zagrożenia, jakim są awarie infrastruktury informatycznej. Przenikają się też wzajemnie obszary tradycyjnych zagrożeń informatycznych oraz technologicznych.

---

[180] *Glosariusz terminów dotyczących kontroli i audytu w administracji publicznej*, Najwyższa Izba Kontroli, Warszawa 2006.

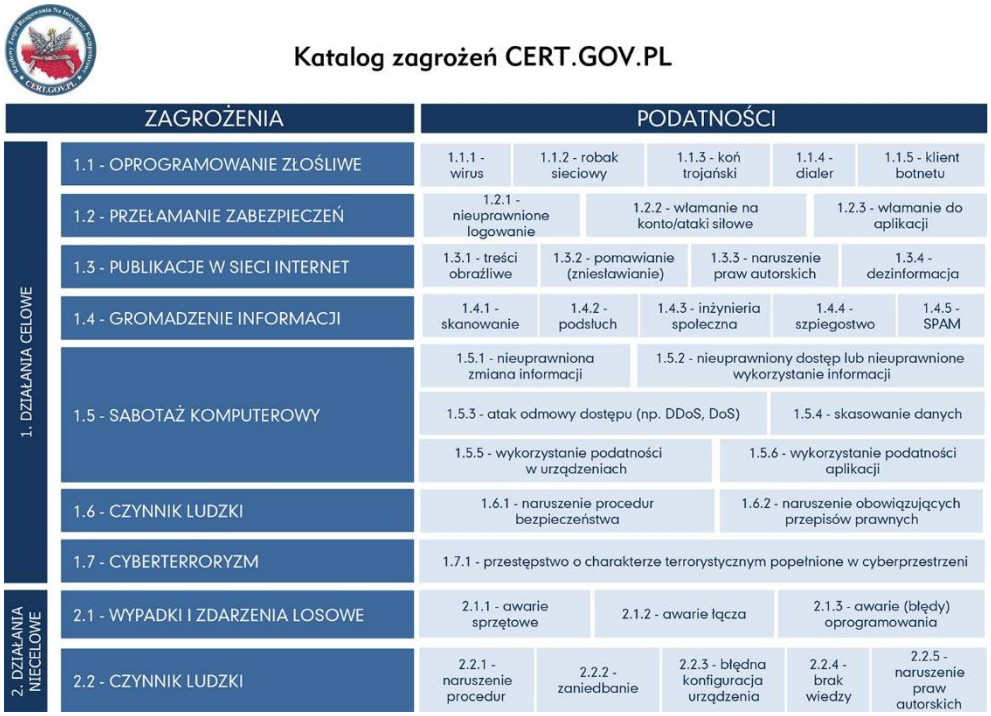
[181] A. Żebrowski, M. Kwiatkowski, *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2000.



Rys. 21. Obszary zagrożeń systemów informacyjnych

Źródło: opracowanie własne.

Warto także polecić katalog zagrożeń stosowany przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, pokazany na rysunku 22. Jest on kompletny, lecz szczegółowa klasyfikacja może być zastosowana jedynie po dogłębnej i skutecznej analizie incydentu.



Rys. 22. Katalog zagrożeń CERT.GOV.PL

Źródło: Katalog zagrożeń stosowany przez CERT.GOV.PL, http://www.cert.gov.pl/cer/publikacje/katalog-zagrozen-stosow/731,Katalog-zagrozen-stosowany-przez-CERTGOVPL.html.

9.3. Metody analizy ryzyka

Metodologie analizy ryzyka systemów informacyjnych zaczęły kształtować się w drugiej połowie XX wieku. Literatura przedmiotu prezentuje wiele przykładów opierających się zarówno na metodach opisowych, jak i wykorzystujących złożone modele matematyczne. Wszystkie jednak podzielić można na 3 podstawowe typy:

- metody ilościowe,
- metody jakościowe,
- metody oparte na rywalizacji.

Ich odpowiedni dobór, w zależności od dostępnych danych, mechanizmów badawczych i charakterystyki badanego systemu, może przesądzić o wiarygodności otrzymanych wyników.

Metody ilościowe (ang. *Quantitative*) wykorzystują miary liczbowe, takie jak określone kwotowo wartości zasobów informatycznych, częstotliwość występowania incydentów czy prawdopodobieństwo ich wystąpienia[182].

Jedną z pierwszych była opublikowana w roku 1975 metoda Courtneya, znana również jako metoda ALE (ang. *Annual Loss Exposure*), gdyż opiera się o wartość oczekiwanej rocznej straty. Parametr *ALE*[183] wyliczany jest ze wzoru:

$$ALE = SLE \cdot ARO$$

gdzie:

SLE (ang. *Single Loss Expectancy*) – wyrażona w walucie oczekiwana roczna strata spowodowana pojedynczym incydentem
ARO (ang. *Annualized Rate of Occurance*) – częstotliwość występowania zdarzenia powodującego stratę.

SLE wyrażone jest wzorem:

$$SLE = AV \cdot RF$$

gdzie:

AV (ang. *Asset Value*) – wartość zasobu
RF (ang. *Exposure Factor*) – procent wartości zasobu, jaki zostanie utracony w wyniku pojedynczego zdarzenia.

Podczas analizy ryzyka metodą Courtneya, do wyliczania ARO w celu uproszczenia, stosuje się jednak następujący wzór:

$$ALE = \frac{10^{f+i-3}}{3}$$

gdzie:

f – indeks częstotliwości zdarzenia
i – indeks wartości straty.

Wartości indeksów częstotliwości zdarzenia i strat przedstawiono w tabeli 19.

[182] E.I. Szczepankiewicz, P. Szczepankiewicz, *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym*, „Audyt" 2006, nr 7.
[183] K. Czerwiński, H. Grocholski, *Podstawy audytu wewnętrznego*, Link, Szczecin 2003.

Tabela 19. Wartości indeksów częstotliwości zdarzenia i strat

Indeks *i*	Częstotliwość zdarzenia	Indeks *f*	Wartość straty
1	Raz na 300 lat	1	10$
2	Raz na 30 lat	2	100$
3	Raz na 3 lata	3	1000$
4	Raz na 100 dni	4	10 000$
5	Raz na 10 dni	5	100 000$
6	Raz dziennie	6	1 000 000$
7	10 razy dziennie	7	10 000 000$
8	100 razy dziennie	8	100 000 000$

Źródło: *Guideline for Automatic Data Processing Risk Analysis*, "Federal Information Processing Standards Publication FIPS 65", National Bureau of Standards, Institute for Computer Sciences and Technology, Gaithersburg 1979.

Podstawową wadą metody Courtneya jest arbitralne wyznaczenie indeksów i oraz f (patrz tabela 19) oraz stosunkowo duża rozpiętość przypisanych im wartości.

Rozwinięciem metody Courtneya w kompletną metodykę projektowania systemów bezpieczeństwa informacji jest metodyka Fishera. Składa się ona z 5 faz:[184]

faza 1 – zebranie informacji,
faza 2 – identyfikacja zagrożeń,
faza 3 – ocena ryzyka,
faza 4 – projektowanie mechanizmów kontrolnych,
faza 5 – analiza ekonomicznej opłacalności.

Innowacyjne podejście Fishera zauważalne jest właśnie w piątej, ostatniej fazie. Wyliczany jest wskaźnik rentowności *ROI* (ang. *Return on Investment*) dla każdego mechanizmu kontrolnego, według wzoru:

$$ROI = \frac{OP}{IC}$$

[184] R. Baskerville, *Information Systems Security Design Methods: Implications for Information Systems Development*, "ACM Computing Surveys" 1993, Vol. 25, No. 4.

gdzie:

OP (ang. *Operating Profit*) – zysk operacyjny,
IC (ang. *Invested Capital*) – zainwestowany kapitał.

Zysk operacyjny interpretowany jest jako wielkość ryzyka, zaś zainwestowany kapitał to koszt mechanizmu kontrolnego.

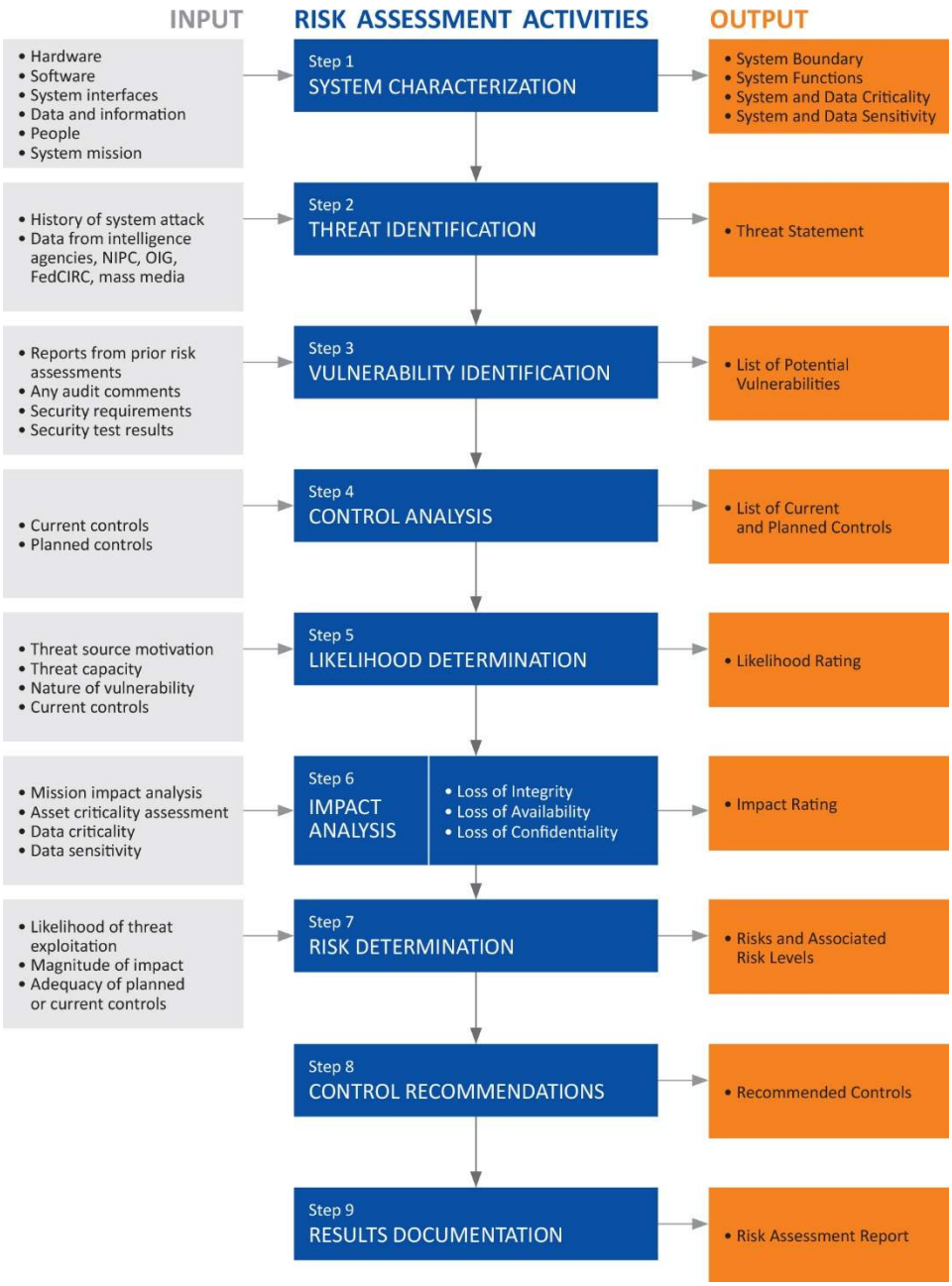
Kolejnym rozwinięciem jest metoda Parkera. Wykorzystuje rozbudowaną macierz analizy zagrożeń (ang. *Exposure Analysis Matrix*). Przy jej konstruowaniu przyjęto założenie, że waga zagrożenia jest funkcją liczby osób, które mogą przyczynić się do powstania straty. Ryzyka analizowane są w podziale na poszczególne grupy zawodowe.

Metody jakościowe prezentują zupełnie inne podejście od prezentowanych w poprzednim podrozdziale metodyk. Jedną z nich jest metodyka NIS 800-30, rekomendowana przez amerykański National Institute of Standards and Technology (NIST). Ryzyko zostało tu zdefiniowane jako funkcja prawdopodobieństwa wykorzystania podatności poszczególnych zagrożeń oraz wielkości wpływu jej wykorzystania. Prawdopodobieństwo zostało sklasyfikowane jako niskie z wagą 0.1, średnie z wagą 0.5 oraz wysokie z wagą 1. Podobnie określono wielkość wpływu wykorzystania podatności, z tym że wagi wynoszą odpowiednio 10, 50 i 100. Przykładowa macierz ryzyka jest pokazana w tabeli 20. Metodyka ta została zaprezentowana na rysunku 23.

Tabela 20. Macierz ryzyka metody NIS 800-30

Prawdopodobieństwo wykorzystania podatności	Wpływ		
	Wysoki (100)	Średni (50)	Niski (10)
Wysokie (1)	1 x 100 = 100	1 x 50 = 50	1 x 10 = 10
Średnie (0,5)	05 x 100 = 50	0,5 x 50 = 25	0,5 x 10 = 5
Niskie (0,1)	0,1 x 100 = 10	0,1 x 50 = 5	0,1 x 10 = 1

Źródło: G. Stoneburner, A. Goguen, A. Feringa, *Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-30, Gaithersburg 2002.



Rys. 23. Schemat blokowy metodyki oceny ryzyka NIS 800-30

Źródło: G. Stoneburner, A. Goguen, A. Feringa, *Risk Management Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology*, op. cit.

Ryzyko wysokie, osiągające wartość powyżej 50, wskazuje, że istnieje duże zapotrzebowanie na środki naprawcze. Istniejący system może nadal działać, ale plan działań naprawczych musi być wprowadzony jak najszybciej. Przy średnim ryzyku, tj. w granicach (10, 50>, działania naprawcze są potrzebne i należy opracować plan włączenia tych działań w rozsądnym terminie. Ryzyko niskie, poniżej 10, wymaga podjęcia przez zarząd decyzji o wprowadzeniu działań naprawczych lub akceptacji ryzyka.

Australijska metodyka analizy ryzyka ASNZS 4360:2004, opracowana przez Australian Capital Territory Insurance Authority (ACTIA), została również przyjęta jako obowiązująca w Federacji Europejskich Managerów do spraw Ryzyka FERMA (ang. *Federation of European Risk Management Associations*).

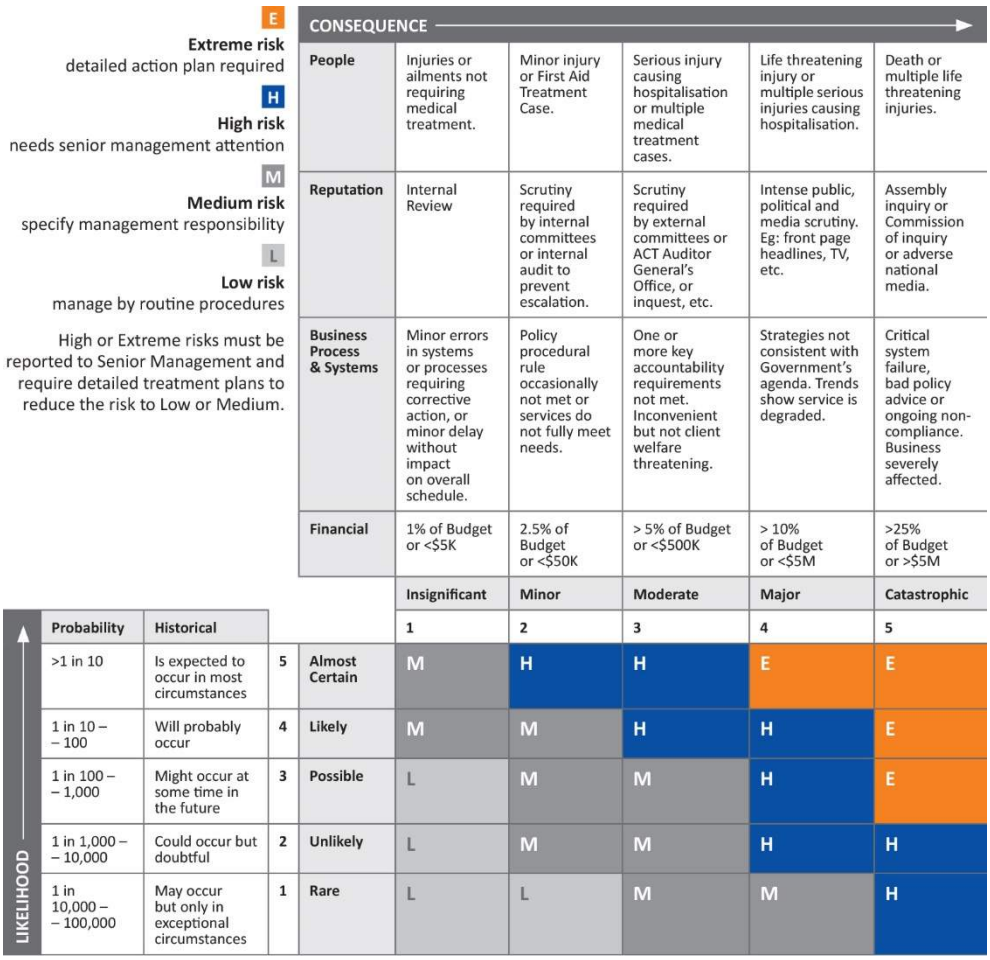
Wyróżnia się w niej 7 faz:

1. Ustalenie zakresu analizy.
2. Identyfikacja ryzyka.
3. Analiza ryzyka.
4. Szacowanie ryzyka.
5. Zapobieganie lub zarządzanie ryzykiem.
6. Monitorowanie i przeglądy.
7. Konsultacje[185].

Identyfikacja ryzyka polega na odpowiedzi na pytania: kiedy, gdzie i jak mogą wystąpić zagrożenia założonych przez nas celów. Jakie są zagrożenia związane z realizacją każdego z naszych priorytetów, jakie jest ryzyko nieosiągnięcia tych priorytetów oraz kto uczestniczy w ich realizacji?

Każdemu zidentyfikowanemu ryzyku przypisywane jest źródło i skutek. Określa się też efektywność mechanizmów kontrolnych, poziom ryzyka oraz akceptowalność, za pomocą macierzy ryzyka, co ilustruje rysunek 24 na następnej stronie.

[185] *Risk Management Toolkit*, Australian Capital Territory Insurance Authority, Canberra 2004.



E **Extreme risk**
detailed action plan required

H **High risk**
needs senior management attention

M **Medium risk**
specify management responsibility

L **Low risk**
manage by routine procedures

High or Extreme risks must be reported to Senior Management and require detailed treatment plans to reduce the risk to Low or Medium.

	CONSEQUENCE →				
People	Injuries or ailments not requiring medical treatment.	Minor injury or First Aid Treatment Case.	Serious injury causing hospitalisation or multiple medical treatment cases.	Life threatening injury or multiple serious injuries causing hospitalisation.	Death or multiple life threatening injuries.
Reputation	Internal Review	Scrutiny required by internal committees or internal audit to prevent escalation.	Scrutiny required by external committees or ACT Auditor General's Office, or inquest, etc.	Intense public, political and media scrutiny. Eg: front page headlines, TV, etc.	Assembly inquiry or Commission of inquiry or adverse national media.
Business Process & Systems	Minor errors in systems or processes requiring corrective action, or minor delay without impact on overall schedule.	Policy procedural rule occasionally not met or services do not fully meet needs.	One or more key accountability requirements not met. Inconvenient but not client welfare threatening.	Strategies not consistent with Government's agenda. Trends show service is degraded.	Critical system failure, bad policy advice or ongoing non-compliance. Business severely affected.
Financial	1% of Budget or <$5K	2.5% of Budget or <$50K	> 5% of Budget or <$500K	> 10% of Budget or <$5M	>25% of Budget or >$5M
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
	1	**2**	**3**	**4**	**5**

LIKELIHOOD ↑	Probability	Historical							
	>1 in 10	Is expected to occur in most circumstances	5	**Almost Certain**	M	H	H	E	E
	1 in 10 – – 100	Will probably occur	4	**Likely**	M	M	H	H	E
	1 in 100 – – 1,000	Might occur at some time in the future	3	**Possible**	L	M	M	H	E
	1 in 1,000 – – 10,000	Could occur but doubtful	2	**Unlikely**	L	M	M	H	H
	1 in 10,000 – – 100,000	May occur but only in exceptional circumstances	1	**Rare**	L	L	M	M	H

Rys. 24. Macierz ryzyka AS/NZS 4360:2004

Źródło: *Risk Management Toolkit*, op. cit.

Metody oparte na rywalizacji (ang. *Competitive methods*) najlepiej spośród wszystkich uwzględniają czynnik ludzki. Zakładają one, że bezpieczeństwo systemów informacyjnych uzależnione jest od skłonności do podjęcia ryzyka zarówno strony broniącej systemu, jak i atakującej go. Angelo Marcello zaproponował następujący wzór na poziom ryzyka R dla systemu informatycznego:

$$R = \theta^2 \cdot \Psi \cdot \frac{1}{t^2} \cdot F$$

gdzie:

θ – poziom wiedzy atakującego o systemie,

Ψ – stosunek skłonności do ryzyka strony broniącej do strony atakującej,

$\frac{1}{t}$ – poziom nieznajomości systemu przez atakującego,

F – poziom przekonania o sukcesie strony atakującej[186].

Niezwykle trudno jest jednak uzyskać wiarygodne dane, które można byłoby zastosować w tej metodzie. Napastnik zazwyczaj jest nieznany, tym bardziej informacja o stanie jego wiedzy. Wzór Marcello odnosi się jedynie do zagrożeń związanych z czynnikiem ludzkim i nie obejmuje pozostałych zagrożeń.

Metodyką opartą na rywalizacji, jest również OSPEC[187]. Stosowana jest w armii Stanów Zjednoczonych i obejmuje pięć etapów:

1) identyfikacja zasobów stanowiących potencjalny cel ataków,
2) identyfikacja strony atakującej, jej celów i potencjału,
3) analiza podatności prowadzących do przełamania zabezpieczeń systemu,
4) wycena efektów wykorzystania podatności oraz przeprowadzenie analizy kosztów i wyników działań naprawczych,
5) określenie i wdrożenie odpowiednich zabezpieczeń[188].

Stosowanie tego typu metodyki jest bardziej racjonalne w armii niż w innych organizacjach. Ma ona bowiem do dyspozycji zupełnie inne środki, za pomocą których może zidentyfikować potencjalne źródła i cele ataku. Są to dane służb wywiadowczych.

[186] M. Ryba, *Oparta na koncepcji rywalizacji metoda analizy ryzyka systemów informatycznych*, „Computer Science" 2004. Vol. 6.

[187] *Operations and Signal Security*, Army Regulation 530–1, Headquarters Department of the Army, Washington 2007.

[188] M. Ryba, *Wielowymiarowa metodyka analizy i zarządzania ryzykiem systemów informatycznych – MIR-2M*, rozprawa doktorska, Akademia Górniczo-Hutnicza w Krakowie, Kraków 2006.

Zakończenie

Przetwarzanie danych osobowych, zgodne z ustawą o ochronie danych osobowych, narzuca liczne obowiązki na administratorów danych. Związane są one z odpowiednią organizacją pracy, prowadzeniem szczegółowej dokumentacji oraz wydatkowaniem środków finansowych na zabezpieczenia techniczne.

Początek roku 2015 przyniósł liczne zmiany w prawie, o niespotykanej od chwili wydania UODO skali. Proces reformy prawa dotyczącego ochrony danych osobowych nadal trwa. Oprócz wejścia w życie opisywanych projektów, można spodziewać się przepisów sektorowych. Postęp techniki, a w szczególności branży ICT, umożliwi stosowanie nowych rozwiązań technicznych w odpowiedzi na rosnące zagrożenia.

Dane osobowe to tylko część informacji, jakie winien chronić przedsiębiorca. Zbiory zawierające dane klientów niebędących osobami fizycznymi, szczegóły kontraktów, know-how, choć nie są prawnie chronione w zbliżonym stopniu, są informacjami mogącymi stanowić o przewadze konkurencyjnej i mają wymierną wartość. Tworząc politykę bezpieczeństwa, należy zastanowić się nad kompleksowym rozwiązaniem i wdrożeniem zintegrowanego systemu zarządzania bezpieczeństwem informacji.

Załącznik 1. Wzór upoważnienia imiennego

.....
(pieczęć podłużna Generalnego Inspektora
Ochrony Danych Osobowych)

L.dz. . .....

Upoważnienie imienne

Na podstawie art. 12 pkt 1 i 2 w związku z art. 14 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 i Nr 153, poz. 1271, z 2004 r. Nr 25, poz. 219 i Nr 33, poz. 285, z 2006 r. Nr 104, poz. 708 i 711, z 2007 r. Nr 165, poz. 1170 i Nr 176, poz. 1238 oraz z 2010 r. Nr 41, poz. 233, Nr 182, poz. 1228 i Nr 229, poz. 1497)

upoważniam

Panią/Pana
.....
.....
(imię i nazwisko inspektora)

stanowisko służbowe ..... nr legitymacji służbowej .....
do przeprowadzenia kontroli:
.....
.....
.....
.....
.....
.....
(określenie: podmiotu objętego kontrolą albo zbioru danych, albo miejsca poddawanego kontroli)
w zakresie:
.....
.....
.....
.....
.....
.....
(określenie zakresu przedmiotowego kontroli)

Data rozpoczęcia kontroli:
.....
Przewidywany termin zakończenia kontroli:
.....

Upoważnienie jest ważne jedynie z równoczesnym okazaniem legitymacji służbowej.

.....
(miejsce i data wystawienia upoważnienia)

pieczęć urzędowa

.....
(podpis Generalnego Inspektora Ochrony Danych Osobowych)

Pouczenie kontrolowanego podmiotu o jego prawach i obowiązkach

1. Zgodnie z art. 15 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, kierownik kontrolowanej jednostki organizacyjnej oraz kontrolowana osoba fizyczna będąca administratorem danych osobowych są obowiązani umożliwić inspektorowi przeprowadzenie kontroli, a w szczególności umożliwić przeprowadzenie czynności oraz spełnić żądania, o których mowa w art. 14 pkt 1-4 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, polegające na:
• umożliwieniu wstępu inspektorom, w godzinach od 600 do 2200, za okazaniem niniejszego imiennego upoważnienia i legitymacji służbowej, do pomieszczenia, w którym jest zlokalizowany zbiór danych, oraz pomieszczenia, w którym przetwarzane są dane poza zbiorem danych, i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą o ochronie danych osobowych,
• żądaniu złożenia pisemnych lub ustnych wyjaśnień oraz wzywania i przesłuchiwania osoby w zakresie niezbędnym do ustalenia stanu faktycznego,
• umożliwieniu wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii,
• przeprowadzaniu oględzin urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.
2. Zgodnie z art. 16 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, z czynności kontrolnych inspektor sporządza protokół, którego jeden egzemplarz doręcza kontrolowanemu administratorowi danych. Protokół podpisują inspektor i kontrolowany administrator danych, który może wnieść do protokołu umotywowane zastrzeżenia i uwagi (art. 16 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych). W razie odmowy podpisania protokołu przez kontrolowanego administratora danych inspektor czyni o tym wzmiankę w protokole, a odmawiający podpisu może, w terminie 7 dni, przedstawić swoje stanowisko na piśmie Generalnemu Inspektorowi (art. 16 ust. 3 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych).

.....
(data i czytelny podpis osoby reprezentującej kontrolowany podmiot)

Załącznik 2. Wzór legitymacji

Awers legitymacji:

legitymacja koloru niebieskiego;
napisy w kolorze czarnym:
Rzeczpospolita Polska,
Biuro Generalnego Inspektora
Ochrony Danych Osobowych;
numer legitymacji;
orzeł z godła RP;
pasek przekątny koloru biało-czerwonego.

Rewers legitymacji:

legitymacja koloru niebieskiego;
napisy w kolorze czarnym:
LEGITYMACJA SŁUŻBOWA
Inspektora
Ochrony Danych Osobowych;
ważna do;
miejsce na fotografię;
miejsce na pieczęć;
nazwisko;
imię
nr ewidencyjny PESEL
podpis wystawcy;
podpis właściciela;
hologram z literami w kolorze niebieskim.

Wymiary legitymacji:

wysokość – 90 mm,
szerokość – 65 mm,
wysokość fotografii – 35 mm,
szerokość fotografii – 25 mm.

Rodzaj papieru i zabezpieczeń:

gramatura papieru 200g/m^3,
papier kredowany, dwustronnie – matowy,
hologram,
w miejscach wpisu nazwiska i imienia oraz numeru ewidencyjnego PESEL nadruk cienkich linii zabezpieczających.

Załącznik 3. Wzór druku zgłoszenia powołania i odwołania administratora bezpieczeństwa danych

ZGŁOSZENIE
POWOŁANIA ADMINISTRATORA BEZPIECZEŃSTWA INFORMACJI DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH

Data wpłynięcia zgłoszenia: ……..
(wypełnia Generalny Inspektor Ochrony Danych Osobowych)*

Część A. Oznaczenie administratora danych

Nazwa administratora danych i adres jego siedziby albo nazwisko, imię i adres miejsca zamieszkania administratora danych oraz nr REGON – jeżeli został nadany.

1. Administrator:
2. REGON:
3. Adres:
   ulica:
   nr domu: nr lokalu:
   kod pocztowy:
   miejscowość:

Część B. Dane osobowe administratora bezpieczeństwa informacji i data jego powołania

1. Imię i nazwisko:
2. Numer PESEL lub, gdy ten numer nie został nadany, nazwa i seria/nr dokumentu stwierdzającego tożsamość:
   PESEL:
   nazwa dokumentu tożsamości: seria/nr dokumentu tożsamości:
3. Adres do korespondencji, jeżeli jest inny niż wskazany w części A zgłoszenia:
   ulica:
   nr domu: nr lokalu:
   kod pocztowy:
   miejscowość:
4. Data powołania administratora bezpieczeństwa informacji:

Część C. Oświadczenie administratora danych o spełnieniu przez administratora bezpieczeństwa informacji warunków określonych w ustawie

Oświadczam, że administrator bezpieczeństwa informacji wskazany w części B zgłoszenia**:

- ☐ ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych,
- ☐ posiada odpowiednią wiedzę w zakresie ochrony danych osobowych,
- ☐ nie był karany za umyślne przestępstwo,
- ☐ podlega bezpośrednio kierownikowi jednostki organizacyjnej lub osobie fizycznej będącej administratorem danych.

(data, podpis i pieczęć administratora danych)*

Objaśnienia:

* Pola nie należy wypełniać, jeżeli zgłoszenie doręczone jest za pomocą środków komunikacji elektronicznej.
** W przypadku odpowiedzi twierdzącej należy zakreślić kwadrat literą „*X*".

Załącznik 4. Wzór zgłoszenia zbioru danych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych

ZGŁOSZENIE ZBIORU DANYCH DO REJESTRACJI GENERALNEMU INSPEKTOROWI OCHRONY DANYCH OSOBOWYCH

* ☐ — zgłoszenie zbioru na podstawie art. 40 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.),
* ☐ — zgłoszenie zmian na podstawie art. 41 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych,
* ☐ — zgłoszenie zbioru, w którym będą przetwarzane dane określone w art. 27 ust. 1 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Nr .....
(nadaje urzędnik Biura GIODO)

Część A. Wniosek

Wnoszę o wpisanie zbioru danych osobowych o nazwie:

.....

do Rejestru Zbiorów Danych Osobowych.

Część B. Charakterystyka administratora danych

1. Wnioskodawca (administrator danych): .....
.....
.....
.....
(nazwa administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania wnioskodawcy oraz nr REGON)

2. Przedstawiciel wnioskodawcy, o którym mowa w art. 31a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych:
.....
.....
(nazwa przedstawiciela administratora danych i adres jego siedziby lub nazwisko, imię i adres miejsca zamieszkania)

3. Powierzenie przetwarzania danych osobowych:
   * ☐ — administrator danych powierzył w drodze umowy zawartej na piśmie przetwarzanie danych innemu podmiotowi (art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych),
   * ☐ — administrator danych przewiduje powierzenie przetwarzania danych innemu podmiotowi.

   W przypadku powierzenia przetwarzania danych innemu podmiotowi, należy podać nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania podmiotu, któremu powierzono przetwarzanie danych osobowych:
   .....
   .....
   ..... * ☐ *ew. cd. w załączniku nr* .....

4. Podstawa prawna upoważniająca do prowadzenia zbioru danych:
   * ☐ — zgoda osoby, której dane dotyczą, na przetwarzanie danych jej dotyczących,
   * ☐ — przetwarzanie jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa —
   .....
   .....
   ..... * ☐ *ew. cd. w załączniku nr* .....

* ☐ — przetwarzanie jest konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą,

* ☐ — przetwarzanie jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego — *w przypadku odpowiedzi twierdzącej, należy opisać te zadania:*

.....

.....

..... * ☐ *ew. cd. w załączniku nr* .....

* ☐ — przetwarzanie jest niezbędne do wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.

Część C. Cel przetwarzania danych, opis kategorii osób, których dane dotyczą, oraz zakres przetwarzanych danych

5. Cel przetwarzania danych w zbiorze:

.....

.....

..... * ☐ *ew. cd. w załączniku nr* .....

6. Opis kategorii osób, których dane dotyczą:

.....

.....

.....

7. Zakres przetwarzanych w zbiorze danych o osobach:

* ☐ — nazwiska i imiona,
* ☐ — imiona rodziców,
* ☐ — data urodzenia,
* ☐ — miejsce urodzenia,
* ☐ — adres zamieszkania lub pobytu,
* ☐ — numer ewidencyjny PESEL,
* ☐ — Numer Identyfikacji Podatkowej,
* ☐ — miejsce pracy,
* ☐ — zawód,
* ☐ — wykształcenie,
* ☐ — seria i numer dowodu osobistego,
* ☐ — numer telefonu.

8. Inne dane osobowe, oprócz wymienionych w pkt 7, przetwarzane w zbiorze — *należy podać, jakie:*

.....

.....

..... * ☐ *ew. cd. w załączniku nr* .....

9. Dane przetwarzane w zbiorze:

a) ujawniają bezpośrednio lub w kontekście:

* ☐ — pochodzenie rasowe,
* ☐ — pochodzenie etniczne,
* ☐ — poglądy polityczne,
* ☐ — przekonania religijne,
* ☐ — przekonania filozoficzne,
* ☐ — przynależność wyznaniową,
* ☐ — przynależność partyjną,
* ☐ — przynależność związkową,
* ☐ — stan zdrowia,
* ☐ — kod genetyczny,
* ☐ — nałogi,
* ☐ — życie seksualne,

b) dotyczą:

* ☐ — skazań,
* ☐ — mandatów karnych,
* ☐ — orzeczeń o ukaraniu,
* ☐ — innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Jeśli nie zakreślono żadnej odpowiedzi, należy przejść do pkt 11.

10. Podstawa prawna przetwarzania danych wskazanych w pkt 9:
    * ☐ — osoby, których dane dotyczą, będą wyrażać na to zgodę na piśmie,
    * ☐ — przepis szczególny innej ustawy zezwala na przetwarzanie bez zgody osoby, której dane dotyczą, jej danych osobowych — *w przypadku odpowiedzi twierdzącej, należy podać odniesienie do przepisu tej ustawy:*

    .....

    .....

    ..... * ☐ *ew. cd. w załączniku nr* .....

    * ☐ — przetwarzanie danych jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby, gdy osoba, której dane dotyczą, nie jest fizycznie lub prawnie zdolna do wyrażenia zgody, do czasu ustanowienia opiekuna prawnego lub kuratora,
    * ☐ — przetwarzanie jest niezbędne do wykonania statutowych zadań kościoła, innego związku wyznaniowego, stowarzyszenia, fundacji lub innej niezarobkowej organizacji lub instytucji o celach politycznych, naukowych, religijnych, filozoficznych lub związkowych, a przetwarzanie danych dotyczy wyłącznie członków tej organizacji lub instytucji albo osób utrzymujących z nią stałe kontakty w związku z jej działalnością i zapewnione są pełne gwarancje ochrony przetwarzanych danych — *w przypadku odpowiedzi twierdzącej, należy podać, jakich*:

    .....

    .....

    ..... * ☐ *ew. cd. w załączniku nr* .....

    * ☐ — przetwarzanie dotyczy danych, które są niezbędne do dochodzenia praw przed sądem,
    * ☐ — przetwarzanie jest niezbędne do wykonania zadań administratora danych odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony w ustawie,
    * ☐ — przetwarzanie jest prowadzone w celu ochrony stanu zdrowia, świadczenia usług medycznych lub leczenia pacjentów przez osoby trudniące się zawodowo leczeniem lub świadczeniem innych usług medycznych, zarządzania udzielaniem usług medycznych i są stworzone pełne gwarancje ochrony danych osobowych,
    * ☐ — przetwarzanie dotyczy danych, które zostały podane do wiadomości publicznej przez osobę, której dane dotyczą,
    * ☐ — przetwarzanie jest niezbędne do prowadzenia badań naukowych, w tym do przygotowania rozprawy wymaganej do uzyskania dyplomu ukończenia szkoły wyższej lub stopnia naukowego, a publikowanie wyników badań naukowych uniemożliwia identyfikację osób, których dane zostały przetworzone,
    * ☐ — przetwarzanie danych jest prowadzone przez stronę w celu realizacji praw i obowiązków wynikających z orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

Część D. Sposób zbierania oraz udostępniania danych

11. Dane do zbioru będą zbierane:
    * ☐ — od osób, których dotyczą,
    * ☐ — z innych źródeł niż osoba, której dane dotyczą.

12. Dane ze zbioru będą udostępniane:
    * ☐ — podmiotom innym niż upoważnione na podstawie przepisów prawa.

13. Odbiorcy lub kategorie odbiorców, którym dane mogą być przekazywane — *należy podać nazwę i adres siedziby lub nazwisko, imię i adres miejsca zamieszkania odbiorcy danych:*

    .....

    .....

    ..... * ☐ *ew. cd. w załączniku nr* .....

14. Informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego — *należy podać nazwę państwa:*

    .....

    .....

    ..... * ☐ *ew. cd. w załączniku nr* .....

Część E. Opis środków technicznych i organizacyjnych zastosowanych w celach określonych w art. 36—39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych

15. Zbiór danych osobowych jest prowadzony:

a) * ☐ — centralnie,
* ☐ — w architekturze rozproszonej,

b) * ☐ — wyłącznie w postaci papierowej,
* ☐ — z użyciem systemu informatycznego,

c) * ☐ — z użyciem co najmniej jednego urządzenia systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną (np. Internetem),
* ☐ — bez użycia żadnego z urządzeń systemu informatycznego służącego do przetwarzania danych osobowych połączonego z siecią publiczną (np. Internetem).

16. Zostały spełnione wymogi określone w art. 36—39 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1]:

a) * ☐ — został wyznaczony administrator bezpieczeństwa informacji nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych,
* ☐ — administrator danych sam wykonuje czynności administratora bezpieczeństwa informacji,

b) * ☐ — do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych,

c) * ☐ — prowadzona jest ewidencja osób upoważnionych do przetwarzania danych,

d) * ☐ — została opracowana i wdrożona polityka bezpieczeństwa,

e) * ☐ — została opracowana i wdrożona instrukcja zarządzania systemem informatycznym,

f) inne środki, oprócz wymienionych w ppkt a—e, zastosowane w celu zabezpieczenia danych:

.....

.....

..... * ☐ *ew. cd. w załączniku nr* .....

Część F. Informacja o sposobie wypełnienia warunków technicznych i organizacyjnych, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024)

17. Zastosowano środki bezpieczeństwa na poziomie[2]:

* ☐ — podstawowym,
* ☐ — podwyższonym,
* ☐ — wysokim.

.....
(data, podpis i pieczęć wnioskodawcy)

Objaśnienia:

* W przypadku odpowiedzi twierdzącej należy zakreślić kwadrat literą *„X"*.

[1] Administrator danych prowadzący zbiór w systemie tradycyjnym (papierowym) zobowiązany jest do zastosowania środków określonych w pkt 16 ppkt a—d, a w przypadku prowadzenia zbioru w systemie informatycznym, ponadto środka określonego w pkt 16 ppkt e.

[2] Należy wskazać odpowiedni poziom bezpieczeństwa określony w § 6 ww. rozporządzenia (UWAGA! Dotyczy wyłącznie administratorów przetwarzających dane w systemie informatycznym):
— jeżeli wnioskodawca przetwarza dane wymienione w pkt 9 zgłoszenia, należy zastosować środki bezpieczeństwa przynajmniej na poziomie podwyższonym;
— w przypadku gdy przynajmniej jedno urządzenie systemu informatycznego służącego do przetwarzania danych osobowych połączone jest z siecią publiczną, należy zastosować środki bezpieczeństwa na poziomie wysokim;
— w pozostałych przypadkach wystarczające jest zastosowanie środków bezpieczeństwa na poziomie podstawowym.

Zgłoszenia można dokonać drogą elektroniczną, za pomocą programu komputerowego umożliwiającego jego prawidłowe wypełnienie, dostępnego na stronie internetowej Generalnego Inspektora Ochrony Danych Osobowych.

Bibliografia

10 Faces of Computer Malware, portal Techrepublic, http://www.techrepublic.com/blog/10-things/the-10-faces-of-computer-malware/

ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych, GIODO. Wydawnictwo Sejmowe, Warszawa 2007

Adamczewski P., *Słownik informatyczny*, Helion, Gliwice 2005

Adams C., Lloyd S., *PKI. Podstawy i zasady działania. Koncepcje, standardy i wdrażanie infrastruktury kluczy publicznych*, WN PWN, Warszawa 2007

Adams C., Lloyd S., *Podpis elektroniczny klucz publiczny*, Wydawnictwo ROBOMATIC, Wrocław 2002

Adres IP może być w pewnych przypadkach uznany za dane osobowe, Portal GIODO, zakładka Odpowiedzi na pytania dotyczące ustawy o ochronie danych osobowych definicji danych osobowych, pytanie: Czy adres IP komputera należy do danych osobowych?, http://www.giodo.gov.pl/319/id_art/2258/j/pl/

Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation, ARTICLE 29 Data Protection Working Party, Brussels, 13 maja 2013 r.

Alter S., *A General, yet Useful Theory of Information Systems*, "Communications of the Association for Information Systems" 1999, Vol. 1., Article 13

Anderson R., Biham E., Knudsen L., *Serpent: A Flexible Block Cipher With Maximum Assurance*, First AES Candidate Conference (AES1), California 1998

Anderson R., *Inżynieria zabezpieczeń*, WNT, Warszawa 2005

Armerding T., *The 15 worst data security breaches of the 21st Century*, portal CSO, http://www.csoonline.com/article/2130877/data-protection/data-protection-the-15-worst-data-security-breaches-of-the-21st-century.html

Bakalarczyk S., *Innowacje bankowe: bankowość elektroniczna, bankowość inwestycyjna i inżynieria finansowa*, Wydawnictwo Politechniki Łódzkiej, Łódź 2006

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych: komentarz*, Wolters Kluwer, Warszawa 2011

Baskerville R., *Information Systems Security Design Methods: Implications for Information Systems Development*, "ACM Computing Surveys" 1993, Vol. 25, No. 4

Bauer F.L., *Sekrety kryptografii*, Helion, Gliwice 2003

Bennett H., *Understanding CD-R & CD-RW*, Optical Storage Technology Association, Rev 1.00 1/2003

Bieńkowski M., *Odcisk palca zamiast hasła*, „IT w administracji" 2009, nr 4

Chyra R., *Usługi terminalowe Windows 2000*, Helion, Gliwice 2003

Cole E., Krutz R.L., Conley J., *Bezpieczeństwo sieci. Biblia*, Helion, Gliwice 2005

Courtois N., Pieprzyk J., *Cryptanalysis of Block Ciphers with Overdefined Systems of Equations*, Cryptology ePrint Archive: Report 2002/044. 2002, https://eprint.iacr.org/2002/044

Czajka A., Pacut A., *Biometria podpisu odręcznego*, w: *Automatyczna identyfikacja w systemach logistycznych*, (red.) Zając P., Kwaśniowski S., Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2004

Czerwiński K., *Analiza ryzyka w audycie wewnętrznym*, Link, Szczecin 2003

Czerwiński K., Grocholski H., *Podstawy audytu wewnętrznego*, Link, Szczecin 2003

Daemen J., Govaerts R., Vandewalle J., *Weak Keys For IDEA*, w: *Advances in Cryptology – CRYPTO 1993, Lecture Notes in Computer Science 773*, (ed.) Stinson D.R., Springer-Verlag, Berlin 1994

Daszkiewicz K., Arnold A., Vogt R., *Jak archiwizować dane na lata*, „PC World" 2009, nr 11

A Dictionary of the social sciences, (eds.) Gould J., Kolb W.L., Free Press, London 1964

Diffie W., Hellman M.E., *New Directions in Cryptography*, "IEEE Transactions on Information Theory" 1976, Vol. IT-22, No. 6

Dimauro G., Impedevo S., Pirlo G. Salzo A., *A Multi-Expert Signature Verification System for Bankcheck Processing*, "International Journal of Pattern Recognition and Artificial Intelligence" 1996/97, Vol. 11, Iss. 2

DLT-S4 Buffer Management – Speed matching White Paper, Quantum Corporation, 5 kwietnia 2006 r.

Długosz T., Wujczyk P., *Behawioralne metody biometryczne – dynamika pisania na klawiaturze*, „Wiadomości Telekomunikacyjne" 2009, nr 10

Drozd A., *Ustawa o ochronie danych osobowych: komentarz: wzory pism i przepisy*, LexisNexis, Warszawa 2004

Dziawgo D., *Creditrating, ryzyko i obligacje na międzynarodowym rynku finansowym*, WN PWN, Warszawa 1998

ElGamal T., *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, "IEEE Transactions on Information Theory" 1985, Vol. IT-31, No. 4

Engelmann M., *Bezpieczeństwo informacji – bezpieczeństwo fizyczne*, „Boston IT Security Review" 2007, nr 3, tom 4

Folga K., *Spoofing: sztuka ataku i obrony*, „Networld" 2005, nr 10

Foryś W., *W kręgu idei kryptologii*, „Alma Mater – miesięcznik Uniwersytetu Jagielońskiego" 2005, nr 69

Glosariusz terminów dotyczących kontroli i audytu w administracji publicznej, Najwyższa Izba Kontroli, Warszawa 2006

Grochowski E., Halem R.D., *Technological impact of magnetic hard disk drives on storage systems*, "IBM Systems Journal" 2003, Vol. 42, No. 2

Gutkowska D., Stolc L., *Techniki identyfikacji osób z wykorzystaniem indywidualnych cech biometrycznych*, Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej nr 20, Gdańsk 2004

Guzik A., *Nowy standard niszczenia dokumentów i nośników danych – DIN 66399*, „Człowiek i dokumenty", 2015, nr 37, http://www.pwpw.pl/kwartalnik_biezacy_numer.html?print=1&id=45&magCid=227

Hinden R., *Virtual Router Redundancy Protocol (VRRP)*, Nokia RFC3768, kwiecień 2004

Holme D., *Efektywne rozwiązania dla specjalistów IT. Resource Kit*, Microsoft Press, Warszawa 2008

infoDOK. Raport o dokumentach. 18 edycja: II kwartał 2014 r., Związek Banków Polskich 2014

Jadczak A., *Jak zarządzać ryzykiem braku prądu*, „Computerworld" 2008, nr 8

Jakubik K., *Jak przechowywać więcej za mniej*, „Computerworld" 2008, nr 5

Jakubik K., *Ochrona danych przed błędami ludzkimi*, „Networld" 2007, nr 9

Jakubik K., *Fibre channel kontra ISCSI*, "Networld" 2006, nr 1

Janowski J., *Elektroniczny obrót prawny*, Wolters Kluwer, Warszawa 2008

Januszewski S., Kosut C., Pietranik M., Pyter M., *Systemy bezprzerwowego zasilania (UPS). Komentarz do norm serii PN-EN 62040*, SEP Centralny Ośrodek Szkolenia i Wydawnictw, Warszawa 2002

Jaroszewski P., *Dobre praktyki: Hasło*, CERT Polska 02/2005

Kamiński M., *Anonimizacja i usuwania danych osobowych*, „Safety and Security" 2015, nr 1

Karbowski M., *Podstawy kryptografii*, Helion, Gliwice 2007

Katalog zagrożeń stosowany przez CERT.GOV.PL, http://www.cert.gov.pl/cer/publikacje/katalog-zagrozen-stosow/731,Katalog-zagrozen-stosowany-przez-CERTGOVPL.html

Keizer G., *New exploit technique nullifies major Windows defense*, "Computerworld" 2010, No. 3

Kisielnicki J., Sroka H., *Systemy informacyjne biznesu. Informatyka dla zarządzania*, Placet, Warszawa 2005

Królikowski B., *Silne uwierzytelnianie z użyciem tokenów kryptograficznych*, „Networld" 2008, nr 9

Krysowaty A., Krysowaty I., Nadziejko P., *Biometria w systemie bezpieczeństwa człowieka – metoda czy konieczność*, Instytut Inżynierii Systemów Bezpieczeństwa, Warszawa 2007

Krysowaty A., Krysowaty I., Niedziejko P., *Nie bójmy się biometrii!*, „Zabezpieczenia" 2007, nr 6

Kubas M., Molski M., *Karta elektroniczna. Bezpieczny nośnik informacji*, Mikom, Warszawa 2002

Kuraś M., *System informacyjny – system informatyczny. Co poza nazwą różni te dwa obiekty?*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2005, nr 770, http://www.uci.agh.edu.pl/uczelnia/tad/PSI11/art/SI-vs-SIT.pdf

Lal K., Rak T., *Linux a technologie klastrowe*, Mikom, Warszawa 2005

Langefors B., *Theoretical Analysis of Information Systems*, 4th ed., Auerbach Publishers, Lund–Philadelphia 1973

Leszek P., *Smart cards – krzemowa inteligencja*, „Chip", wyd. specjalne *Security*, 2003

Li T., Cole B., Morton P., Li D., *Cisco Hot Standby Router Protocol (HSRP)*, CISCO Systems, RFC 2281, marzec 1998

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Mikom, Warszawa 2008

Liszcz T., *Ochrona prywatności pracownika w relacjach z pracodawcą*, „Monitor Prawa Pracy" 2007, nr 1

LTO Ultrium 2 Tape Drive Introducing Next Generation Tape Technology, Fujitsu White Paper, 2003 Lipiec

Luther J., *Macierze RAID*, „PC World" 2003, nr 10, wyd. specjalne *Sprzęt – urządzenia peryferyjne*

Luther J., *Napędy taśmowe*, „PC World" 2003, nr 10

Łukaj M., *Fleszowa wieża Babel*, „CHIP" 2004, nr 8

Maćkowiak K., *Złam szyfr i odkryj tajemnicę*, „Software 2.0" 2004, nr 9

Mazur M., *Pojęcie systemu i rygory jego stosowania*, „Postępy Cybernetyki" 1987, z. 2

Menezes A.J., Oorschot P.C. van, Vanstone S.A., *Handbook of Applied Cryptography*, CRC Press, Boca Raton 1996

Meszczyński M., *Edukacja przede wszystkim*, „IT w administracji" marzec 2010

Metzger P., *Anatomia PC. Kompendium*, wyd. IV, Helion, Gliwice 2008

Mężyk B., *UPS Line-Interactive – co to naprawdę jest*, „Computerworld" 1994, nr 5

Mueller S., Ogletree T.W., Soper M.E., *Rozbudowa i naprawa sieci*, wyd. V, Helion, Gliwice 2006

Niedziejko P., Krysowaty I., *Biometria. Charakterystyka danych człowieka i ich wykorzystanie w bezpieczeństwie*, „Zabezpieczenia" 2007, nr 1

NSA Releases Top Secret Crypto Papers, Cryptome, 3 marca 2007 r., http://cryptome.org/nsa-nse/nsa-nse-01.htm

Odor P., *Nieodwracalne niszczenie danych*, „NEXT" 2009, nr 1

Olszewska W., *Paragraf na stalkera*, „Na wokandzie" 2010, nr 3

Państwowa Inspekcja Pracy i GIODO zawarły porozumienie o współpracy, portal GIODO, zakładka Aktualności, http://www.giodo.gov.pl/259/id_art/5767/j/pl

Pawełczyk W., *Redundancja komunikacji w sieci Ethernet – JETNet Ring*, „Biuletyn Automatyki" 2006, nr 1, tom nr 47

Pawlak R., *Okablowanie strukturalne sieci. Teoria i praktyka*, Helion, Gliwice 2008

Pfeffer I., *Insurance and economic theory. Pub. for SS Huebner Foundation for Insurance Education*, University of Pennsylvania, Philadelphia 1956

Pinheiro E., Weber W.D., Barroso L.A., *Failure Trends in a Large Disk Drive Population*, 5th USENIX Conference on File and Storage Technologies (FAST'07), San Jose, luty 2007

Polok M., *Bezpieczeństwo danych osobowych*, C.H. BECK, Warszawa 2008

portal RejestrABI, https://rejestrabi.pl/

Preston W.C., *Archiwizacja i odzyskiwanie danych*, Helion, Gliwice 2008.

Pyrchla A., Danowski B., *BIOS. Przewodnik*, wyd. III, Helion, Gliwice 2007

Raport z X Badania wykorzystania poczty elektronicznej w Polsce, Sare S.A., http://sare.pl/ [2014]

Rejestr podmiotów kwalifikowanych NCC 2015, http://www.nccert.pl/podmioty.htm

Risk Management Toolkit, Australian Capital Territory Insurance Authority, Canberra 2004

Rivest R., Shamir A., Adleman L., *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, "Communications of the ACM" 1978, Vol. 21, No. 2

Robson G.D., *The Origins of Phreaking*, "Blacklisted! 411" 2004, Vol. 6, Iss. 2

Romanowska-Słomka I., Słomka A., *Zarządzanie ryzykiem zawodowym*, wyd. 3, Tarbonus, Tarnobrzeg 2003

Ryba M., *Oparta na koncepcji rywalizacji metoda analizy ryzyka systemów informatycznych*, „Computer Science" 2004, Vol. 6

Ryba M., *Wielowymiarowa metodyka analizy i zarządzania ryzykiem systemów informatycznych – MIR-2M*, rozprawa doktorska, Akademia Górniczo-Hutnicza w Krakowie, Kraków 2006

Satyanarayanan M., Ebling M.R., Raiff J., Braam P.J., Harkes J., *Coda File System User and System Administrators Manual*, Coda Team 2000, http://coda.cs.cmu.edu/doc/html/manual/index.html

Schneier B., *Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)*, Fast Software Encryption, Cambridge Security Workshop Proceedings (December 1993), Springer–Verlag, 1994, https://www.schneier.com/paper-blowfish-fse.html

Scrimger R., LaSalle P., Leitzke C., Parihar M., Gupta M., *TCP/IP. Biblia*, Helion, Gliwice 2002

Serial Attached SCSI: Meeting the Growing Needs of Enterprise Storage, White Papers, Adaptec, Inc., Singapore 2004

Shannon C.E., *Communication Theory of Secrecy Systems*, "The Bell System Technical Journal" 1948, Vol. 27

Sibiga G., *Postępowanie w sprawach ochrony danych osobowych*, Dom Wydawniczy ABC, Warszawa 2003

Sieńczyło-Chlebowicz J., *Naruszenie prywatności osób publicznych przez prasę. Analiza cywilnoprawna*, Zakamycze, Kraków 2006

Sikora A., *Przegląd zagadnień kryptografii*, „PC World" 2003, wyd. specjalne *Security*

Singh S., *Księga szyfrów*, Albatros, Szczecin 2001

Słownik języka polskiego, (red.) Szymczak M., PWN, Warszawa 1979

Sosinsky B., *Sieci komputerowe. Biblia*, Helion, Gliwice 2011

Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2013, http://www.giodo.gov.pl/data/filemanager_pl/sprawozdaniaroczne/2013.pdf

Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, ISP PAN, Warszawa 1996

Steinmüller W., *Zautomatyzowane systemy informacyjne w administracji prywatnej i publicznej*, „Organizacja – Metoda – Technika" 1977, nr 9

Stinson D.R., *Kryptografia w teorii i praktyce*, WNT, Warszawa 2005

Stoneburner G., Goguen A., Feringa A., *Risk Management Guide for Information Technology Systems*, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-30, Gaithersburg 2002

Studzińska E., *Bezpieczeństwo techniczne. Więcej niż ochrona*, raport specjalny *Bezpieczeństwo techniczne*, „Computerworld" 2009

Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer, Warszawa 2010

Szczepankiewicz E.I., Szczepankiewicz P., *Analiza ryzyka w środowisku informatycznym do celów zarządzania ryzykiem operacyjnym*, „Audyt 2006, nr 7

Świat zaszyfrowany, Marcin Bójko rozmawia z wiceprezesem RSA Security, „Komputer" nr 7, dodatek do „Komputer" 2002, nr 36

Świniarski J., *Filozoficzne podstawy edukacji dla bezpieczeństwa*, Egros, Warszawa 1999

Tanenbaum A.S., Steen M. van, *Systemy rozproszone. Zasady i paradygmaty*, WNT, Warszawa 2005

The Ten Most Critical Web Application Security Risks, OWASP Foundation 2010, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Trautman L.J., *Cybersecurity: What About US Policy?*, artykuł niepublikowany, 2015, http://works.bepress.com/lawrence_trautman/26

Vilsbeck C., *Twarde dyski IDE, a praca ciągła*, „PC World", wydanie specjalne *Sprzęt–podzespoły*, 2003

Wacławska P., *Jak dobrać bezbłędnych pracowników: czyli minimalizowanie ryzyka osobowego na etapie poprzedzającym nawiązanie stosunku pracy*, Wolters Kluwer, Warszawa 2008

Wessels T., Omlin C., *A hybrid system for signature verification*, Neural Networks, 2000. IJCNN 2000, Proceedings of the IEEE-INNS-ENNS International Joint Conference on, Vol. 5

Wiatr J., Miegoń M., *Zasilacze UPS oraz baterie akumulatorów w układzie zasilania gwarantowanego*, Dom Wydawniczy MEDIUM, Warszawa 2008

Wiewiórowski W., wypowiedź na forum GoldenLine w temacie Zbiór danych w elektronicznym obiegu, http://www.goldenline.pl/grupy/Pozostale/abi/zbior-danych-w-elektronicznym-obiegu,2996230/

Willet A.H., *The Economic Theory of Risk Insurance*, Columbia University Press, New York 1951

Witczak T., *Początki identyfikacji*, „Detektyw" 2007, nr 3, wydanie specjalne

Wobst R., *Kryptologia. Budowa i łamanie zabezpieczeń*, Grupa Wydawnicza READ ME, Warszawa 2002

Żebrowski A., Kwiatkowski M., *Bezpieczeństwo informacji III Rzeczypospolitej*, Oficyna Wydawnicza Abrys, Kraków 2000

Normy i standardy

8 mm Wide Magnetic Tape Cartridge for Information Interchange – Helical Scan Recording – AIT-3 Format, ECMA, 12/2001, Ecma International, Geneva 2001

Announcing the Standard for DATA ENCRYPTION STANDARD (DES), Federal Information Processing Standards Publication 46-2 1988, National Institute of Standards and Technology, Gaithersburg 1988

Data interchange on read-only 120 mm optical data disks (CD-ROM), ECMA 6/1996, Ecma International, Geneva 1996

DIN 32757-2, Office machines; destruction of information media; machines and devices; minimum informations, Deutsches Institut für Normung, Berlin 1985

Guideline for Automatic Data Processing Risk Analysis, "Federal Information Processing Standards Publication FIPS 65", National Bureau of Standards, Institute for Computer Sci-ences and Technology, Gaithersburg 1979

Guidelines for the Regulation of Computerized Personal Data Files, A/RES/45/95, Organizacja Narodów Zjednoczonych, 14 grudnia 1990 r.

Guidelines for the Regulation of Computerized Personal Data Files, G.A. res. 44/132, 44 U.N. GAOR Supp. (No. 49) at 211, U.N. Doc. A/44/49 (1989), Organizacja Narodów Zjednoczonych, 1989 r.

IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges, Institute of Electrical and Electronics Engineers, Inc., Carol Stream 2012

Information technology — 120 mm (8,54 Gbytes per side) and 80 mm (2,66 Gbytes per side) DVD recordable disk for dual layer (DVD-R for DL), ISO/IEC12862 2009(E), International Organization for Standardization, Geneva 2009

Operations and Signal Security, Army Regulation 530–1, Headquarters Department of the Army, Washington 2007

Polska Norma PN-93/E-08390/14:1993 Systemy alarmowe – Wymagania ogólne – Zasady stosowania, PKN, Warszawa 1993

Polska Norma PN-ISO/IEC 27000:2012, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Przegląd i terminologia, PKN, Warszawa 2012

Polska Norma PN-ISO/IEC 27001:2014-12, Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, PKN, Warszawa 2012

Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), ANSI X9.62 Standard, American National Standards Institute, New York 1998

Akty prawne, rozporządzenia i decyzje administracyjne

Code of conduct for Law Enforcement Officials adopted by General Assembly resolution 34/169 of 17 December 1979, A/RES/34/16, Rezolucja Zgromadzenia Ogólnego ONZ z 17 grudnia 1979 r.
Decyzja GIODO z 26 lipca 2011 r., DOLiS/DEC-609/11
Decyzja GIODO z 24 kwietnia 2008 r., DIS/DEC-254/10616/08
Decyzja GIODO z 28 lutego 2008 r., DIS/DEC-134/4605/08
Decyzja GIODO GI-DP-430/37/02/
Decyzja GIODO GI-DEC-DS-59/02
Decyzja GIODO GI-DP-024/855/02
Decyzja GIODO GI-DP-403/1473/00
Decyzja GIODO GI-DP-97/99
Decyzja Komisji Europejskiej 2000/520/WE z 26 lipca 2000 r., O.J. L 215
Decyzja Parlamentu Europejskiego i Rady z 4 grudnia 2014 r. w sprawie mianowania Europejskiego Inspektora Ochrony Danych i jego zastępcy, 2014/886/UE
Dyrektywa Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych 95/46/WE, Dz.U. WE OJ L 281, 23.11.1995
Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r., Dz.U. z 1997 r. Nr 78, poz. 483
Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu 28 stycznia 1981 r., Dz.U. z 2003 r. Nr 3, poz. 25
Odpowiedź podsekretarza stanu w Ministerstwie Sprawiedliwości – z upoważnienia ministra – na interpelację nr 8701 w sprawie ochrony danych osobowych osób zmarłych, SPS-023-8701/07

Opinia 4/2007 w sprawie pojęcia danych osobowych, 01248/07/PL WP 136, 20 czerwca 2007 r., GrupY Roboczej ds. Ochrony Danych powołanej na mocy Art. 29, http://www.giodo.gov.pl/462/id_art/2375/j/pl/

Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC, ARTICLE 29 Data Protection Working Party, 11601/EN WP 90, Adopted on 27 February 2004

Orzeczenie Trybunału Sprawiedliwości Unii Europejskiej z 13 maja 2014 roku w sprawie C-131/12, ECLI:EU:C:2014:317

Postanowienie Naczelnego Sądu Administracyjnego z 9 listopada 1999 r., II SAB 153/99

Projekt rozporządzenia Ministra Spraw Wewnętrznych w sprawie przetwarzania informacji przez Policję z 18 listopada 2014 r., http://bip.msw.gov.pl/bip/projekty-aktow-prawnyc/2014/23298,Projekt-rozporzadzenia-Ministra-Spraw-Wewnetrznych-w-sprawie-przetwarzania-infor.html

Recommendation of the council concerning guidelines governing the protection of privacy and transborder flows of personal data, OECD 23 September 1980

RozporządzeniE MSWiA z 14 października 1998 r. w sprawie szczegółowych zasad i wymagań, jakim powinna odpowiadać ochrona wartości pieniężnych przechowywanych przez przedsiębiorców i inne jednostki organizacyjne, Dz.U. Nr 129, poz. 858

RozporządzeniE Prezydenta Rzeczypospolitej Polskiej z 3 listopada 2006 r. w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych Dz.U. z 2006 r. Nr 203, poz. 1494

Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz.U. L. 8 z 12 stycznia 2001 r.

Rozporządzenie Ministra Administracji i Cyfryzacji z 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji, Dz.U. z 2014 r., poz. 1934

Rozporządzenie Ministra Administracji i Cyfryzacji z 11 maja 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 Spraw Wewnętrznych i Administracji z 11 grudnia 2008 r. w sprawie wzoru zgłoszenia zbioru do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych, Dz.U. z 2008 r. Nr 229, poz. 1536

Rozporządzenie ministra spraw wewnętrznych i administracji z 11 maja 2011 r. zmieniające rozporządzenie w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych, Dz.U. z 2011 r. Nr 103, poz. 601

Rozporządzenie ministra spraw wewnętrznych i administracji z 22 kwietnia 2004 r. w sprawie wzorów imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych, Dz.U. z 2004 r. Nr 94, poz. 923

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U. z 2004 r. Nr 100, poz. 1024

Rozporządzenie Rady Ministrów z 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych, Dz.U. z 2012 r. poz. 683

Rozporządzeniem Ministra Administracji i Cyfryzacji z 11 maja 2015 roku w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych, Dz.U. z 2015 r. poz. 719

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U. z 2004 r. Nr 100, poz. 1024

Uchwała Sejmu Rzeczypospolitej Polskiej z 3 grudnia 2014 r. w sprawie odwołania Generalnego Inspektora Ochrony Danych Osobowych, M.P. 2015 nr 0 poz. 364

Ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U. z 2000 r. Nr 116, poz. 1216

Ustawa z 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników, Dz.U. z 1995 r. Nr 142, poz. 702

Ustawa z 15 kwietnia 2011 r. o systemie informacji oświatowej, Dz.U. z 2011 r. Nr 139, poz. 814
Ustawa z 16 lipca 2004 r. Prawo telekomunikacyjne, Dz.U. z 2004 r. Nr 171, poz. 1800
Ustawa z 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej, Dz.U. z 2011 r. Nr 230, poz. 1371
Ustawa z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, Dz.U. z 2002 r. Nr 144, poz. 1204
Ustawa z 2 lipca 2004 r. o swobodzie działalności gospodarczej, Dz.U. z 2004 r. Nr 173, poz. 1807
Ustawa z 24 września 2010 r. o ewidencji ludności, Dz.U. z 2010 r. Nr 217, poz. 1427
Ustawa z 26 czerwca 1974 r. Kodeks pracy, Dz.U. z 1974 r. Nr 24 poz. 141
Ustawa z 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, Dz.U. z 2004 r. Nr 210 poz. 2135
Ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. z 2014 r. poz. 1182
Ustawa z 29 sierpnia 1997 r., Prawo bankowe, Dz.U. z 1997 r. Nr 140, poz. 939
Ustawa z 5 sierpnia 2010 roku o ochronie informacji niejawnych, Dz.U. z 2010 r. Nr 182, poz. 1228
Ustawa z 6 czerwca 1997 r. Kodeks karny, Dz.U. z 1997 r. Nr 88, poz. 553
Ustawa z 8 września 2006 r. o Państwowym Ratownictwie Medycznym, Dz.U. z 2006 r. Nr 191, poz. 1410
Ustawa z 15 kwietnia 2011 r. o systemie informacji oświatowej, Dz.U. z 2011 r. Nr 139, poz. 814
Ustawa z 23 kwietnia 1964 r. – Kodeks cywilny, Dz.U. z 1964 r. Nr 16, poz. 93
Ustawa z 26 stycznia 1984 r. Prawo prasowe, Dz.U. z 1984 r. Nr 5, poz. 24
Ustawa z 6 lipca 1982 r. o księgach wieczystych i hipotece, Dz.U. z 1982 r. Nr 19, poz. 147
Wyrok Naczelnego Sądu Administracyjnego w Warszawie z 1 grudnia 2009 r., I OSK 249/09
Wyrok Naczelnego Sądu Administracyjnego z 3 lipca 2009 r., I OSK 633/08
Wyrok Naczelnego Sądu Administracyjnego z 4 marca 2002 r., II SA 3144/01

Wyrok Naczelnego Sądu Administracyjnego z 4 kwietnia 2003 r., SA 2135/2002
Wyrok Wojewódzkiego Sądu Administracyjny z 28 listopada 2008 r., II SA/Wa 903/08

Polskie Towarzystwo Informatyczne (PTI) zostało założone w roku 1981. Stowarzyszenie zrzesza zarówno osoby posiadające wysokie kompetencje i doświadczenie zawodowe w zakresie informatyki, studentów ostatnich lat kierunków informatycznych, jak i specjalistów innych dziedzin, intensywnie wykorzystujących technologie informatyczne.

PTI skupia informatyków działających w administracji publicznej, środowiskach akademickich i biznesowych.

Polskie Towarzystwo Informatyczne należy do Europejskiej Rady Stowarzyszeń Informatycznych CEPIS (Council of European Professional Informatics Societies).

Podstawowe cele **Polskiego Towarzystwa Informatycznego:**

- wspieranie działalności naukowej i naukowo-technicznej we wszystkich dziedzinach informatyki i doskonalenia metod jej efektywnego wykorzystania w gospodarce narodowej,
- popularyzacja zagadnień i zastosowań informatyki w społeczeństwie,
- ułatwianie wymiany informacji w środowisku zawodowym,
- podnoszenie poziomu kwalifikacji i etyki zawodowej informatyków,
- reprezentowanie członków Towarzystwa, ich opinii, potrzeb, interesów i uprawnień wobec społeczeństwa, władz i instytucji w kraju i za granicą.

Izba Rzeczoznawców Polskiego Towarzystwa Informatycznego

Działająca przy Polskim Towarzystwie Informatycznym **Izba Rzeczoznawców PTI** wspiera profesjonalną wiedzą oraz doświadczeniem zrzeszonych w Polskim Towarzystwie Informatycznym przedstawicieli zawodowego i naukowego polskiego środowiska teleinformatycznego.

Izba Rzeczoznawców PTI świadczy usługi na rzecz podmiotów państwowych, samorządowych, organizacji publicznych, firm komercyjnych oraz osób fizycznych w sytuacjach, gdy odwołanie się do opinii niezależnego i obiektywnego autorytetu:

- podnosi szanse powodzenia zaplanowanego przedsięwzięcia informatycznego,
- jest niezbędne do zapewnienia przejrzystości wyboru,
- służy bezstronnemu rozstrzygnięciu dylematów wynikających z realizacji przedsięwzięcia.

Ekspertyzy **Izby Rzeczoznawców PTI** realizowane są przez zespoły specjalistów z wieloletnim doświadczeniem w branży IT. Ich kwalifikacje potwierdzone są akredytacjami i certyfikacjami zarówno niezależnych organizacji takich jak The Open Group (TOGAF), ISC2 (certyfikaty CISSP), ISACA (certyfikaty CISA, CRISC, CISM), CCTE (certyfikaty PRINCE2), PMI, jak i czołowych krajowych i międzynarodowych producentów sprzętu i oprogramowania.

W obszarze zarządzania bezpieczeństwem informacji wśród ekspertów PTI znajdują się osoby posiadające kwalifikacje w zakresie prowadzenia testów penetracyjnych, certyfikaty Certified Ethical Hacker (CEH) wydane przez EEC-Council, certyfikaty audytorów wiodących systemu zarządzania bezpieczeństwem informacji zgodnego z normą ISO/IEC 2700.

Rzeczoznawcy PTI posiadają Poświadczenia Bezpieczeństwa ABW umożliwiające dostęp do informacji niejawnych do poziomu objętego klauzulą „tajne" lub „poufne".

Kluczowe obszary prac realizowanych przez **Izbę Rzeczoznawców PTI** to:

- opracowywanie strategii i koncepcji informatyzacji,
- wykonywanie ekspertyz i opinii,
- przeprowadzanie audytów, w tym audytów bezpieczeństwa systemów informatycznych,
- wsparcie merytoryczne przy przygotowywaniu SIWZ oraz przy prowadzeniu procesu przetargowego,
- wsparcie i udział w pracach komitetów sterujących projektów informatycznych,
- badanie, analiza i ocena projektów informatycznych oraz systemów i rozwiązań informatycznych,
- pełnienie obowiązków biegłego instytucjonalnego.

Gwarancją ochrony interesów klientów **Izby Rzeczoznawców PTI** są:

- niezależność i obiektywizm rzeczoznawcy,
- rzetelność treści odniesiona do aktualnej wiedzy i najlepszych praktyk zawodowych,
- zachowanie poufności wszelkich otrzymanych informacji,
- recenzja wewnętrzna wykonanych przez rzeczoznawców opracowań.

Siłą **Izby Rzeczoznawców PTI** są profesjonalni, bezstronni, obiektywni i niezależni eksperci oraz wysoka jakość świadczonych przez nich usług.

dr inż. Przemysław Jatkiewicz – jest rzeczoznawcą Polskiego Towarzystwa Informatycznego, biegłym sądowym w zakresie informatyki obejmującej zagadnienia bezpieczeństwa informacji, wdrażania technologii informatycznych, zarządzania systemami informatycznymi oraz informatyki śledczej przy Sądzie Okręgowym w Gdańsku, a także biegłym skarbowym przy Izbie Skarbowej w Gdańsku. W swojej karierze zawodowej był technikiem, wdrożeniowcem i programistą. Związany jest z Gdańskim Zarządem Nieruchomości Komunalnych Samorządowy Zakład Budżetowy, gdzie początkowo zatrudniony był na stanowisku kierownika działu informatycznego. Obecnie pełni funkcję pełnomocnika dyrektora do spraw bezpieczeństwa informacji. Bierze również udział w projektach realizowanych przez Gminę Gdańsk jako członek komitetu sterującego oraz członek zespołu zadaniowego.

Prowadził badania, za które uzyskał stypendium InnDoktorant, II edycja 2011. Jego zainteresowania badawcze skupiają się na bezpieczeństwie informacji jednostek samorządu terytorialnego. Prowadzi wykłady na Uniwersytecie Gdańskim.

ISBN 978–83–60810–71–2

POLSKIE TOWARZYSTWO INFORMATYCZNE

Polskie Towarzystwo Informatyczne
Izba Rzeczoznawców
www.pti.org.pl