CYBERBEZPIECZEŃSTWO

redakcja naukowa
Cezary Banasiński, Marcin Rojszczak

Cezary Banasiński, Jacek Maria Chmielewski
Władysław Hydzik, Jacek Łuczak, Włodzimierz Nowak
Marcin Rojszczak, Kazimierz Waćkowski

PRAWO W PRAKTYCE

Wolters Kluwer

CYBERBEZPIECZEŃSTWO

redakcja naukowa
Cezary Banasiński, Marcin Rojszczak

Cezary Banasiński, Jacek Maria Chmielewski
Władysław Hydzik, Jacek Łuczak, Włodzimierz Nowak
Marcin Rojszczak, Kazimierz Waćkowski

PRAWO W PRAKTYCE

Wolters Kluwer

WARSZAWA 2020

Recenzent
Dr hab. Paweł Fajgielski, prof. KUL

Wydawca
Agata Jędrasik

Redaktor prowadzący
Kinga Zając

Opracowanie redakcyjne i łamanie
Violet Design Wioletta Kowalska

Projekt okładek serii
Wojtek Kwiecień-Janikowski, Przemek Dębowski

Poszczególne rozdziały napisali:

Cezary Banasiński – I
Władysław Hydzik – VII
Jacek Łuczak – III
Włodzimierz Nowak – IV
Marcin Rojszczak – II, VIII, IX
Kazimierz Waćkowski, Jacek Maria Chmielewski – V, VI

ISBN 978-83-8187-059-7

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

www.wolterskluwer.pl
księgarnia internetowa www.profinfo.pl

SPIS TREŚCI

WYKAZ SKRÓTÓW

Akty prawne

dyrektywa NIS	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 194, s. 1)
dyrektywa PSD2	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z 25.11.2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz.Urz. UE L 337, s. 35, ze sprost.)
k.c.	–	ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2019 r. poz. 1145 ze zm.)
k.k.	–	ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2019 r. poz. 1950 ze zm.)
k.p.k.	–	ustawy z 6.06.1997 r. – Kodeks postępowania karnego (Dz.U. z 2018 r. poz. 1987 ze zm.)
pr. tel.	–	ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2019 r. poz. 2460 ze zm.)
RODO	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1, ze sprost.)
rozporządzenie 2018/151	–	rozporządzenie wykonawcze Komisji (UE) 2018/151 z 30.01.2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz.Urz. UE L 26, s. 48)
rozporządzenie 2018/389	–	rozporządzenie delegowane Komisji (UE) 2018/389 z 27.11.2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (Dz.Urz. UE L 69 z 2018 r., s. 23)

rozporządzenie 2019/881 – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z 17.04.2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.Urz. UE L 151, s. 15)

u.k.s.c. – ustawa z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. poz. 1560 ze zm.)

u.o.d.o. – ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781)

u.ś.u.d.e. – ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2019 r. poz. 123 ze zm.)

u.z.k. – ustawa z 26.04.2007 r. o zarządzaniu kryzysowym (Dz.U. z 2019 r. poz. 1398)

Inne

ABW – Agencja Bezpieczeństwa Wewnętrznego

API – interfejs programowania aplikacji (ang. *Application Programming Interface*)

CERT/CC – zespół szybkiego reagowania na zagrożenia komputerowe/centrum koordynacji (ang. *Computer Emergency Response Team/Coordination Center*)

CIRT – zespół reagowania na incydenty komputerowe (ang. *Computer Incident Response Team*)

COBIT – cele kontrolne dla informatyki i technologii powiązanych (ang. *Control Objectives for Information and related Technology*)

CSIRT – zespół reagowania na incydenty bezpieczeństwa komputerowego (ang. *Computer Security Incident Response Team*)

DHS – Departament Bezpieczeństwa Wewnętrznego

ENISA – Europejska Agencja do spraw Bezpieczeństwa Sieci i Informacji (ang. European Network and Information Security Agency)

FTC – Federalna Komisja Handlu (ang. Federal Trade Commission)

GRC – zarządzanie, ryzyko, zgodność (ang. *Governance, Risk, Compliance*)

IAM – system zarządzania tożsamością (ang. *Identity and Access Management*)

ICT – systemy teleinformatyczne (ang. *Information and Communication Technologies*)

IDS – system wykrywania intruzów (ang. *Intrusion Detection System*)

IEC – Międzynarodowa Komisja Elektrotechniczna (ang. International Electrotechnical Commission)

IoT – ochrona tzw. Internetu rzeczy (ang. *Internet of Things*)

IPS – system wykrywania i blokowania ataków (ang. *Intrusion Prevention System*)

ISO – Międzynarodowa Organizacja Normalizacyjna (ang. International Standards Organization)

IT – technologia informacyjna (ang. *information technology*)

ITIL – standard dla zarządzania usługami informatycznymi (ang. *Information Technology Infrastructure Library*)

KNF – Komisja Nadzoru Finansowego

KPI – współczynniki skuteczności i efektywności procesu (ang. *Key Performance Indicators*)

SABSA – metoda budowy architektury bezpieczeństwa (ang. *Sherwood Applied Business Security Architecture*)
MON – Minister Obrony Narodowej
NASK – Naukowa Akademicka Sieć Komputerowa
NATO – Organizacja Traktatu Północnoatlantyckiego (ang. North Atlantic Treaty Organization)
NIST – Narodowy Instytut Standardów i Technologii
ONZ – Organizacja Narodów Zjednoczonych
OT – systemy sterowania przemysłowego (ang. *Operational Technology*)
OTP – szyfr strumieniowy z jednorazowym kluczem symetrycznym (ang. *One-Time Pad*)
PDCA – zaplanuj – wykonaj – sprawdź – działaj (ang. *Plan – Do – Check – Act*)
PIB – Państwowy Instytut Badawczy
PKB – produkt krajowy brutto
PKI – infrastruktura klucza publicznego (ang. *Public Key Infrastructure*)
PPK – Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa
RCB – Rządowe Centrum Bezpieczeństwa
RP – Rzeczpospolita Polska
SCADA – system informatyczny nadzorujący przebieg procesu technologicznego (ang. *Supervisory Control And Data Acquisition*)
SERT – zespół szybkiego reagowania na zagrożenia bezpieczeństwa (ang. *Security Emergency Response Team*)
SN – Sąd Najwyższy
SSO – system jednokrotnej rejestracji (ang. *Single Sign-On*)
SZBI – system zarządzania bezpieczeństwem informacji (ang. *Information Security Management System*)
UE – Unia Europejska
UKE – Urząd Komunikacji Elektronicznej
UODO – Urząd Ochrony Danych Osobowych
UOKiK – Urząd Ochrony Konkurencji i Konsumentów
ZUS – Zakład Ubezpieczeń Społecznych

WSTĘP

W dobie coraz bardziej powszechnej cyfryzacji i zarazem komunikacji za pośrednictwem sieci teleinformatycznych kwestia bezpieczeństwa systemów IT przestaje być wyłącznie przedmiotem zainteresowania wąskiej grupy specjalistów. Problematyka ta pojawia się w centrum uwagi nie tylko prawodawcy stojącego przed wyzwaniem regulowania zjawisk dotychczas mu nieznanych, administracji zobowiązanej do sprawnego adresowania problemów coraz bardziej sieciowego państwa i społeczeństwa, lecz także gospodarki wykorzystującej technologie informatyczne umożliwiające uruchomianie nowych kanałów generowania przychodów i tym samym dotarcie do nowych rynków. Cyfryzacja niesie ze sobą nie tylko korzyści, ale również istotne ryzyka społeczne i gospodarcze, jak zakłócające działanie systemów informatycznych włamania, wycieki danych czy inne negatywne zjawiska, nie tylko podważające zaufanie do procesów cyfryzacji, ale przede wszystkim przynoszące wymierne straty użytkownikom sieci.

Stąd też wiedza dotycząca bezpieczeństwa systemów IT staje się standardem działania każdego ich użytkownika. Niniejsza książka jest próbą usystematyzowania wiedzy o zagrożeniach dla systemów IT oraz środkach i procesach umożliwiających bezpieczne z nich korzystanie. Adresowana jest zarówno do administracji, przedsiębiorców, jak i zwykłych użytkowników Internetu.

Książka zawiera najważniejsze kwestie z zakresu bezpieczeństwa w cyberprzestrzeni. Jej punktem wyjścia jest omówienie najważniejszych regulacji wpływających na obszar cyberbezpieczeństwa, obejmujących nie tylko przepisy prawa powszechnie obowiązującego, lecz także rekomendacje regulatorów i organizacji branżowych oraz niezbędne regulacje własne dotyczące architektury korporacyjnej i architektury bezpieczeństwa w każdej organizacji (rozdział I). Istotnym elementem każdego systemu cyberbezpieczeństwa są użytkownicy. Dlatego też w kolejnym rozdziale przedstawiono kluczowe zasady cyberhigieny, rozumiane jako zestaw najważniejszych zasad, których przestrzeganie może znacząco zminimalizować narażenie na ryzyka związane z cyberzagrożeniami. W rozdziale II przedyskutowano także dostępne dla użytkowników mechanizmy ochrony prawnej związane z naruszeniami danych osobowych, jak również omówiono procedury postępowania w przypadku zabezpieczenia

dowodów elektronicznych. Przenosząc dyskusję na poziom cyberbezpieczeństwa organizacji, przedstawione wcześniej podstawowe informacje stały się podstawą dla analizy cyberbezpieczeństwa jako procesu, jego oceny, w tym stopnia dojrzałości systemu bezpieczeństwa oraz oceny ryzyka w zarządzaniu nim. Omówiono także pętlę PDCA i kluczowe zabezpieczenia proceduralne na przykładzie międzynarodowych norm standaryzacyjnych ISO 27001 oraz ISO 27032 (rozdział III). W dalszej kolejności opisano specyfikę zagrożeń w cyberprzestrzeni oraz ich podział, kształtujący warstwowy model cyberbezpieczeństwa (jednostka, organizacja, państwo), a także podział zagrożeń ze strony intruza wewnętrznego i zewnętrznego z ich odmiennymi motywacjami, wiedzą atakującego czy możliwymi konsekwencjami (rozdział IV). Kwestie te uzupełnia przegląd najważniejszych zabezpieczeń technicznych, pozwalający na poznanie technik zwiększających poziom ochrony systemów IT, takie jak: zarządzanie podatnościami, testy penetracyjne czy mechanizmy ochrony przed malware (rozdział V). Odrębnie omówiono wprowadzenie do kryptograficznej ochrony danych (rozdział VI), wyjaśniając podstawowe koncepcje, takie jak funkcje skrótu czy kryptografia klucza publicznego, a także przedstawiając mechanizmy ochrony kryptograficznej oraz podstawowe techniki kryptoanalizy. Niezależnie od zastosowanych mechanizmów bezpieczeństwa IT ryzyko wystąpienia incydentów nie może być całkowicie wyeliminowane. Dlatego istotne jest także poznanie procedur postępowania w przypadku wystąpienia incydentu oraz omówienie możliwych działań przygotowawczych i następczych (rozdział VII). Dopełnieniem tej problematyki jest prezentacja możliwych strategii ataku i obrony w cyberprzestrzeni – a więc analiza przypadków, przedstawiająca wybrane cyberataki wraz z praktycznym wyjaśnieniem, jaka była rola błędów ludzkich, złej konfiguracji, istniejących podatności na ich wystąpienie, a także jaka była motywacja atakujących i czy ich cele zostały osiągnięte, a w końcu jakie działania doskonalące zostały wdrożone (rozdział VIII). Ostatnia część książki jest próbą odpowiedzi na pytanie, na ile istniejące regulacje prawne dotyczące bezpieczeństwa w cyberprzestrzeni są skuteczne, oraz przedstawieniem bardziej ogólnych wniosków związanych z oczekiwanymi zmianami w zakresie wdrażanego w Polsce i UE modelu ochrony cyberprzestrzeni (rozdział IX).

Założeniem autorów było praktyczne połączenie niezbędnej wiedzy teoretycznej oraz informacji praktycznych, umożliwiających skuteczne wdrożenie systemów bezpieczeństwa IT w każdej organizacji. Łącząc problematykę z obszaru nauk ścisłych, jak i nauk społecznych, książka dąży do ich zrównoważenia, co sprawia, że jest przystępna dla każdego Czytelnika niezależnie od kierunku jego wykształcenia. Każdy, kto jest zainteresowany bezpieczeństwem systemów IT, znajdzie w niej coś interesującego dla siebie.

Autorzy

Rozdział I

PRAWNE I POZAPRAWNE ŹRÓDŁA WYMAGAŃ DLA SYSTEMÓW CYBERBEZPIECZEŃSTWA

1. Wprowadzenie

Podstawy prawne cyberbezpieczeństwa przedsiębiorcy nie są jednolite z punktu widzenia charakteru norm prawnych regulujących bezpieczeństwo w cyberprzestrzeni. Obok unormowań prawa powszechnie obowiązującego nie bez znaczenia są także unormowania tzw. prawa miękkiego (*soft law*), zawarte zarówno w rekomendacjach organów regulacyjnych, jak i krajowych i międzynarodowych organizacji branżowych. Równie istotne są unormowania własne, zwłaszcza oparte na normach ISO lub standardach korporacyjnych.

2. Krajowy system cyberbezpieczeństwa

Podstawy prawne cyberbezpieczeństwa zawarte w przepisach prawa powszechnie obowiązującego tworzy ustawa z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa[1]. Ustawa ta wdraża do krajowego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[2], zmieniając również niektóre przepisy w ustawy z 7.09.1991 r. o systemie oświaty[3], ustawy z 16.07.2004 r. – Prawo telekomunikacyjne[4] oraz ustawy z 26.04.2007 r. o zarządzaniu kryzysowym[5]. Ustawa powiela materialne i proceduralne postanowienia dyrektywy NIS, dostosowując jednocześnie jej regulacje do warunków krajowych.

[1] Dz.U. poz. 1560 ze zm.; dalej u.k.s.c.
[2] Dz.Urz. UE L 194, s. 1; dalej dyrektywa NIS.
[3] Dz.U. z 2019 r. poz. 1481 ze zm.
[4] Dz.U. z 2019 r. poz. 2460 ze zm.; dalej pr. tel.
[5] Dz.U. z 2019 r. poz. 1398; dalej u.z.k.

Celem ustawy o krajowym systemie cyberbezpieczeństwa jest określenie organizacji oraz sposobu funkcjonowania krajowego systemu cyberbezpieczeństwa, jak i sposobu sprawowania nadzoru i kontroli w zakresie stosowania jej przepisów; uzupełniająco ustawa normuje także zakres i tryb stanowienia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Ustawa o krajowym systemie cyberbezpieczeństwa nie ma zastosowania wobec przedsiębiorców telekomunikacyjnych w rozumieniu art. 2 pkt 27 pr. tel. w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, dostawców usług zaufania, czyli usług elektronicznych świadczonych za wynagrodzeniem i obejmujących: 1) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; 2) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; 3) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami[6] oraz podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Agencji Wywiadu.

Cyberbezpieczeństwo oznacza – w myśl ustawy o krajowym systemie cyberbezpieczeństwa – odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy (art. 2 pkt 4 u.k.s.c.). Pojęcie to stanowi w istocie normatywną konstrukcję myślową oznaczającą bezpieczeństwo systemów i sieci (IT).

Działania tego rodzaju, jeżeli mają lub mogą mieć niekorzystny wpływ na cyberbezpieczeństwo, określane są w ustawie jako incydenty (art. 2 pkt 5 u.k.s.c.). Tę ogólną definicję konkretyzuje w pewnym sensie norma ISO/IEC 27000, w której przyjmuje się w odniesieniu do systemów zarządzania bezpieczeństwem informacji, że incydentem jest każde pojedyncze, nieoczekiwane i niechciane zdarzenie lub ich seria, jeżeli wiąże się z istotnym prawdopodobieństwem narażenia działalności danego podmiotu, stanowiąc zagrożenie dla bezpieczeństwa przetwarzanych informacji.

Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa incydenty podlegają różnicowaniu w zależności od stopnia ich oddziaływania na systemy informacyjne.

Incydent krytyczny to taki, który skutkuje znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi;

[6] Art. 3 pkt 16 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z 23.07.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz.Urz. UE L 257, s. 73).

incydent krytyczny klasyfikowany jest przez właściwy tzw. zespół reagowania na incydenty bezpieczeństwa komputerowego (ang. *Computer Security Incident Response Team* – CSIRT).

Incydent poważny odnosi się do usług kluczowych i oznacza spowodowanie lub możliwość spowodowania poważnego obniżenia jakości lub przerwaniem ciągłości świadczenia usługi kluczowej. Progi uznania incydentu za poważny, w poszczególnych sektorach i podsektorach określonych w załączniku nr 1 do ustawy o krajowym systemie cyberbezpieczeństwa, określa rozporządzenie Rady Ministrów z 31.10.2018 r. w sprawie progów uznania incydentu za poważny[7].

Incydent istotny odnosi się do usług cyfrowych i oznacza incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z 30.01.2018 r. ustanawiającego zasady stosowania dyrektywy NIS w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ[8]. W myśl tego przepisu incydent uznaje się za mający istotny wpływ, jeżeli zaistniała co najmniej jedna z następujących sytuacji: a) usługa świadczona przez dostawcę usług cyfrowych była niedostępna przez ponad 5 000 000 użytkownikogodzin, przy czym pojęcie „użytkownikogodzina" odnosi się do liczby dotkniętych incydentem użytkowników w Unii przez okres sześćdziesięciu minut; b) incydent doprowadził do utraty integralności, autentyczności lub poufności przechowywanych lub przekazywanych bądź przetwarzanych danych lub powiązanych usług, oferowanych bądź dostępnych poprzez sieci i systemy informatyczne dostawcy usług cyfrowych, która dotknęła ponad 100 000 użytkowników w Unii; c) incydent spowodował ryzyko dla bezpieczeństwa publicznego lub ryzyko wystąpienia ofiar śmiertelnych; d) incydent wyrządził co najmniej jednemu użytkownikowi w Unii stratę materialną, której wysokość przekracza 1 000 000 euro. Progi istotności dla incydentów w odniesieniu do usług kluczowych określa rozporządzenie Rady Ministrów z 11.09.2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych[9].

Szczególną kategorią jest incydent w podmiocie publicznym, czyli taki, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.

Incydent zwykły to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo; tego rodzaju incydenty nie podlegają zgłoszeniu.

[7] Dz.U. poz. 2180.
[8] Dz.Urz. UE L 26, s. 48; dalej rozporządzenie 2018/151.
[9] Dz.U. poz. 1806.

Cezary Banasiński – pracownik naukowy na Wydziale Prawa i Administracji Uniwersytetu Warszawskiego; specjalista w dziedzinie publicznego prawa gospodarczego; w latach 1999–2001 był wiceministrem w Urzędzie Komitetu Integracji Europejskiej odpowiedzialnym za dostosowanie prawa polskiego do prawa UE; w latach 2001–2007 pełnił funkcję Prezesa Urzędu Ochrony Konkurencji i Konsumentów; obecnie łączy pracę naukową z praktyką stosowania prawa, w tym zwłaszcza prawa ochrony konkurencji; autor wielu publikacji z zakresu prawa gospodarczego oraz prawa Unii Europejskiej.

Marcin Rojszczak – doktor nauk prawnych; pracownik naukowy Politechniki Warszawskiej; specjalista w zakresie bezpieczeństwa IT oraz ochrony prywatności w internecie; od ponad 15 lat realizuje i nadzoruje projekty z obszaru bezpieczeństwa informacji, zarządzania usługami IT oraz ciągłości działania (DRP/BCP) w największych polskich firmach sektorów: energetycznego, finansowego i produkcyjnego, a także urzędach administracji centralnej; w latach 2012–2015 członek Rady ds. Certyfikacji Polskiego Komitetu Normalizacyjnego.

Autorzy omawiają najważniejsze kwestie z zakresu bezpieczeństwa w cyberprzestrzeni zarówno z perspektywy prawa, jak i technologii.

W opracowaniu przedstawiono m.in.:
- najważniejsze regulacje wpływające na obszar cyberbezpieczeństwa,
- mechanizmy ochrony prawnej związane z naruszeniami danych osobowych,
- procedury postępowania w zakresie zabezpieczenia dowodów elektronicznych,
- najważniejsze zasady, które należy uwzględnić w budowanych programach cyberhigieny dla użytkowników,
- cyberbezpieczeństwo jako proces, a także wyjaśniono, w jaki sposób możliwe jest zdefiniowanie mierników jego oceny,
- najważniejsze zabezpieczenia techniczne, w tym związane z kryptograficzną ochroną danych,
- procedury postępowania w przypadku wystąpienia incydentu,
- strategie ataku i obrony w cyberprzestrzeni.

Publikacja jest przeznaczona dla osób zajmujących się cyberbezpieczeństwem; będzie cennym źródłem wiedzy nie tylko dla operatorów usług kluczowych i dostawców usług cyfrowych, lecz także wszystkich innych przedsiębiorców, których dotyczą zagadnienia z obszaru bezpieczeństwa IT oraz zarządzania incydentami i audytem wewnętrznym struktur IT. Zainteresuje również pracowników administracji rządowej, a zwłaszcza administracji samorządowej. Jest przeznaczona również dla studentów oraz słuchaczy studiów podyplomowych nie tylko na uczelniach technicznych.

9788381870597 W01P01

ISBN 978-83-8187-059-7

9 788381 870597

CENA 129 ZŁ (W TYM 5% VAT)