NOWOCZESNE SYSTEMY ŁĄCZNOŚCI I TRANSMISJI DANYCH NA RZECZ BEZPIECZEŃSTWA

SZANSE I ZAGROŻENIA

redakcja naukowa
Andrzej R. Pach, Zbigniew Rau, Michał Wągrowski

LEX
a Wolters Kluwer business

PPBW

NOWOCZESNE SYSTEMY ŁĄCZNOŚCI I TRANSMISJI DANYCH NA RZECZ BEZPIECZEŃSTWA

SZANSE I ZAGROŻENIA

redakcja naukowa
Andrzej R. Pach, Zbigniew Rau, Michał Wągrowski

Zamów książkę w księgarni internetowej
profinfo.pl
księgarnia internetowa

LEX
a Wolters Kluwer business

Warszawa 2013

Praca naukowa finansowana ze środków na naukę w latach 2010–2012 jako projekt badawczo-rozwojowy Ministerstwa Nauki i Szkolnictwa Wyższego pt.: Prototyp terminala radiokomunikacyjnego o zwiększonej odporności na zakłócenia i podsłuchy, przeznaczony dla administracji publicznej nr OR00015211, realizowanego przez Akademię Górniczo-Hutniczą im. St. Staszica w Krakowie, PPBW sp. z o.o. oraz DGT sp. z o.o.

Redaktorzy naukowi dziękują Panu Łukaszowi Ignatowiczowi za pomoc w pracach nad publikacją.

Recenzent
Prof. dr hab. inż. Andrzej Dąbrowski – kierownik Zakładu Systemów Teletransmisyjnych Politechniki Warszawskiej, członek IEEE, AFCEA, członek Komitetu Elektroniki i Telekomutacji PAN, członek szeregu rad naukowych i komitetów programowych, w tym: przewodniczący Komitetu Programowego KSTiT, wiceprzewodniczący Rady Naukowej NASK, koordynator ze strony polskiej szeregu programów międzynarodowych, w tym projektu TWISTER.

Wydawca
Monika Pawłowska

Redaktor prowadzący
Ewa Fonkowicz

Opracowanie redakcyjne
„Littera" Maria Beata Wawrzyńczak-Jędryka

Łamanie
„Littera" Maria Beata Wawrzyńczak-Jędryka

© Copyright by
Wolters Kluwer Polska SA, 2013

ISBN: 978-83-264-4255-1
ISBN PDF-a: 978-83-264-6248-1

Wydane przez:
Wolters Kluwer Polska SA

Redakcja Książek
01-231 Warszawa, ul. Płocka 5a
tel. 22 535 82 00, fax 22 535 81 35
e-mail: ksiazki@wolterskluwer.pl

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

Spis treści

Wykaz skrótów

Akty prawne

k.k.	– ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. Nr 88, poz. 553 z późn. zm.)
k.k.w.	– ustawa z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Dz. U. Nr 90, poz. 557 z późn. zm.)
Konstytucja RP	– Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.)
k.p.k.	– ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555 z późn. zm.)
Prawo telekomunikacyjne	– ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800 z późn. zm.)
u.b.i.m.	– ustawa z dnia 20 marca 2009 r. o bezpieczeństwie imprez masowych (tekst jedn.: Dz. U. z 2013 r. poz. 611 z późn. zm.)
ustawa o ABW oraz AW	– ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jedn.: Dz. U. z 2010 r. Nr 29, poz. 154 z późn. zm.)
ustawa o CBA	– ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (tekst jedn.: Dz. U. z 2012 r. poz. 621 z późn. zm.)
ustawa o KRS	– ustawa z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym (tekst jedn.: Dz. U. z 2007 r. Nr 168, poz. 1186 z późn. zm.)
ustawa o Policji	– ustawa z dnia 6 kwietnia 1990 r. o Policji (tekst jedn.: Dz. U. z 2011 r. Nr 287, poz. 1687 z późn. zm.)
ustawa o SKW oraz SWW	– ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 z późn. zm.)

Czasopisma, promulgatory, inne

ABW	– Agencja Bezpieczeństwa Wewnętrznego
AW	– Agencja Wywiadu
CBA	– Centralne Biuro Antykorupcyjne
CBŚ	– Centralne Biuro Śledcze
Dz. U.	– Dziennik Ustaw
Dz. Urz. UE	– Dziennik Urzędowy Unii Europejskiej
ETPC	– Europejski Trybunał Praw Człowieka

GIODO	– Generalny Inspektor Ochrony Danych Osobowych
KCIK	– Krajowe Centrum Informacji Kryminalnych
KGP	– Komenda Główna Policji
KSIP	– Krajowy System Informacyjny Policji
LEX	– System Informacji Prawnej „Lex Omega" Wolters Kluwer Polska
OSNKW	– Orzecznictwo Sądu Najwyższego. Izba Karna i Wojskowa
OSPiKA	– Orzecznictwo Sądów Polskich i Komisji Arbitrażowych
OTK	– Orzecznictwo Trybunału Konstytucyjnego
OTK-A	– Orzecznictwo Trybunału Konstytucyjnego – zbiór urzędowy, Seria A
PSTD	– Policyjna Sieć Transmisji Danych
SA	– Sąd Apelacyjny
SN	– Sąd Najwyższy
TK	– Trybunał Konstytucyjny
UE	– Unia Europejska
ZSIP	– Zintegrowany System Informacyjny Policji

Wprowadzenie

Niniejsza monografia powstała z inicjatywy Polskiej Platformy Bezpieczeństwa Wewnętrznego oraz dzięki środkom finansowym ze zrealizowanego projektu badawczo-rozwojowego NCBiR nr OR00015211, pt. „Prototyp terminala radiokomunikacyjnego o zwiększonej odporności na zakłócenia i podsłuchy, przeznaczony dla administracji publicznej" (*A Prototype of a Disruption – and Eavesdropping – resistant Radiocommunication Terminal for Public Administration*), kierowanego przez Akademię Górniczo-Hutniczą w Krakowie. Monografia dotyczy wykorzystania nowoczesnych środków łączności oraz metod przechowywania, przetwarzania i transmisji danych na rzecz szeroko rozumianego bezpieczeństwa. Zaproszenie do udziału w przedsięwzięciu zostało skierowane do ośrodków naukowych, przemysłowych, firm komercyjnych, organów porządku prawnego i bezpieczeństwa państwa oraz wymiaru sprawiedliwości. Redakcja nie ingerowała w merytoryczną treść artykułów – są one zamieszczone w wersji autorskiej i na odpowiedzialność Autorów. Przedstawione opracowania traktują tematykę bezpieczeństwa z różnej perspektywy, zarówno w aspekcie technicznym, jak i prawnym, ekonomicznym oraz etyczno-społecznym. Naszym zamierzeniem było przedstawienie możliwości, jakie niesie ze sobą rozwój nowoczesnych rozwiązań teleinformatycznych, ale także zagrożeń dotyczących naruszeń prywatności, które trzeba wziąć pod uwagę przy ich wdrażaniu. Mamy nadzieję, że lektura monografii dostarczy Państwu argumentów z tych różnych płaszczyzn i pozwoli wyrobić sobie własne zdanie w sprawie powyższego kompromisu.

Monografia stanowi kompendium wiedzy z zakresu budowy bezpiecznych systemów przechowywania, przetwarzania i transmisji danych, jak również ich wykorzystania w świetle obowiązujących przepisów prawa i orzecznictwa sądów powszechnych, w tym Sądu Najwyższego. Artykuły nawiązują z jednej strony do problemu likwidacji podziałów wynikających z wykluczenia cyfrowego oraz budowy społeczeństwa informacyjnego, z drugiej zaś podejmuje problem osób, które z różnych względów nie chcą lub nie mogą korzystać z sieci teleinformatycznej. Przedstawiono zagadnienia związane z budową polskiego systemu łączności bezpieczeństwa publicznego, ale zawarto również rozważania o skali możliwej ingerencji Państwa w wolności obywatelskie w kontekście zapisów prawa telekomunikacyjnego i tzw. ustaw branżowych poszczególnych służb policyjnych uprawnionych do niejawnego pobierania i przetwarzania danych o obywatelach.

Nadesłane artykuły pogrupowano tematycznie w pięć części. Pierwsza dotyczy bezpieczeństwa przechowywania i przesyłu danych, w tym głównie aspektów kryptograficznych. W części drugiej przedstawiono systemy bezpieczeństwa publicznego z uwzględnieniem różnych rozwiązań technologicznych, stosowanych obecnie w Polsce i na świecie. W kolejnej części podjęto temat ochrony infrastruk-

tur krytycznych, w ramach którego zaprezentowano m.in. stosowane metodyki zapewnienia bezpieczeństwa informacji. Część czwarta zawiera artykuły techniczne na temat urządzeń i systemów teleinformatycznych przeznaczonych do zastosowania w administracji, kryminalistyce i sądownictwie. W tej części zamieszczono również szereg artykułów opisujących potrzeby oraz doświadczenia wynikające z użytkowania nowoczesnych narzędzi informatycznych przez powyższe organy państwowe w realiach obecnej sytuacji prawno-ekonomicznej. Ostatnia, piąta część, zawiera opracowania o charakterze prawno-etycznym i dotyczy ochrony prywatności i bezpieczeństwa obywateli w kontekście wykorzystania nowoczesnych technologii.

W Polsce temat konieczności zbudowania niezawodnej, profesjonalnej sieci łączności dla służb publicznych obecny jest w dialogu technicznym i społecznym już od dłuższego czasu. Pierwsze pomysły na modernizację i integrację systemów łączności pojawiły się w latach 2001–2003 w kontekście środków offsetowych, związanych z zakupem amerykańskich samolotów bojowych F16. Jednak przedstawiane co pewien czas kolejne propozycje nie doczekały się jak dotąd realizacji, nawet te ostatnio mocno akcentowane i podejmowane w związku z organizacją w naszym kraju turnieju piłkarskiego EURO 2012. Typowe systemy PPDR (*Public Protection and Disaster Relief*) cechują się szczególnymi wymaganiami dotyczącymi realizacji połączeń grupowych oraz niezawodności działania w sytuacjach kryzysowych. Wykorzystywane m.in. przez służby publiczne (policję, pogotowie ratunkowe, straż pożarną i inne), stanowią ważny element sprawnego zarządzania kryzysowego. W przypadku wystąpienia katastrof, klęsk żywiołowych, awarii przemysłowych, zagrożeń militarnych, w tym ataków terrorystycznych lub nawet podczas organizacji imprez masowych, gdy zawodzą publiczne sieci telekomunikacyjne, łączność dla służb powinna opierać się na niezależnej infrastrukturze systemów PMR (*Professional Mobile Radio*). Polska nadal stoi przed ważnymi decyzjami w tej sprawie i jak do tej pory, niestety, prezentuje się nie najlepiej, w porównaniu z innymi krajami Unii Europejskiej, pod względem posiadanej infrastruktury i rozwiązań (zarówno tych technicznych, jak i prawnych) stosowanych w zakresie systemów PPDR. Mamy nadzieję, że niniejsza monografia wniesie konstruktywny wkład do dyskursu prowadzonego w kwestii tak kluczowej dla naszego kraju, jak zapewnienie bezpieczeństwa, w tym, w szczególności, bezpieczeństwa łączności i przesyłu danych.

Składamy podziękowania wszystkim Autorom artykułów oraz instytucjom współpracującym przy wydaniu tej monografii za wkład intelektualny i pomoc organizacyjno-merytoryczną przy wydaniu tego tak obszernego opracowania.

Redaktorzy naukowi:
prof. dr hab. inż. Andrzej R. Pach
dr Zbigniew Rau
dr inż. Michał Wągrowski

Introduction

The present monograph has been prepared thanks to the initiative of the Polish Platform for Homeland Security and to the funds from the National Center for Research and Development project no. OR00015211, entitled "A Prototype of a Disruption- and Eavesdropping-resistant Radiocommunication Terminal for Public Administration", led by the AGH University of Science and Technology in Krakow. The subject matter of the monograph is the use of state-of-the-art means of communication and methods of storage, processing, and transmission of data for enhancing broadly-defined security. The invitation to participate in the project was sent to scientific and industrial centers, commercial companies, law enforcement and state security bodies, and institutions of the judiciary. The editors did not interfere with the essential contents of the articles: they are presented in their original versions and at the authors' responsibility. The articles of the monograph present the subject of security from different standpoints, in its legal, economic, ethical, and social aspects. Our intent was to present the opportunities associated with the development of modern information and communication technologies, but also the threats associated with violation of privacy, which must be taken into account when implementing the technologies. We hope that to the readers the contents of this monograph will be a source of knowledge in various fields and will enable them to form their own opinions about the aforementioned dilemma.

The monograph is a digest of knowledge in the field of development of secure systems for storage, processing, and transmission of data, as well as their use in observance of the applicable laws and in the light of verdicts of courts, to include the Supreme Court. On the one hand, the articles discuss the problem of elimination of the digital divide and the development of an information society and, on the other hand, they analyze the problem of persons who, for various reasons, do not want to or are unable to use the Internet. The authors present problems associated with the construction of the Polish system of public security telecommunication but also discuss the extent of possible interference of the state in the citizens' freedoms in the context of the provisions of the telecommunication law and the so-called sector statutes of the different police services authorized to clandestinely download and process data on citizens.

The articles are divided into five groups according to their topics. The first group focuses on secure storage and transfer of data, mainly the cryptographic aspects. The second group presents public security systems, taking into account the different technologies currently used in Poland and abroad. The third part focuses on the topic of protection of critical infrastructure and presents, among others, the contemporary information security methods. The fourth part comprises technical articles on information and communication technology equipment and systems in-

tended for use in public administration, criminalistics, and the judiciary. This part also comprises a number of articles that describe the needs and experiences related to the use of modern information technologies by the aforementioned state bodies given the current legal and economic conditions. The last, fifth group comprises articles on legal and ethical aspects of information and communication technology and focuses on the protection of privacy and security of citizens in the context of use of modern technologies.

In Poland the need to build a reliable, professional communication network for public agencies and institutions has been discussed by technical and social experts for quite a long time. The first ideas to upgrade and integrate the existing communication systems came up in the years 2001–2003 in the context of the offset funds associated with the purchase by Poland of the American F16 fighter planes. However, the recurring proposals have not been implemented so far, even those that have been stressed and recommended lately in connection with the EURO2012 held in Poland. Typical PPDR (Public Protection and Disaster Relief) systems have special requirements concerning group calls and reliability in crisis situations. They are used among others by public agencies and institutions (police, ambulance, fire brigade, etc.) and constitute an important element of effective crisis management systems. In the event of natural or industrial disasters and military threats, to include terrorist attacks, or even during mass events, when public communication networks fail, state agencies must be able to maintain communication using the independent infrastructure of PMR (Professional Mobile Radio) systems. Poland still needs to make important decisions in this area and, unfortunately, so far it has not fared very well compared to other states of the European Union with regards to the infrastructure and solutions (both technical and legal) used in the area of PPDR systems. We hope that the present monograph will make a contribution to the discourse concerning the topic of security, in particular the security of communications and data transfer, which is of such a great importance to Poland.

We would like to thank all the authors of the articles and the institutions that have cooperated in the publication of this monograph for their intellectual input and for their organizational and technical assistance with the publication of such an extensive book.

Scientific Editors:
Professor Andrzej R. Pach
Dr. Zbigniew Rau
Dr. Michał Wągrowski

Einführung

Die vorliegende Monographie entstand auf Initiative der Polnischen Plattform für innere Sicherheit und dank der Finanzmittel aus dem realisierten Forschungsprojekt des Nationalen Zentrums für Forschung und Entwicklung NCBiR mit der Nummer OR00015211 „Prototyp eines Funkterminals mit erhöhtem Störungs- und Abhörwiderstand für die öffentliche Verwaltung (*A Prototype of a Disruption- and Eavesdropping- resistant Radiocommunication Terminal for Public Administration*), das von der Akademie für Bergbau und Metallurgie in Kraków geleitet wird. Diese Monographie betrifft die Nutzung moderner Kommunikationsmittel und der Methoden zur Speicherung, Verarbeitung und Übertragung von Daten zur Gewährleistung einer breit verstandenen Sicherheit. Einladungen zur Teilnahme an dieser Unternehmung wurden an wissenschaftliche und industrielle Zentren, kommerzielle Firmen, Organe der öffentlichen Ordnung und der Staatssicherheit sowie die Justizbehörden versandt. Die Redaktion greift nicht in den sachlichen Inhalt der Artikel ein – diese werden in der eingesandten Version auf ausschließliche Verantwortung ihrer Autoren veröffentlicht. Die vorgestellten Ausarbeitungen behandeln das Thema der Sicherheit von verschiedenen Gesichtspunkten aus – sowohl in technischer, wie auch in rechtlicher, wirtschaftlicher und ethisch-gesellschaftlicher Hinsicht. Unsere Absicht war es, die Möglichkeiten vorzustellen, die durch die Entwicklung moderner teleinformatischer Lösungen entstehen. Gleichzeitig sollten jedoch auch die Gefahren in Bezug auf die Verletzung der Privatsphäre angesprochen werden, die bei der Umsetzung solcher Lösungen auftreten können. Ich hoffe, dass die Lektüre dieser Monographie Sie mit Argumenten auf verschiedenen Ebenen versorgt und es Ihnen ermöglicht, sich ein eigenes Bild über den oben erwähnten Kompromiss zu machen.

Die Monographie stellt ein Kompendium des Wissens im Bereich des Baus sicherer Systeme zur Speicherung, Verarbeitung und Übertragung von Daten sowie ihrer Nutzung vor dem Hintergrund der geltenden Rechtsvorschriften und der Rechtsprechung der ordentlichen Gerichte, darunter des Obersten Gerichts, dar. Die Artikel knüpfen auf der einen Seite an das Problem der Liquidierung von Teilungen infolge digitaler Ausgrenzung und den Bau einer Informationsgesellschaft an, und behandelt auf der anderen Seite das Problem von Personen, die aus den verschiedensten Gründen die teleinformatischen Netze nicht nutzen können oder wollen. Dabei wurden Fragen behandelt, die mit dem Bau eines polnischen Fernmeldesystems der öffentlichen Sicherheit verbunden sind. Gleichzeitig wurden jedoch auch Erwägungen über den Umfang der zulässigen Eingriffe des Staates in die bürgerlichen Freiheitsrechte im Zusammenhang mit den Festlegungen des Telekommunikationsrechts und den sogenannten „Branchengesetzen" der einzelnen Polizeidienste, die zur geheimen Erhebung und Verarbeitung von Daten über die Bürger berechtigt sind, angestellt.

Die eingesandten Artikel wurden thematisch in fünf Teile gruppiert. Die erste Gruppe betrifft dabei die Sicherheit der Speicherung und Übertragung von Daten, dar-

unter insbesondere kryptographische Aspekte. In der zweiten Gruppe wurden die Systeme der öffentlichen Sicherheit unter Berücksichtigung verschiedener technologischer Lösungen vorgestellt, die aktuell in Polen und in der Welt zum Einsatz kommen. Der nächste Teil konzentriert sich auf das Thema des Schutzes kritischer Infrastruktur – hier wurden unter anderem Methoden der Garantierung der Informationssicherheit präsentiert. Der vierte Teil umfasst technische Artikel zum Thema der teleinformatischen Geräte und Anlagen, die zum Einsatz in der Verwaltung, der Kriminalistik und dem Gerichtswesen bestimmt sind. Dieser Teil enthält außerdem eine Reihe von Artikeln, die den Bedarf und die Erfahrungen beschreiben, die aus der Nutzung moderner EDV-Werkzeuge durch die oben genannten Staatsorgane unter der Realität der aktuellen Rechts- und Wirtschaftssituation folgen. Der letzte, fünfte Teil enthält Ausarbeitungen mit rechtlich-ethischem Charakter und betrifft den Schutz der Privatsphäre und der Sicherheit der Bürger im Zusammenhang mit der Nutzung moderner Technologien.

In Polen ist das Thema der Notwendigkeit des Baus eines zuverlässigen, professionellen Fernmeldesystems für die öffentlichen Dienste bereits seit längerer Zeit Bestandteil des technischen und gesellschaftlichen Dialogs. Die ersten Ideen zur Modernisierung und Integration der Kommunikationssysteme erschienen in den Jahren 2001–2003 im Zusammenhang mit den Offsetmitteln, die durch den Kauf der amerikanischen Kampfflugzeuge F16 verfügbar waren. Die immer wieder auftauchenden Vorschläge in dieser Hinsicht wurden bisher jedoch nicht umgesetzt, nicht einmal – trotz starker Akzentuierung und Diskussion – im Zusammenhang mit der Organisation der Fußballeuropameisterschaft EURO 2012 in unserem Land. Typische PPDR-Systeme (englisch: Public Protection and Disaster Relief) zeichnen sich durch besondere Anforderungen in Bezug auf die Realisierung von Gruppenverbindungen und ihre Zuverlässigkeit in Krisensituationen aus. Sie werden unter anderem durch die öffentlichen Dienste (Polizei, Rettungsdienste, Feuerwehr u.a.m.) genutzt und stellen ein wichtiges Element eines leistungsfähigen Krisenmanagements dar. Im Falle von Natur- und anderen Katastrophen, schweren industriellen Störungen, militärischen Bedrohungen, wie etwa terroristischen Angriffen, oder sogar bei der Organisation von Massenveranstaltungen muss sich – wenn die öffentlichen Telekommunikationsnetze ausfallen – die Kommunikation der verantwortlichen Dienste auf eine unabhängige Infrastruktur der Systeme des Bündelfunks (PMR – Professional Mobile Radio) stützen. Polen steht immer noch vor wichtigen Entscheidungen in dieser Frage – und das Lande präsentiert sich dabei im Vergleich zu den anderen Ländern der Europäischen Union in Hinsicht auf die verfügbare Infrastruktur und die technischen und rechtlichen Lösungen im Bereich der PPDR-Systeme nicht besonders gut. Wir hoffen, dass diese Monographie einen konstruktiven Beitrag zur Diskussion in dieser für unser Land so wichtigen Frage der Sicherheit und dabei insbesondere der Sicherheit von Verbindungen und Datenübertragungen leisten kann.

Wir möchten an dieser Stelle allen Autoren und mit uns bei der Veröffentlichung dieser Monographie zusammenarbeitenden Institutionen für ihren intellektuellen Beitrag und die organisatorisch-inhaltliche Unterstützung bei der Verlegung einer so umfangreichen Ausarbeitung danken.

Wissenschaftliche Reaktion:
Prof. Dr. hab. Ing. Andrzej R. Pach
Dr. Zbigniew Rau
Dr. Ing. Michał Wągrowski

Введение

Данная монография возникла по инициативе Польской платформы внутренней безопасности, а также благодаря финансовым средствам реализованного исследовательского проекта Национального центра исследований и развития (NCBiR) № OR00015211, под названием „Прототип терминала радиосвязи с повышенной степенью защиты от помех и прослушивания, предназначенный для государственного управления" (*A Prototype of a Disruption- and Eavesdropping- resistant Radiocommunication Terminal for Public Administration*), который вела Краковская горно-металлургическая академия. Монография описывает использование современных средств связи, а также методов хранения, обработки и передачи данных в области безопасности в широком смысле этого слова. Приглашение к участию в проекте было направлено в научные и промышленные центры, коммерческие компании, органы правопорядка и госбезопасности, а также в органы юстиции. Редакция не вмешивалась в существенное содержание статей – они умещены в авторской версии и ответственность за него несут авторы. Представленные разработки по-разному подходят к вопросу безопасности, как с технической точки зрения, так и юридической, экономической и общественно-этической. Нашей целью было показание возможностей, которые несет с собой развитие современных решений в области телеинформатики, но также опасностей, связанных с нарушением приватности, которые нужно принять во внимание при их внедрении. Мы надеемся, что прочтение монографии предоставит вам аргументы в каждой области и позволит выработать собственное мнение по данному вопросу.

Монография представляет собой свод информации в области создания безопасных систем хранения, обработки и передачи данных, а также их использования на основании действующего законодательства и судебной практики судов, включая Верховный суд. В статьях с одной стороны говорится о проблеме устранения информационного неравенства и создании информационного общества, а с другой стороны затрагивается проблема лиц, которые по разным причинам не хотят или не могут пользоваться телеинформатическими сетями. Представлены вопросы, связанные с созданием государственной системы связи национальной безопасности, но также рассмотрены масштабы возможного вмешательства государства в гражданскую свободу в контексте положений закона о телекоммуникациях и, так называемых, отраслевых законов, касающихся различных подразделений полицейских служб, которые имеют право тайно получать и обрабатывать данные о гражданах.

Присланные статьи были сгруппированы по темам и поделены на пять разделов. Первый касается безопасности хранения и передачи данных, в частности аспектов криптографии. Во втором разделе представлены системы об-

щественной безопасности с учетом различных технологических решений, используемых в Польше и во всем мире. В следующем разделе затронута тема защиты критических инфраструктур, в рамках которой представлены, в частности, применяемые методы обеспечения информационной безопасности. Четвертый раздел – это технические статьи об устройствах и телеинформатических системах предназначенных к применению в органах управления, криминалистике и органах юстиции. Этот раздел содержит ряд статей, описывающих потребности и опыт использования вышеупомянутыми органами современных информатических средств в реалиях сегодняшней правовой и экономической ситуации. Последний, пятый раздел, включает в себя разработки, имеющие правовой и этический характер и касаются защиты частной жизни и безопасности граждан в связи с использованием современных технологий.

В Польше тема необходимости создания надежной, профессиональной сети связи для общественных служб уже длительное время присутствует в техническом и общественном диалоге. Первые идеи модернизации и интеграции систем связи появились в 2001–2003 годах в контексте офсетных средств, связанных с закупкой американских боевых самолетов F16. Тем не менее, представляемые раз на какое-то время очередные предложения до сих пор не дождались реализации, даже те, которые особо подчеркивались и предпринимались в последнее время в связи с организацией в нашей стране чемпионата Европы по футболу Евро-2012. Типичные системы PPDR (*Public Protection and Disaster Relief*) отличаются особыми требованиями, касающимися реализации групповых вызовов и надежностью в критических ситуациях. Используются, в частности, общественными службами (полиция, скорая помощь, пожарная охрана и другие), являются важным элементом эффективного управления в чрезвычайных ситуациях. В случае возникновения катастроф, стихийных бедствий, промышленных аварий, военных опасностей, в том числе терактов или даже во время организации массовых мероприятий, когда отказывают общественные телекоммуникационные сети, связь для служб должна базироваться на независимой инфраструктуре систем PMR (*Professional Mobile Radio*). Польша по-прежнему стоит перед необходимостью принятия важных решений по этому вопросу но, к сожалению, по сравнению с другими странами Европейского союза она представляется слабо, с точки зрения имеющейся инфраструктуры и решений (как технических, так и правовых) применяемых в области систем PPDR. Мы надеемся, что данная монография внесет конструктивный вклад в дискурс, проводимый по так важному вопросу для нашей страны, как обеспечение безопасности, особенно безопасности связи и передачи данных.

Мы благодарим всех авторов статей и все учреждения, сотрудничающие при издании этой монографии за интеллектуальный вклад, а также организационную и существенную помощь при издании такой обширной разработки.

Научные редакторы:
Профессор, доктор наук, инженер Анджей Р. Пах
Кандидат наук Збигнев Рау
Кандидат наук, инженер Михал Вонгровски

Część I

BEZPIECZEŃSTWO PRZECHOWYWANIA I PRZESYŁU DANYCH

Tomasz Bilski, Krzysztof Bucholc, Krzysztof Chmiel,
Anna Grocholewska-Czuryło, Ewa Idzikowska,
Izabela Janicka-Lipska, Janusz Stokłosa

Bezpieczeństwo kryptograficzne przesyłania i gromadzenia informacji[1]

Streszczenie

Głównym celem pracy jest zaprezentowanie problemów związanych z projektowaniem bezpiecznych algorytmów kryptograficznych w postaci szyfrów blokowych i funkcji skrótu. Przedstawiono szczegółowo dwa rozwiązania opracowane w Zakładzie Bezpieczeństwa Systemów Informatycznych Instytutu Automatyki i Inżynierii Informatycznej Politechniki Poznańskiej: szyfr blokowy PP-1 i funkcję skrótu HaF. Tytułem wprowadzenia omówiono podstawowe kwestie związane z bezpieczeństwem danych, kryptografią, kryptoanalizą oraz ochroną danych w sieciach komputerowych i systemach przechowywania danych. Głównym celem rozdziału poświęconego szyfrom blokowym jest prezentacja algorytmu PP-1. Jednak na wstępie omówiono ogólnie podstawowe problemy związane z projektowaniem szyfrów blokowych. Szyfr PP-1 jest szyfrem skalowalnym umożliwiającym przetwarzanie bloków danych o rozmiarach 64, 128, 192, 256 bitów (itd.; rozmiar bloku można zwiększać o kolejne 64 bity). Stosowany klucz kryptograficzny może mieć rozmiar równy długości bloku lub podwójnej długości bloku. HaF jest sparametryzowaną rodziną funkcji skrótu i obejmuje trzy funkcje: HaF-256, HaF-512 i HaF-1024, wytwarzające skrót o długości, odpowiednio, 256, 512 i 1024 bitów. Została zaprojektowana zgodnie z modelem Merklego-Damgårda, z uwzględnieniem podejścia HAIFA. Zastosowano w niej duże bloki podstawień o rozmiarze 16×16. Zarówno w PP-1, jak i w HaF położono nacisk na bezpieczeń-

[1] Praca naukowa finansowana ze środków na naukę w latach 2010–2013 jako projekt badawczy.

stwo, godząc się z nieco dłuższymi w stosunku do będących obecnie w użyciu funkcjami skrótu, czasami przetwarzania. Szczególnie jest to widoczne w algorytmie HaF. W pracy zamieszczono wyniki pomiarów wydajności przetwarzania funkcji HaF. Specyficzne dla produktów kryptograficznych jest to, że pojedynczy błąd w procesie przetwarzania prowadzi do wielu błędów na wyjściu. W pracy zaproponowano metody detekcji błędów w implementacjach szyfru blokowego i funkcji skrótu. Szyfr blokowy i funkcja skrótu mogą być użyte w procesie szyfrowania uwierzytelnionego. Zwrócono uwagę na możliwości zastosowania tej techniki z użyciem algorytmów PP-1 i HaF.

Abstract

The main goal of the work is clarification of problems related to secure cryptographic algorithm design with a special emphasis to block ciphers and hash functions. Two, original solutions, developed in Information System Security Department of Institute of Control and Information Engineering on Poznan University of Technology: block cipher PP-1 and hash function HaF are presented. Article introduction explains basic issues related to data security, cryptography, cryptanalysis and data protection in computer networks and data storage systems. The second chapter is dedicated to PP-1 block cipher. The chapter starts with some remarks on general questions related to block cipher design. PP-1 is a scalable cipher, with block sizes of 64, 128, 192, 256 bits (etc; block size may be increased by subsequent 64 bits). The length of cryptographic key may be equal to a given block size or may be two times greater than the given block size. HaF is a family of parameterized hash functions. The family consists of three functions: HaF-256, HaF-512 and HaF-1024 with message digests equal to 256, 512 and 1024 bits, respectively. The functions were designed according to Merkle-Damgård model and HAIFA construction. Significant features of the functions are large S-boxes, each of dimension 16×16. In PP-1 as well as in HaF we have focused on security. The objective leads to algorithms with relatively long processing times. It is particularly observable in the case of HaF algorithms – the results of HaF efficiency tests are provided. An important problem of cryptographic algorithms is related to data processing errors. Single error during data processing may lead to multiple errors in the ultimate result. In the chapter 4 of the paper, some error detection methods for block cipher and hash function have been proposed. Block cipher and hash function may be used in the authenticated encryption process. Usage of PP-1 and HaF algorithms for the process is referred to at the end of the article.

1. Ochrona danych

1.1. Poufność, integralność i dostępność danych

Bezpieczeństwo danych (dane rozumiemy jako wiadomości przetwarzane przez komputer, zapisane w pewnym alfabecie) polega na ich ochronie, czyli zabezpieczeniu przed nieuprawnionym lub nieprawidłowym, przypadkowym bądź umyślnym ujawnieniem, zmianą lub zniszczeniem. Wyróżniamy trzy podstawowe aspekty bezpieczeństwa danych: poufność, integralność i dostępność (Stokłosa i in. 2001).

Poufność oznacza niedostępność treści zawartej w danych dla wszystkich podmiotów nieuprawnionych do jej odczytania. Bezpośrednim sposobem zapewnienia poufności jest szyfrowanie danych. Procedury uwierzytelniania, ograniczania uprawnień dostępu czy ograniczanie fizycznego dostępu do systemu komputerowego są środkami pośrednimi prowadzącymi do osiągnięcia tego celu. Pomimo tego, że stosuje się różnego rodzaju środki zapewniające poufność, istnieje niebezpieczeństwo przypadkowego lub celowego jej naruszenia. W związku z tym system ochrony powinien nie tylko zapewniać poufność, lecz także gwarantować możliwość wykrycia prób i przypadków naruszenia danych.

Integralność danych oznacza, że dane nie zostaną w żaden nieuprawniony sposób zmienione, a tym samym ich stan pozostanie zgodny z wymaganym i oczekiwanym stanem właściwym. Integralność danych może być naruszona przez nieuprawnionego użytkownika, błędy i zaniedbania popełniane przez użytkownika upoważnionego, a także zakłócenia w transmisji danych, błędy w oprogramowaniu, działania wirusów czy w wyniku awarii. Nieupoważniona modyfikacja nie musi wiązać się z naruszeniem poufności danych. Podobnie jak poufność, integralność musi być zapewniona podczas przetwarzania, przechowywania i przesyłania informacji. Integralność danych weryfikuje się, stosując głównie algorytmy kryptograficzne zwane funkcjami skrótu. W sposób pośredni można przyczynić się do osiągnięcia tego celu poprzez stosowanie protokołów uwierzytelniania, ograniczanie uprawnień dostępu, ograniczanie fizycznego dostępu do systemu komputerowego, stosowanie metod zwiększających niezawodność sprzętu i tolerancję na błędy.

Dostępność oznacza niczym nieograniczoną możliwość korzystania z danych przez uprawnionego do tego użytkownika. Dostępność danych może być naruszona przez nieupoważnionego użytkownika, błędy popełniane przez użytkownika upoważnionego, a także w wyniku awarii, zakłóceń w transmisji, błędy oprogramowania, przeciążenia systemu. Wstrzymanie przez nieupoważnionego użytkownika dostępu do zasobów może stanowić wstęp do ataku na poufność i integralność danych. Zatem pożądane może być zapewnienie możliwości wykrycia każdego przypadku nieuzasadnionej odmowy dostępu do danych. Dostępność zapewnia się przez stosowanie odpowiednio zabezpieczonych systemów operacyjnych, stały nadzór nad stopniem wykorzystania zasobów, stosowanie systemów sterowania ruchem sieciowym i obciążeniem

Książka stanowi kompendium wiedzy z zakresu budowy bezpiecznych systemów przechowywania, przetwarzania i transmisji danych, jak również ich wykorzystania w świetle obowiązujących przepisów prawa i orzecznictwa sądów powszechnych, w tym Sądu Najwyższego.

W publikacji zaprezentowano szczegółowe rozważania dotyczące m.in. następujących zagadnień:
- systemów bezpieczeństwa publicznego,
- bezpieczeństwa przechowywania i przesyłu danych,
- ochrony infrastruktur krytycznych,
- systemów teleinformatycznych wykorzystywanych w administracji publicznej, kryminalistyce i sądownictwie.

Autorzy przedstawiają tematykę bezpieczeństwa zarówno w aspekcie technicznym, jak i prawnym, ekonomicznym oraz etyczno-społecznym. Głównym zamierzeniem było zaprezentowanie możliwości, jakie niesie ze sobą rozwój nowoczesnych rozwiązań teleinformatycznych, ale także zagrożeń dotyczących naruszeń prywatności, które trzeba wziąć pod uwagę przy wdrażaniu tych rozwiązań.

Książka jest przeznaczona dla przedstawicieli organów bezpieczeństwa publicznego, organów prawa, infrastruktury teleinformatycznej oraz pracowników naukowych dziedzin zajmujących się m.in. systemami bezpieczeństwa publicznego, bezpieczeństwem przesyłu i przechowywania danych, systemami teleinformatycznymi.

„*Nowoczesne systemy łączności i transmisji danych na rzecz bezpieczeństwa* to obszerne opracowanie i kompendium wiedzy o unikatowym zakresie tematycznym. Łączy w sobie najistotniejsze kwestie techniczne z analizą zagadnień prawnych, ekonomicznych i społecznych, dotyczących opracowywania oraz wdrażania zaawansowanych rozwiązań teleinformatycznych w służbie ogólnie pojętego bezpieczeństwa. Autorzy prezentują punkt widzenia różnych środowisk i instytucji, dając tym samym możliwość spojrzenia na pewne problemy, a szczególnie te kontrowersyjne, z różnych perspektyw".

Prof. dr hab. inż. Andrzej Dąbrowski

ISBN 978-83-264-4255-1

Cena 239 zł
(w tym 5% VAT)

Zamówienia:
infolinia 801 04 45 45, fax 22 535 80 01
zamowienia.ksiazki@wolterskluwer.pl
www.wolterskluwer.pl
księgarnia internetowa www.profinfo.pl