FIRST-PERSON NARRATIVE SUMMARY OF THE THESIS

1. Name and last name: **Maciej Kiedrowicz**

2. Degrees awarded:

   dr inż. (PhD, Eng) – technical sciences, information technology, database systems

   Military University of Technology in Warsaw, July 8, 1999

   Subject: **Method for supporting the design of distributed databases in IT systems operated in conditions of deliberate destruction of computer network elements.**

   Thesis supervisor: **dr hab. inż. (PhD, Eng) Tadeusz Nowicki**
   Reviewer: **prof. dr hab. inż. (Assoc. Prof., PhD, Eng) Juliusz L. Kulikowski**
   dr hab. inż. (PhD, Eng) Bolesław Szafrański

   mgr inż. (MSc) – cybernetics, IT systems, July 3, 1987

3. History of employment in research facilities:

   Military University of Technology in Warsaw, Faculty of Cybernetics – assistant professor (2000-now)

   (functions: Director of Department of Software Engineering, Deputy Director of the Institute of Computer and Information Systems, currently: **Deputy Dean of the Faculty of Cybernetics responsible for development and cooperation)**

   Maria Skłodowska-Curie Warsaw University – assistant professor (2012-2017)

   Łazarski University – assistant professor (2004)

   Military University of Technology in Warsaw, Faculty of Cybernetics – assistant (1994-2000)

   Military Institute of Information Technologies, Branch No. 2 – programmer (1991), senior designer (1991-1993), senior chess composer (1993-1994)

4. Achievements:

   a) Name of academic achievement:

   Information technologies for secure processing
   of information resources of public administration

b) Publication (contents of all publications included in appendices).

1. [A_6] **M. Kiedrowicz**, J. Stanik, 2018, *Multicriteria optimization used for the information security - ideal and anty-ideal,* w: Conference Proceedings of Geographic Information Systems Conference And Exhibition - "GIS ODYSSEY 2018", 2018, Perugia, Italy, Sep 10-14, 2018, Publisher: Croatian Information Technology Society - GIS Forum, Croatia, pp. 237-251, ISSN: 2623-5714 (Online), 2459-7619 (Print).
2. [A_9] **M. Kiedrowicz**, 2018, *Application possibilities of Advanced Analysis of Public Data Sources in the Fight Against Child Maltreatment,* w: Conference Proceedings of Geographic Information Systems Conference And Exhibition - "GIS ODYSSEY 2018", 2018, Perugia, Italy, Sep 10-14, 2018, Publisher: Croatian Information Technology Society - GIS Forum, Croatia, pp. 204-211, ISSN: 2623-5714 (Online), 2459-7619 (Print).
3. [A_14] **M. Kiedrowicz**, A. Ameljańczyk, 2018, *Multicriteria Methods for Identifying Patterns in the Analysis of the Flow of "Dangerous Financial Documents",* w: 22nd International Conference on Circuits, Systems, Communications and Computers (CSCC 2018), MATEC Web of Conferences, vol. 210, ISSN: 2261-236X, DOI: 10.1051/matecconf/ 201821004010.
4. [A_29] **M. Kiedrowicz**, 2018, *Metodyka zarządzania ryzykiem w bezpieczeństwie zasobów informacyjnych,* w: Roczniki Kolegium Analiz Ekonomicznych, SGH, Warszawa, nr 49, str. 287-305, ISSN: 1232-4671.
5. [A_40] **M. Kiedrowicz**, 2017, *Multi-faceted methodology of the risk analysis and management referring to the IT system supporting the processing of documents at different levels of sensitivity,* w: 21st International Conference on Circuits, Systems, Communications and Computers (CSCC 2017), MATEC Web of Conferences, vol. 125, ISSN: 2261-236X, DOI: 10.1051/matecconf/ 201712502010
6. [A_42] **M. Kiedrowicz**, J. Stanik, 2017, *Models and method for the risk assessment of an intellectual resource,* w: WSEAS Transactions on Communications, ISSN: 2224-2864, Volume 16, Art. #18, pp. 149-158.
7. [A_44] **M. Kiedrowicz**, 2017, *Generalized data model in distributed registers,* w: Geographic Information Systems Conference and Exhibition "GIS ODYSSEY 2017", 4th to 8th of September 2017, Trento – Vattaro, Italy, Conference proceedings, pp. 171-183.
8. [A_45] **M. Kiedrowicz**, 2017, *Interoperability and globalization of information models,* w: Geographic Information Systems Conference and Exhibition "GIS ODYSSEY 2017", 4th to 8th of September 2017, Trento – Vattaro, Italy, Conference proceedings, pp. 161-170.
9. [A_66] **M. Kiedrowicz**, 2016, *Use of biometric data in identification documents,* w: Zeszyty Naukowe, Maria Skłodowska-Curie Warsaw University, Warsaw, vol. 4(54), pp. 89-102, ISSN: 1897-2500.
10. [A_67] **M. Kiedrowicz**, 2016, *Location with the use of the RFID and GPS technologies - opportunities and threats,* w: Proceedings of Geographic Information Systems Conference And Exhibition - GIS ODYSSEY 2016, 2016, Perugia, Italy, sep 05-09, Publisher: Croatian Information SOC-GIS Forum, Croatia, pp. 122-128, ISBN: 978-953-6129-55-3.
11. [A_68] **M. Kiedrowicz**, 2016, *Objects identification in the information models used by information systems,* w: Proceedings of Geographic Information Systems Conference And Exhibition - GIS ODYSSEY 2016, Perugia, Italy, sep 05-09, Publisher: Croatian Information SOC-GIS Forum, Croatia, pp. 129-136, ISBN: 978-953-6129-55-3.
12. [A_88] **M. Kiedrowicz**, 2015, *Rejestry i zasoby informacyjne wykorzystywane przez organy odpowiedzialne za wykrywanie i przeciwdziałanie przestępczości,* w: Jawność i jej ograniczenia, G. Szpor (red.), Monografie Prawnicze, tom IX, Zadania i kompetencje, B. Szmulik (red.), C.H. Beck, Warszawa, str. 170-264, ISBN: 978-83-255-7664-6.

13. [A_96] **M. Kiedrowicz**, 2014, *The importance of an integration platform within the organisation,* w: Zeszyty Naukowe, Maria Skłodowska-Curie Warsaw University, Warsaw, vol. 4(46), pp.83-94, ISSN: 1897-2500.
14. [A_98] **M. Kiedrowicz**, 2014, *Uogólniony model danych w rozproszonych rejestrach ewidencyjnych,* w: Roczniki Kolegium Analiz Ekonomicznych, SGH, Warszawa, nr 33, str. 209-234, ISSN: 1232-4671.
15. [A_105] **M. Kiedrowicz**, 2011, *Wspomaganie zarządzania - zasoby publiczne w wybranych krajach unijnych,* w: Nowoczesne Systemy Zarządzania, vol. 6, WAT, Warszawa, ISSN: 1896-9380.
16. [A_106] **M. Kiedrowicz**, 2010, *Wspomaganie zarządzania w administracji - podejście procesowe a realizacja usług publicznych,* w: Nowoczesne Systemy Zarządzania, vol. 5, WAT, Warszawa, str. 321-340, ISSN: 1896-9380.
17. [A_114] **M. Kiedrowicz**, 2002, *Mathematical and Simulation Model of Fault Tolerance Distributed Database Systems,* w: ICDM '02 The 2002 IEEE International Conference on Data Mining, International Workshop on Active Mining (AM-2002), pp. 75-79, December 9, Maebashi City, Japan.
18. [P_1] **M. Kiedrowicz**, 2018, *Raport końcowy – sprawozdanie merytoryczne z wykonanych badań naukowych i prac rozwojowych w ramach projektu „Zaawansowane technologie informatyczne wspierające procesy analizy danych (gł. finansowych) w obszarze przestępczości finansowej*" (Projekt IAFEC).
19. [P_2] **M. Kiedrowicz**, 2017, *Raport końcowy – sprawozdanie merytoryczne z wykonanych badań naukowych i prac rozwojowych w ramach projektu „Elektroniczny system zarządzania cyklem życia dokumentów o różnych poziomach wrażliwości*" (Projekt RFID).

c) Discussion of the academic objective of the above-mentioned studies and achievements, including discussion of their potential use. – pages 4 – 29

5. Discussion of other scientific and research achievements. – pages 29 – 30

Introduction

Academic achievement entitled "**Information technologies for secure processing of information resources of public administration**" covers technological achievements described in [P_1] and [P_2]:

1. IAFEC Project[1] (economic and financial crimes, money laundering).
2. RFID Project[2] (processing of sensitive documents, safe access).

A series of publications (mentioned in point 4(b)) divided by topics into three sections:

I. General and thematic data models with respect to public administration repositories and registers; information resources of public administration.
II. Selected aspects of security in the processing of information resources of public administration; process-oriented approach based on risk analysis.
III. Application of proposed models for combating economic and financial crimes; legislative conditions.

For the sake of clarity of the presented publications, the areas of research and applied technologies are shown in table 1.

NOTE: Publications included in academic achievements are marked as **[A_xxx]**, publications that supplement academic achievements are marked as **[B_xxx]**, and other publications are marked as **[C_xxx]**. The publications concerning projects are marked as **[P_xxx]**. The numbering is according to the sequence of publication releases (the higher the number, the older the publication).

	1	**2**	**3**
research / technology	Data resources Repositories, registers Models	Security Processes Risk	Combating crime Legislation
1. IAFEC Project	A: 44, 45, 98 B: 61, 89, 108, 109	A: 6, 29, 40, 106 B: 1, 5, 7, 11, 12, 15, 16, 41, 94, 111	A: 9, 14, 66, 88 B: 3, 8, 10, 17, 38, 39, 60, 110
2. RFID Project	B: 108, 109	A: 106 B: 19, 41, 81, 111	A: 9, 67, 68 B: 10
Other	A: 105, 114 B: 112, 113, 115	A: 42, 96 B: 28, 35, 93, 107	

Table 1. Assignment of publications included in academic work (A) and supplementary publications (B) to research areas in the context of technologies.

The material presented for assessment covers all aspects related to the processing of data resources, which are significant in terms of adapting administration to the changing environment. Another important issue, which was described in the publications, is the necessity to consider the

[1] Project entitled "Advanced information technologies supporting (mainly financial) data analysis processes in the field of financial crime" – hereinafter referred to as the "IAFEC Project" or "IAFEC".
[2] Project entitled "Electronic system for management of lifecycle of documents at varying sensitivity levels" – hereinafter referred to as the "RFID Project" or "Project of RFID office".

correlations between various fields of administrative operations, in particular those related to legal environment. The environment of the data resource management system is particularly complex and variable. On one hand, we are dealing with the ever changing ICT technologies and variable legal environment (both national and EU), on the other – with relatively regular habits of IT system users, who are trying to stay up to date. An important issue, which is often neglected, is the necessity to develop the already existing ICT systems or design new systems to support all stakeholders of the changing environment in terms of new areas subject to "computerization". The time of execution of particular stages of the software lifecycle often makes them outdated already during their implementation. In so far as the issues resulting from the same process of producing the software were resolved (use of standards, modular structure, application of agile design methodologies, etc.), the issues related to the implementation of constant changes in the environment are still to be solved. The above refers, among other things, to **the necessity of adapting the information systems to the changing legal environment**, in particular due to changing definitions and scope of data resources, which are used in such systems. It was also very important to **maintain security** of access to the growing volume of data. On one hand, the security is understood as protection against unauthorized access to sensitive data, but on the other – as full accountability for making certain data available.

The concept of information resources (data resources) of public administration is broad and includes all data resources, which are used by public administration (government and self-government). The resources are processed in a traditional manner using ICT technologies. The method of their collection, processing and making them available is subject to separate provisions of law. Constant development of ICT technologies makes it also necessary to continuously adapt the whole administrative apparatus used to manage such resources. The necessity to consider habits of potential users of such systems, who, in many cases would like to maintain the traditional (often "paper") methods of access thereto, also raises a number of problems.

The original **proposition to create the general data model** based on the broadest possible (covering the largest data volume and the scope thereof) data resource allows to properly apply the information technologies for the purpose of managing such resource. The proposed approach also includes characteristics of appropriate activities, which were performed prior to the development of the aforesaid model as well as characteristics of the method of application of the existing ICT solutions. It was also crucial to show a possibility of later application of the proposed model. In particular, the above refers to practical application for the purpose of advanced data analysis in the selected areas of life. One of the main advantages of such approach is to become **more independent of the changes in the environment** that are gaining momentum. In other words, the aforesaid approach allows to create (modify) IT systems so that they meet the requirements of the actual and potential stakeholders of such systems.

It was proven that the **proposed methods for designing data models allow their practical application** while designing IT systems and their more complete use – in accordance with the requirements of users and strict provisions of law, **with special emphasis on data security** and hence **information security**.

The analysis of available literature (traditional publications – in paper and electronic form) shows that there is no publication that would describe the issues being the subject of interest of the thesis author in such a comprehensive manner. The bibliographies included in particular publications of the academic achievement usually include publications devoted to single terms or concepts which were described in the literature. It should be also noticed that both the subject and number of appearances at international conferences confirm great interest in the discussed topics.

Furthermore, there are no publications covering the results of research (either in Polish or in English) into the aforementioned areas. It may be due to the fact that the described research usually includes the resources from various repositories and records. What is more, in many cases, the aforesaid

resources concern sensitive data (e.g. personal data) or data that are confidential (e.g. trade secret, financial secret or bank secret). The presented method, which covers a comprehensive approach to many areas of research, allows to assume that the results of such research significantly contribute to the development of the entire discipline and may constitute grounds for further application of ICT technology in the fields, in which such technology has not been applied before.

The results of R&D studies conducted by the thesis author largely supplement the publications in the area of this summary. The above mainly refers to two projects led by the thesis author, which were the results of the contests announced by the National Center for Research and Development. The first project entitled: "Advanced information technologies supporting (mainly financial) data analysis processes in the field of financial crime", described in [P_1]. The second project "Electronic system for management of lifecycle of documents at varying sensitivity levels" was characterized in [P_2]. Both projects were implemented in the area of "Public security and defense".

I. General and thematic data models with respect to public administration repositories and registers; information resources of public administration.

The characteristics of the existing repositories, registers and records are presented in studies [A_44, A_45, A_98, A_105, A_114]. Publications [B_61, B_89, B_108, B_109, B_110, B_112, B_113, B_115] constitute their extension and provide more details with respect to the selected issues related to thematic models and the scope of the processed data. Starting with general deliberations on the functioning of centralized and distributed databases [A_114, B_115, B_110, B_108, B_109], through issues of diversity of the database systems (heterogeneous and homogeneous systems) and operating IT systems [A_45, B_61, B_110] as well as areas in which they are applied [A_44, A_98, B_112, B_113], and ending with a comparative analysis of information resources in Poland and EU Member States [A_105, B_110].

The achievements presented in [A_44, A_45, A_98] include a proposition to generalize the contents of data resources used in IT systems. The deliberations were mainly based on the analysis of the already existing solutions, but also on the applications that may (or should) emerge in the nearest future. It is not only due to the natural development of IT technologies, but also the already existing and planned legal regulations [A_98, B_112, B_113]. It is important, since some of the future legislative modifications have already been forced by the implemented (or announced) changes at the European Union level.

A great advantage of such generalization of data models is the fact that the conducted analyses of data contents refer not only to their formal structures (as resulting from the applied information technologies), but also to data semantics. Additionally, such approach allows to assume that the presented solutions are so universal that they could be applied not only nationally, but also in the European Union. The presented propositions of contents of the information models include the data on both natural and legal persons. Due to the ambiguity of many terms in this area and discrepancies in their interpretation, it was necessary to make certain assumptions that would make it possible to include them in one model [A_98]. The analysis was conducted on the basis of national and EU solutions.

The developed technologies (presented in [P_1] and [P_2]) included the necessity to solve a series of research problems, which were later verified during the preparation of the publication.

The characteristics of registers and records of public data resources presented in [A_44, A_45, A_98, A_105, A_114] included databases used by public administration. The research referred to registers and records, whose creation was necessary under legislative regulations in Poland, but the

research also included data resources from EU Member States. The aforementioned approach resulted, among other things, from the necessity to include solutions implemented in other countries due to cooperation between EU Member States. The collection, processing and accessing of data from the analyzed registers resulted from legal regulations (both at national and European Union level).

Study [A_98] offers a broader outlook on data resources processed in IT systems, whose scope and processing are closely related to the necessity of satisfying formal and legal requirements. The analysis covers all types of data, which are connected with the information about natural and legal persons as well as unincorporated entities. The analysis also includes attempts to create the general model of homogeneous environment, which would allow to use traditional ICT methods and tools, while considering the existing and currently created legal standards in that respect. The presented analysis also includes potential effects that may occur as a result of changes in the manner and mode of data processing due to changes in legal regulations.

In the first part of study [A_44], a comparison was made between the registers and records kept in the selected EU Member States (9 Member States). The comparison concerns basic data registers connected with natural persons, person running business activity, properties and basic records of vehicles (cars, aircrafts and vessels). In case of some of the discussed countries, the information on certain registers and records was omitted due to the lack of access to such information or ambiguity of such information. The presented characteristics of the selected data resources of the chosen EU Member States apparently do not exhaust the topic. It may be noticed that the scope of data, method of their processing, method of access vary depending on the level of development and legal conditions specific for a given country. Poland does not differ from other EU Member States in that respect. The second part of [A_44] includes a proposition of some elements of the general data model, which is connected with the scope of data processed in the aforementioned registers and records and which covers all of the discussed countries.

The first part of study [A_45] includes basic records and registers with the most important information on natural and legal persons. All these resources are collected, processed, made available and archived in compliance with the binding Polish regulations (usually, regulations equivalent and complementary to the acts of parliament - statutory regulations and internal regulations of appropriate government departments). Due to a large number of various registers, lists, records and breakdowns, only those which include the most important information on natural and legal persons as well as those with the most complete information (in the context of both data collected about particular entities and the number of such entities about which the data are processed) are subject to further analysis. The second part of study [A_45] covers the characteristics of the generalized model, which assumes existence of one system allowing the analysis of all data processed in the homogeneous environment. While an attempt to carry out various types of analyses in the existing heterogeneous environments may be compared to the "big data" processing, the construction of one model for all the processed resources shall result in a possibility of using "traditional" data analysis methods. In particular, the above refers to such resources that are processed in "their" environments, while using the already existing traditional information methods and tools. The analysis of legal bases related to the processing of collected data is another important aspect examined in this part. While considering the imposed - often very strict - restrictions, which are contained in the regulations on specific areas of application (sometimes strictly defined), an analysis of effects that may occur in case of amendments to such regulations was performed. On one hand, the above is aimed at further specification of such restrictions, but on the other - at their generalization. Therefore, it should be noted that some of the characterized resources might be processed (in whole or in parts) in a traditional manner, i.e. without using the ICT tools.

It is also important to state what advantages may arise from the application of the above-mentioned approach. Study [A_105] includes a proposition to use the analyzed resources for the purpose of supporting management processes in any organization. The process of preparing an organization for

the implementation of any IT system or integration of the already implemented systems shall begin with answering the following questions: (i) Does the organization know what kind of information is or shall be necessary in the future? (ii) Is the organization ready to use the integrated information? and (iii) Do formal restrictions (national legislation, EU legislation, bylaws of the organization, etc.) provide for a possibility of obtaining and using the information, including the information derived from integrated sources? Study [A_105] includes an attempt to introduce some of the issues tackled in the above questions, with special emphasis placed on a possibility of obtaining data from public resources. Due to complexity of the integration process and broad scope of data that may be potentially used, the presented deliberations were limited to certain types of organizations and specific information resources. It should be also mentioned that a possibility of access to certain information resources changes over time. It mainly results from technological developments and the fact that the broader scope of data is of interest to many people and organizations. Rapid growth of integration platforms and changed interest in obtaining data by various types of organizations make it necessary for analysts and designers to adopt a comprehensive approach to the proposed solutions. The above refers to both integration of the already existing data sources and a possibility of obtaining new data (either through the integration of various resources or design of new systems including the ever-widening data resources). The study also characterizes basic resources (registers, records, databases), which have been made public and whose integration will possible in near future, not only at a national level, but also at European Union level. The studies concerning integration of the aforesaid resources were conducted also at European Union level (e.g. STARK project - the project related to electronic identity of all inhabitants of EU Member States). The presented characteristics of data resources referred to the selected EU Member States: the Czech Republic, France, Spain, the Netherlands, Lithuania, Germany, Hungary, Great Britain and Italy

The analysis of information resources collected by various institutions and organizations allows perceiving them as a huge database (often referred to as the data resources in the research literature). The resources are collected in different forms, both electronic and traditional - paper. In combination with the modern technology, which may be applied in this analysis, the data resources provide a possibility of gaining extensive knowledge of any entity (refers to both natural and legal persons). Due to different technologies used for the purpose of processing such resources, it is impossible to apply universal information tools that would allow to easily obtain interesting analytical data. It is especially important in case of access to the data, which are processed in whole or in parts n a traditional manner. The above applies to the resources processed in an isolated information environment to a lesser extent.

Working practical solutions using large numbers of data resources entail the necessity to design extensive (and distributed) IT systems, which use distributed data resources. Article [A_114] describes certain elements related to the design of distributed databases, with special emphasis on IT systems, which are at risk of deliberate destruction of the computer network components (e.g. military systems). The issues of distribution, allocation and replication of the distributed database were also taken into consideration. They were discussed in detail in monograph [B_115]. The book contains a description of the method of fragmentation, allocation and replication of data sets from the distributed database (DDB). The first chapter defines basic terms and methods for solving problems related to the design of the distributed databases. Additionally, the issue of DDB application in specific IT systems at risk of deliberate destruction of the computer network components as well as other issues that may be related thereto were characterized. Chapter two contains a description of the mathematical model of fragmentation, allocation and replication of data sets in DDB. Chapter three shows different ways of creating tasks related to fragmentation, allocation and replication of data sets in DDB as well as presents specific methods for solving such issues. In the subsequent chapter, the author described a simulation method for choosing fragmentation, allocation and replication of data sets in DDB resistant to destruction of nodes of the distributed network (including the characteristics of the simulation experiment for setting such strategy). The last chapter shows how to interpret the results of the developed

method in the DDB design process. Both publications, i.e. [A_114] and [B_115], indicate to a possibility of solving complex issues by using both analytical and simulation methods.

The use of data warehouse as one of the methods for supporting the management of large volumes of data has been presented by showing how to improve the knowledge management - [B_108] and [B_109]. Publication [B_108] includes a description of the method for using data warehouse in systems supporting knowledge management. The first part includes a description of the systems supporting knowledge management in Poland. The following was described in detail: public and secret knowledge, method of knowledge management and methodologies of design of knowledge management systems. Basic tools supporting the knowledge management processes have been mentioned and described. In the final part, the author outlined the use of a diverse environment with data warehouse in the knowledge management systems. The final part also includes a description of the architecture of the knowledge management system and basic functions of such system (gathering, cleaning, storing, searching and distribution of knowledge) implemented based on the data warehouse. On the other hand, publication [B_109] shows how to use certain tools to design the data warehouse (SAS Institute) in the system for supporting knowledge management. The tools are mentioned in the first part thereof and briefly characterized. The adopted criteria were used to evaluate the knowledge management system on the basis of a multi-dimensional data model of the system based on the relational data model. Furthermore, the concept of the knowledge management system using the extended relational data model was described. The model was developed using the results of such evaluation with respect to the two previous applications.

Theoretical considerations included in the above-mentioned publications were used by the author in practice. Publication [B_112] describes the implementation of PESEL2 project in broader context and the role that the project should play in terms of modernizing the operations of Polish administration and public services rendered thereby. On the other hand, in publication [B_113], the author described PESEL2 program as one of the components of the whole concept of information society, which includes in particular the offering of services to citizens and entrepreneurs as well as creating opportunities to enable public administration render services via electronic communication means. PESEL2 project, whose implementation was planned in the years 2006-2008, constituted a part of PESEL2 program. In the above-mentioned program, one of the main assumptions was to design new IT systems and integrate the existing ones, while introducing organizational and legal changes. It was an attempt to establish modern e-administration, which would be something more than just technical integration of IT systems used in public administration, based on uniform technical standards of interfaces and data. The introduced changes should mainly concern all definitions of the new information processes, directing the operations of public administration towards elimination of the existing asymmetry of laws, obligations and responsibilities between the state and citizen, including in particular elimination of information asymmetry between the state and citizen. It may be also noticed that the **concept of biometric ID card** as presented by the thesis author was implemented as late as in March 2019.

Monograph [B_110] constitutes a compendium of knowledge useful for national officers of authorities that conduct proceedings aimed at recovering the so-called proceeds of the crime by using international legal aid instruments. The fundamental goal was to discuss the manner of obtaining information collected in different sets, registers, databases, which may be mainly used to determine individual components of the aforementioned proceeds of the crime, their current legal status and location. Despite rather dynamically developing EU regulations on the subject issue, which make it necessary to adopt certain solutions in national laws of particular EU Member States, for the purpose of submitting the motion for legal, it is very useful to synthetically present the substantive and procedural assumptions in the internal legal system of a given EU Member State.

Another example of implementation of the proposed generalization of the used patterns of data resources is in chapter 4: "Interoperability of information models used by geographic information system in terms of globalization" in monograph [B_89] written by the thesis author. To harmonize the policy regarding data used in the IT systems, including geographic information systems, it is necessary to standardize both the systems and the registers related to such areas. The above issues refer not only to legal aspects related to the aforesaid data areas, but also to IT solutions used in different EU Member States. It is possible to achieve full interoperability in the future, however, the preparatory work in this field should begin immediately. The first step should be to build an appropriate information model, which shall constitute grounds for further activities. It is possible to obtain a homogeneous system for the level of data model (for example, as part of standardization of the database scheme) by developing a specialist data meta-model and using methods of data exploration (especially in the so-called thematic data warehouses) or designing and building a dedicated specialized system. In the first part, a comparison was made between the registers and records kept in the selected EU Member States. The comparison concerns basic data registers connected with natural persons, person running business activity, properties and basic records of vehicles (cars, aircrafts and vessels). In case of some of the discussed countries, the information on certain registers and records was omitted due to the lack of access to such information or ambiguity of such information. The presented characteristics of the selected data resources of the chosen EU Member States apparently do not exhaust the topic. It should be noticed that the scope of data, method of their processing, method of access vary depending on the level of development and legal conditions specific for a given country. Poland does not differ from other EU Member States in that respect. The second part includes a proposition of some elements of the general data model, which is connected with the scope of data processed in the aforementioned registers and records that covers all of the discussed countries.

The developed technology (as part of IAFEC [P_1]) was also described in studies [B_61] and [B_110], where the author indicated to a possibility of using the developed general data models in the processes related to prevention and combating of crimes. Both studies show how important it is to integrate IT systems. In particular, the above refers to the integration of information resources, which are used both in the area of uniform identifiers and semantics of the processed data.

A list of titles of basic and supplementary publications used for the discussed issue appears below. The details of a given publication may be found in the list of the published academic papers.

[A_44] *Generalized data model in distributed registers.*
[A_45] *Interoperability and globalization of information models.*
[A_98] *Uogólniony model danych w rozproszonych rejestrach ewidencyjnych.*
[A_105] *Wspomaganie zarządzania - zasoby publiczne w wybranych krajach unijnych.*
[A_114] *Mathematical and Simulation Model of Fault Tolerance Distributed Database Systems.*
[P_1] *Projekt IAFEC.*
[P_2] *Projekt RFID.*
[B_61] *Rejestry publiczne wykorzystywane przez organy odpowiedzialne za wykrywanie i przeciwdziałanie przestępczości.*
[B_89] *Enhancing a City via GIS: Issues and challenges. Rozdział 4. Interoperability of information models used by geographic information systems in the context of globalization.*
[B_108] *Hurtownie danych w systemach zarządzania wiedzą.*
[B_109] *Hurtownia danych w systemie zarządzania wiedzą - rozwiązanie modelowe.*
[B_110] *Odzyskiwanie mienia w wybranych krajach Unii Europejskiej - rozwiązania prawne i bazy danych. Czechy, Francja, Hiszpania, Holandia, Litwa, Niemcy, Węgry, Wielka Brytania, Włochy.*
[B_112] *PESEL2 - projekt, program realizacyjny i rola systemu.*
[B_113] *Przebudowa i integracja rejestrów państwowych.*

[B_115] *Wybrane problemy projektowania rozproszonych baz danych*.

II. Selected aspects of security in the processing of information resources of public administration; process-oriented approach based on risk analysis.

Constant development of IT technologies and equally rapid changes in the environment of the designed IT systems make it necessary to find new solutions, which would consider such dynamics to a greater extent. One of the issues that should be (or even must be) taken into account is information protection and security as well as risk assessment in terms of maintaining such security. The propositions outlined in studies [A_6], [A_29], [A_40], [A_42], [A_96] and [A_106] allow to consider many elements related to the information security, regardless of the currently applied solutions or solutions that shall be applied in the future.

The issues of system integration based on the creation of integration platforms and support of such activities by adopting a process approach to the design of IT solutions have been described in [A_96] and [A_106] as well as in supplementary publications: [B_35], [B_41], [B_81], [B_94], [B_107] and [B_111]. The security of information resources (information security) has been described in [A_6] and [B_1], [B_3], [B_5], [B_7], [B_11], [B_12], [B_15], [B_16], whereas the issues of risk management in terms of the security of information resources in [A_29], [A_40] and [A_42] as well as in supplementary publications: [B_93], [B_19], [B_28]. The risk management models and methods described therein in many cases refer to the solutions that are known and applied in other areas (for example, the use of a multi-criteria optimization method).

Study [A_96] shows how important it is to integrate all components of the ICT infrastructure. The integration at the technical level and level of system software is generally highly advanced. The greatest challenge is the integration at the information level. Apart from aspects related to the data integration (as a result, the information integration is obtained), the integration at the organizational level and the integration at the level of formal and legal environment closely related thereto are equally important. In many organizations, frequent discussions and meetings are held because of the impression that the employees tend to work more and more in the company, but the economic results tend to be worse and worse (or at least – not better). Companies are looking for extraordinary specialists and execute investments carefully, while considering market changes and those related to customer behavior. Generally, members of the management board behave in line with the management principles and businesses are not developing the way they should. However, not everybody has the same problems - other companies operating on the same or similar markets develop or grow much faster. What is or might be the reason for such situation? Perhaps such companies are more sure-footed thanks to the solid fulcrum of actions, integrated business processes and flexible IT systems using the integration platform. Perhaps such companies implement the technologies that enable them to execute basic operations related to business activity in a more reliable and efficient manner. Perhaps such companies decide which operations need to be developed and which require special treatment, for example, by introducing or upgrading IT systems responsible for or supporting the subject operations. In such companies, the IT technologies, including the integration platform, become assets and constitute one of the main elements of the company's foundations, ensuring efficiency and flexibility of its operations.

Another aspect that needs to be taken into consideration is a possibility or - in some cases - the necessity to adopt the process approach to the design and creation of IT systems supporting the delivery of services (including public services). The approach is described in article [A_106]. The systems supporting the delivery of services (in particular, public services) require constant development and

adaptation to the ever-changing conditions (mainly legal), whereas the application of the process approach allows to significantly simplify the procedure and reduce the time necessary to introduce all the essential changes. A model catalog of services, which may be executed by such systems, was also described in the article. The article includes an example of the actually implemented solution, which is used on the basis of the aforesaid approach. The issues related to the application of the process approach in the integrated environments were supplemented with elements that are necessary to maintain a specific level of security of resources. The characteristics of such approach may be found, among other things, in studies [A_42], [A_29], [A_6] and [A_40].

The subject of article [A_42] was the security of intellectual resources and the necessity to provide going concern. The article was aimed at showing the impact of various categories of risk factors related to intellectual resources, i.e. the components of intellectual capital, on their security and going concern. Following an analysis of the literature on this subject and the authors' own observations, an attempt was made to define three types of risk models related to intellectual assets. A substantial part of the study was devoted to the methodology of risk assessment of the intellectual resource. The presented approach considers various categories of risk factors, resulting from both the architecture of the intellectual resource as well as other elements used in the processes and areas of intellectual capital management. The models outlined in that article could be the starting point for developing the methodology of risk assessment of the intellectual assets and appropriate policies of the organization, e.g. its information security, risks or quality, which may in turn constitute input values for developing the risk management system related to the intellectual capital of such organization.

In study [A_29], the author outlined the risk management methodology, including the adopted risk model of information resource, analysis method and risk assessment as well as sample risk areas and factors referring to the risks occurring at particular stages of the information resource lifecycle and linked them in such a manner so that it was possible to completely and explicitly determine the level of risk, while maintaining practical utility of the proposed approach. Recently, the concept of risk assessment has become more popular in almost all areas of life, starting from business through medicine and ending with information security. The subject of article [A_29] is the risk management methodology in terms of ensuring security of the information resources, which are processed using information technologies, in particular IT technologies. The purpose of the article was to present the original information resource risk management methodology, including different methods, models and techniques related to risk engineering, which are significant from the point of view of ensuring completeness of the risk management process in term of security and setting the level of risk of the information resources. At the stage of developing the methodology, the following research methods and tools were used: studies of professional literature, critical analysis of documents and various information resources of the analyzed organizational units and discussions with owners of the information resources, administrators of databases or IT systems. The article describes the risk management methodology, which includes the original model of the information resource risk as well as the original method of risk analysis and assessment, which are interlinked so to allow efficient risk management. An element of objectivization of the methodology proposed in the study is to depart from copying the traditional risk management process and to introduce additional elements at the stage of risk analysis, estimation and evaluation. In the first part of the article, the author reviewed currently available risk management methodologies derived from both the literature and ISO standards. The subsequent part contains a description of the information resource risk management methodologies. The basic components of the presented methodology are principles, framework structure and review of the information resource risk management process. The last chapter provides details and clarification of the concept of the information resource risk management.

Article [A_6] outlines the concept of assessing the utility of the security configuration, using two reference points (ideal and anti-ideal). The concept is in line with the natural intention of getting

closer to the ideal point. In case of several such solutions, it is possible to come up with the one that would allow the greatest possible detachment from the situation considered the most undesirable. In the context of methodology, the article was presented in two layers. The first layer includes the security configuration model, including values describing the utility properties and partial criteria for measuring utility. The second layer refers to the issue of multi-criteria optimization of the security configuration and proposed method of its resolution. The efficiency of the information processing process in the organization to a large extent depends on the present qualitative properties, e.g. functionality, reliability, utility, security of the security system. Therefore, it is crucial to appropriately control the current properties of the security system by generating the most desired security configurations from among the set of permissible solutions after the occurrence of an emergency situation. The most desired security configuration is the one that not only ensures maintenance of the required level of security, but also has the best utility properties. The issue was analyzed as the task of multi-criteria optimization of the security configuration. The issue constitutes the main theme of the article and determines its framework. The article includes the following elements: (i) development of the models of the Security System and Security Configuration allowing to consider the interdependence between the current level of security and random changes of risk factors having material impact on the safety of the information processing processes; (ii) proposal of the values describing the utility properties of the security configuration and partial criteria for measuring their usability, and (iii) formulation of the issue of multi-criteria optimization of the security configuration and proposed method of its resolution.

Additionally, article [A_40], which outlines the methodology of the IT system risk analysis and management, including various categories of risk factors significant from the point of view of the sensitive data processing and completeness of the procedure for determining the level of IT system risk, constitutes a continuation of the above-mentioned issues. The presented methodology was divided into the analysis of IT system risk and the method of risk management. The level of IT system risk assessed by the risk analysis method constitutes an input value for the IT risk management method outlined in the further part of the article, referring to the risk of IT systems used for the processing of documents at different levels of sensitivity.

When analyzing various approaches to assessment of the risk level and proper risk treatment, a question arises whether a possibility of creating a complete and consistent methodology for analyzing the processing of documents at different sensitivity levels, including various categories of risk factors allowing their combination so that it is possible to determine the risk level of sensitive documents, while maintaining practical usability of the proposed solution, does actually exist. Article [A_40] is an attempt to answer the above question by outlining the methodology of the risk assessment and management, referring to the IT system responsible for the processing of the documents at different levels of sensitivity, which is - according to the authors - complete and consistent. Furthermore, the presented methodology provides grounds for qualitative risk assessment and more detailed analysis; provides grounds for developing a more specific methodology of risk assessment in terms of the information security; allows risk evaluation at different levels of certainty; the risk of processes used for the processing of documents at different levels of sensitivity; is useful from the perspectives of both the risk resulting “from” (a specific threat) and risk “for” (a given protected value), e.g. risk of fire spread in a given infrastructure, regardless of the risk source; allows to apply the scenario approach; allows to classify the risks according to reliable levels of their impact; allows to identify the occurring risks being under control and those which require additional control or enhancement of the existing control; produces results comparable to those which are come from the requirements on risk mitigation. The described risk management process is an organized method of risk identification, analysis and evaluation within the framework of the entire risk assessment process, which allows to undertake repeatable, reasonable and efficient actions as part of the adopted risk management strategy. Details and

clarification of the above-mentioned issues are in studies [B_35], [B_41], [B_81], [B_94], [B_107], [B_111] – with respect to methods for modeling the processes implemented in organizations, and in [B_1], [B_5], [B_7], [B_11], [B_12], [B_15], [B_16], [B_19], [B_28], [B_93] – with respect to areas related to information security.

The article [B_14] presents the concept of business process modeling by using dynamic processes. An extended definition of the business process allows to construct a mechanism for dynamic selection of actions performed in order, which makes it possible to achieve the process goal assumed in the definition. The mechanism for selecting actions subsequently taken in the dynamic process constitutes extension of the functionalities in the workflow process, including the process progress and service environments status. The process approach applied during the modeling, design, implementation and use of IT systems makes it necessary for the authors to model and design such business processes that shall constitute fundamental and necessary structure elements of the system based on the process approach. It is possible to model basically all of the processes used in the company's operations, however, such a comprehensive approach would cause a significant increase of complexity and hence the costs related to the implementation of such system. If the system based on the process approach is implemented in the incremental form, it means that the processes or groups of processes, which should be modeled or implemented in the first row, need to be distinguished. If the organization already uses the process automation systems, the analysis of definitions and instances of such processes may contribute to the decisions made with respect to their efficiency and quality, using methods and tools for process analyses. The main selection criteria include the processes: that are most often implemented within the organization (quantitative factor), that have significant impact on efficiency and operating costs of the company (economic factor) and that have significant impact on the implementation of the company's main targets (strategic factor). On the other hand, the processes rarely implemented or characterized by high variability of their structure require a lot of effort on the part of creators of the business processes, which consequently results in the fact that such processes often have very complex structures. In such processes, the correlation between the cost of their implementation and potential profit during their automated processing may be largely unsatisfactory. It is possible to model and design such processes that would not require from their creators any high structural precision at the beginning. The aforesaid processes include adaptation, generic and dynamic processes.

In article [B_111], the author developed the concepts described in [A_96] and [A_106]. The application of the process approach was characterized in the context of public services, including an example of their implementation based on such approach. It may be easily imagined that a citizen or employee of a company, who wants to perform a certain action that requires contact with public administration, opens their website and executes the action without “leaving home”. It seems reasonable to expect that in the nearest future people will be offered public services by electronic means. The process approach makes it possible to comprehensively consider such issues and quickly implement the solutions related to e-administration, e-citizenship, e-services and e-society (and maybe other e-activities). However, it should be remembered that the website contents still represent only the tip of the iceberg. The remaining part, i.e. the systems, which actually render the services, are invisible to users. The whole structure is useful as much the systems are able to execute services. And it does not matter if the systems are manual or automatic.

On the other hand, the methodology described in article [B_35] constitutes a proposition of a certain approach to the analysis and management of the risk of business processes, while considering different categories of risk factors from various areas of activities of the organization. The presented methodology is divided into the risk analysis method concerning business processes and risk management method. The level of the risk of business processes assessed by the risk analysis method constitutes an input value of the risk management method and is used for developing the strategy for ongoing concern management as well as risk prevention and mitigation. A modern organization is

competitive not only in terms of prices and quality of the offered goods and services, but also, just like a traditional organization, in terms of quality and security of its business processes. Therefore, customers are set to see added value, which they expect. The value is added thanks to quick incident response and reduction of the decision-making processes. When analyzing various approaches to the assessment of the risk level, a question arises whether a possibility of creating a complete and consistent methodology for analyzing business processes, including various categories of risk factors allowing their combination so that it is possible to determine the risk level of business processes, while maintaining practical usability of the proposed solution, does actually exist.

The dynamic development of information technologies and their applications in many areas of science and life is getting more extensive and intense. It has huge impact on daily activities in both the world of business and life of an average person. Some technical and technological innovations may significantly improve the operations and security of material data, hence, the so-called sensitive documents. The technology for tagging and identification of documents, which was used to present the proposed approach, is the RFID (*Radio-Frequency Identification*) technology. The example of application of the RFID technology described in [B_81] is connected with the processing of documents at various levels of sensitivity and may have practical impact on their flow in a secret office and other organizations, where archiving and document flow processes are crucial for their operations. Such solutions are not only very complex, but also composed of many different elements – the variety results from the technologies, scope of operations and impact of the said elements (i.a.: IT, ICT, electronic, mechanical, organizational, formal and legal systems). Therefore, the purpose of the study was to verify possibilities of modeling main activities traditionally performed in a secret office (without automation), using systems that automatize processing via ICT systems (workflow systems, registers and data resources) and RFID technology as well as to verify their compliance with the BPMN notation standard, also by applying the process simulation method. Theoretical deliberations included in study [B_81] were verified in practice as part of the technology development, while implementing the RFID project, which was described in more detail in [P_2].

Article [B_94] contains deliberations on the significance of information security in the information society in terms of the selected legal aspects. Some aspects of standardization for the protection of public databases, registers and services rendered by public administration were described. For each of the aforementioned standards, e.g. acts, norms or best practices, the author established minimum requirements and activities that should be undertaken and executed buy security service to ensure basic level of security of the information processed by different institutions. Furthermore, it was stressed that data, information and knowledge play a significant role in modern information societies, legal frameworks, people-to-people contacts and daily life of a specific person.

Study [B_107] includes a referential model of corporate structure – xGEA (*cross-Government Enterprise Architecture*), which allows to identify opportunities that support innovations in the areas of focus of the strategies. In particular, the areas are the following: (i) orientation of service design using IT technologies as needed by the users (citizens and companies); (ii) application of the co-shared services approach, and (iii) development and broadening of professionalism in government agencies. The model directs the activities into re-use and co-sharing of resources. It also begins to direct the work into common techniques and methods. A common language is created, which allows to establish the co-sharing and cooperation processes in government organizations. Potential benefits include: promotion of the design of common infrastructure, improvement of risk management, identification and aggregation of needs to promoted efficient use of resources, establishment of co-shared standards to promote better cooperation between government agencies, increase of competitiveness in the delivery of IT products and services, improvement of business flexibility and reduction of ownership costs. In every country, the citizens would like to have at least one contact point allowing them to cooperate with public administration. Businesses want to provide government administration with the information only

once. Such needs must be met with constant pressure on providing good quality of the delivered information and reducing costs. The presented model may satisfy the needs on a larger scale.

In studies [B_19], [B_28] and [B_93], the author described methods of analysis and assessment of the risk of information resources. Article [B_28] contains a description of the original method of analysis and assessment of the risk of information resources/IT system, including different categories of risk factors, significant from the point of view of ensuring the completeness of the process of determination and setting of the level of the risk of information resource processed both in a traditional manner and via IT systems. The presented method is qualitative and divided into risk analysis stage and risk assessment stage. An element of objectivization of the proposed qualitative method is to depart from traditional risk maps at the stage of risk evaluation and move towards a vector, whose components reflect a broad range of factors having significant impact on the current level of the information resource risk. To develop the aforementioned method, the authors studied professional literature and conducted critical analysis of the currently available quantitative and qualitative risk analysis methods applied in the subject organizations, in particular office units processing the documents at different levels of sensitivity. The number of risk factors included in the proposed method as well as their versatility definitely allow to distinguish the proposed approach from other currently applied methods for assessing the risk of information resources/IT systems, which - according to the authors - constitutes an undeniable advantage of the said approach. The subject of article [B_19] is the risk model of the information system processing the documents at various levels of sensitivity in office units, using IT systems and RFID technologies to process the data. The model constitutes a multi-dimensional approach to the analysis of IT system risk and IT processes implemented therein. The article includes a description of the risk model and sample risk factors referring to the risks occurring at particular stages of the IT system lifecycle and linked them in such a manner so that it was possible to completely and explicitly determine the level of risk, while maintaining practical utility of the proposed approach. The article is an attempt to answer the following question: Is it possible to create a comprehensive and adequate risk assessment model for the information system, in which the resources at different levels of sensitivity are processed? The proposed model was used to develop a framework structure of the risk management system and appropriate security policy of the information system in the analyzed office unit, in which the risk was assessed by using the developed model.

To ensure the required level of security of the organization or high level of security of certain information processing areas, it is necessary to develop the protection strategy or project of security measures, in accordance with a reliable methodology, and then implement such project by experts, using appropriately selected technologies and maintaining efficient security configurations. The designed security configurations of technical or organizational nature should be to a large extent based on the results of the risk analysis, specifications of security requirements as well as general theory of security measures (i.a. it is required to assess utility of the current security configuration, verify resistance of the applied security measures to different types of attacks and re-configure the security system following the occurrence of various types of emergency situations and loss of the required level of security). In the available literature, there are no methods for assessing efficiency of the security system built on the basis of security configurations or configurations of security measures of technical or organizational nature. A method proposed in the studies by Szulim and Kuchta ()[3] is worth mentioning. It is the qualitative method. A possibility of its practical application is limited to a very narrow class of quality indicators. It may not be used to assess the usability of the current security configurations and the process of allocation of security measures to particular security configurations – reconfiguration process. The available studies show that there is a growing need to automate the reconfiguration process and

[3] M. Szulim, M. Kuchta, *Metoda analizy skuteczności systemu bezpieczeństwa obiektu*, Newsletter of the Military University of Technology, vol. LIX, no. 4, 2016.

develop appropriate procedures for controlling the risk in business processes. The lack of methods and criteria for assessing efficiency of the security measures (technical and organizational) hinders quantitative efficiency assessment of the security systems. Therefore, it is necessary to conduct qualitative assessment. The qualitative assessment is subjective and its results, i.e. acceptance of the protection level of the resources or their rejection, depend on the knowledge and experience of the assessor. Efficient protection of the information processing areas requires implementation of various types of configurations of security measures, including application of several or a dozen or so technical and organizational security measures simultaneously. While considering a group of such security measures and different characteristics of their correlations (relationships, properties), what emerges is the security system. The purpose of article [B_ 15] was to outline and recommend both theoretical and practical approaches to efficiency assessment of the system of security measures. When determining the security level of the information processing areas in the organization, three main issues, typical for the structure of the article, must be taken into consideration: (1) it must be possible at current moments to process the data (the required set of the information resources) in a secure manner, (2) protection processes should be created for sensitive sets, allowing to maintain appropriate security attributes at an acceptable level of risk, and (3) precise security configurations should be established, implemented and maintained for the purpose of keeping the required security attributes related to the selected group of resources of the security service, ensuring appropriate security level of such resources or acceptable risk value. In light of the above, the current security level of such resources shall be understood as a possibility of activating an appropriate set of security measures in the information system of the organization by the security service. The correlations between such security measures create a set of permissible security configurations, built on the basis of the set of currently working technical or organizational security measures, which are at the disposal of the team operating the system of security measures.

Studies [B_1], [B_5], [B_7], [B_11], [B_12], [B_16] cover issues related to the modeling of the systems of security measures [B_12] and [B_1], assessment of their efficiency [B_11], automatic configuration, control and monitoring [B_7] and [B_5], and include the security service model [B_16] used to maintain the required level of information security.

The purpose of article [B_16] was to determine the security service model and provide grounds for the method used to control the current properties (e.g. performance, functionality, reliability, security, etc.) of its components, allowing to maintain the required level of information security in the organization. The required level of information security in the organization may be achieved by making appropriate steering decisions, which activate relevant sets of protection processes improving the current security level of the protected facilities. The protection processes use appropriate protection methods and techniques (security measures) of technical and organizational nature. The correlations between active security measures create appropriate security configurations. Proper control of utility properties of such security configurations allows to maintain the required level of information security in the organization. The article [B_12]outlines the concept of maintaining the required security level of the information system in the organization through appropriate control of the security configurations of the security system. The security system model was proposed and its basic elements characterized to maintain the current security level of the information resources. The desired current security feature shall be obtained by generating appropriate security technical and organizational configurations from the set of permissible solutions. The proposed concept, which takes into account the impact of not only basic security elements of the information resources (e.g. types of resources, security attributes, risks, vulnerability), but also changes in the working conditions of the information system and security system as well as the entire security and quality management environment of the organization. On the other hand, study [B_11] addresses the issue of efficiency assessment of the security system in terms of the information security management (information resources of the information system in the organization).

It is assumed that the purpose of such security system is to achieve a declared level of protection of the information system resources. Therefore, the level of security of information system in a given organization shall be determined by the efficiency assessment of the security system. The efficiency of the security system mainly depends on the functional properties of its components and other factors occurring in its environment. The article mainly focuses on security configuration, i.e. technical configuration and security organization configuration. The thesis was adopted that the efficiency of the security system may be considered as a set-theoretic efficiency sum of the security configurations invoked in such system. Additionally, it was assumed that a prerequisite for the desired measures (indicators) of the efficiency assessment of the security system shall be to propose such measures and develop appropriate ways (methods) of their calculation. In the article [B_7] the model of automated control and monitoring system of the current level of information security was proposed. Basic system elements, such as: subject of activities, object of activities and purpose of activities were selected and characterized. Furthermore, the concept of security configuration and subsystem model for controlling the current level of information security in case of an emergency situation were defined. Theoretical considerations were illustrated with examples. Article [B_5] outlines a method of assessment of the usefulness of the security configuration from a set of available security configurations, after occurrence of an emergency situation. It is believed that the best security configuration is the one that not only ensures maintenance of the required security level of the information resources, but also provides the best values describing its utility properties. The values describing the utility properties of the security configuration and partial criteria for measuring their utility were proposed. The utility measures of the security configuration include performance, reliability and security indicators. Study [B_1] outlines a concept of maintaining the required level of security of assets of the information system in the organization by making appropriate steering decisions, initiating the generation of correct security configurations. The authors proposed and formulated the models of security subject and object as well as the model of the information system in the organization for controlling current level of information security (information resources) and current performance properties of the operation subsystems, included in the information system of the organization.

A list of titles of basic and supplementary publications used for the discussed issue appears below. The details of a given publication may be found in the list of the published academic papers.

[A_6] *Multicriteria optimization used for the information security - ideal and anty-ideal.*
[A_29] *Metodyka zarządzania ryzykiem w bezpieczeństwie zasobów informacyjnych.*
[A_40] *Multi-faceted methodology of the risk analysis and management referring to the IT system supporting the processing of documents at different levels of sensitivity.*
[A_42] *Models and method for the risk assessment of an intellectual resource.*
[A_96] *The importance of an integration platform within the organisation.*
[A_106] *Wspomaganie zarządzania w administracji - podejście procesowe a realizacja usług publicznych.*
[P_1] *Projekt IAFEC.*
[P_2] *Projekt RFID.*
[B_1] *Model of the Information System in the Organization for Controlling Current Level of Information Security.*
[B_3] *Zintegrowany system dostępu i analizy danych rejestrowych i ewidencyjnych* -w przygotowaniu
[B_5] *Assessment of the usefulness of the security configuration.*
[B_7] *Model of automated control and monitoring system of the current level of information security.*
[B_11] *Method for Assessing Efficiency of the Information Security Management System.*
[B_12] *The Security System for Maintenance of the Required Information Security Level.*
[B_15] *Ocena użyteczności systemu zabezpieczeń w systemie bezpieczeństwa informacji.*
[B_16] *Model służby bezpieczeństwa na potrzeby utrzymywania wymaganego poziomu bezpieczeństwa*

informacji w organizacji.

[B_19] *An information system risk model for the risk management system of an organisation processing sensitive data.*

[B_28] *Metoda analizy i szacowania ryzyka zasobu informacyjnego.*

[B_35] *Wieloaspektowa metodyka analizy i zarządzania ryzykiem procesów biznesowych.*

[B_41] *Dynamic business process in workflow systems.*

[B_81] *Modelowanie procesów biznesowych przetwarzania dokumentów wrażliwych z wykorzystaniem technologii RFID.*

[B_93] *Selected aspects of risk management in respect of security of the document lifecycle management system with multiple levels of sensitivity.*

[B_94] *Wybrane aspekty standaryzacji w ochronie publicznych zasobów informacyjnych i świadczonych usług w kontekście społeczeństwa informacyjnego.*

[B_107] *Opis ram xGEA.*

[B_111] *Podejście procesowe a usługi publiczne realizowane przez administrację.*

III. Application of proposed models for combating economic and financial crimes; legislative conditions.

Studies [A_9], [A_14], [A_66], [A_67], [A_68] and [A_88] describe a possibility of using the predefined general data model in the systems supporting the prevention of different crimes. In the majority of the studies, the above refers to combating financial crimes, but also fighting against child abuse. The main achievement is a possibility of implementing the proposed models in practical solutions. Many research issues and tasks, which were later verified as part of the developed technology, were solved. The aforementioned publications tackled the issues of applying the already existing solutions in the areas, in which such solutions have not existed before. For example, the above refers to the application of biometrics and RFID technology [A_67], [P_2]. It should be stressed that the propositions of the new solutions have always considered variability of environment, in particular legal environment and its potential impact on the proposed applications. Furthermore, supplementary publications [B_3], [B_8], [B_10], [B_17], [B_38], [B_39] and [B_60] indicate to a possibility of using the integrated and general models in the crime prevention systems. The majority of them refer to the elements implemented during the execution of project [P_1]. On one hand, the developed technologies allowed to verify and solve many research issues, on the other – the analytical and project studies allowed to develop increasingly better technological solutions (e.g. in the context of their efficiency). The invoked publications also show how significant the impact of the legal environment (legislation) may be on the construction of efficient IT systems, in particular those that use public data resources. The result of the research studies is, among other things, a conclusion on the necessity to extend the "impact assessment" ()[4], which may significantly affect the existing and planned IT systems.

Contemporary development of the RFID and GPS technologies, miniaturization of devices and substantial reduction of production costs all translate into broader application of such technologies. As a result, it is possible to obtain additional information from the data derived from the operations of

[4]Impact assessment - one of the appendices to the draft normative act, which described expected effects of the proposed regulations according to the method of cost analysis and advantages. In theory, the impact assessment should be used to inform the entities responsible for creating law about the consequences, which the prepared legislative act may have on social life. The impact assessment constitutes an important element in the process of rule making, as it allows to provide specific merit-based arguments to introduce particular legislation.

devices with the RFID technology. In combination with the technology applied in GPS systems, it is possible to obtain data used not only for current operations of the operational systems, but also for conducting special analyses and research that may cover a broad thematic scope. It refers to, among other things, the issues of location and even (desirable) distribution of resources, possibility of appropriate reaction to adverse demographic or economic phenomena, making quick and correct decisions related to the management of resources. It also concerns man-made resources (products, infrastructure, pollution) and natural resources (water, animal populations, natural plants). The development of modern technologies, such as: biometrics, RFID or GPS allows to apply the same in many areas of human activity. The combination of the aforesaid technologies is an even greater challenge, giving even more possibilities of practical application. The result of such combination may be additional data and hence additional information, which would be time-consuming and expensive to obtain otherwise. Study [A_67] outlines the idea of creating a system for tracking and monitoring people, employing familiar technological solutions, which are partially used in the field of biometrics, RFID and GPS. The practical application of the proposed solutions depends on the level of technological advancement in the particular areas as well as organizational and legal development of interested parties.

Creation of uniform models for registration and recording of data used in IT systems has become an unquestioned necessity. It results, among other things, from a possibility of using a free flow of persons, goods, services, capital, e.g. within the territory of the European Union. Attempts to integrate the resources of the functional data and IT systems, where such resources function, show how complicated and costly this process is. Despite that, it seems justified to develop general data models (at least at the term and conceptual level) including both the scope and data flow. It is possible to obtain the desired result e.g. in the form of a uniform system at the level of data model. Thanks to the creation of specialist data meta-model, the methods used for data exploration may be applied. Another solution is to design and build from scratch the dedicated, specialist IT systems. Regardless of the approach, the point to integrate the systems by unifying the methods of identification of all objects, about which the information is collected, processed and made available. Without solving the identification issues, presented in [A_68], all further activities related to integration may be doomed to fail. The main issue, which is tackled during the analysis of the various data resources, are problems related to the **use of various methods for identifying the objects**. In practice, only recently the attention has been paid to the fact that the objects in different registers and records should be identified in the same manner. This conclusion results, among other things, from the fact that during the attempts of simultaneous analysis of the content of various registers and records some serious errors occurred. Even if identification of objects was correct within the framework of single register, then, in case of attempts of simultaneous use of a couple thereof, some serious problems occurred with respect to connecting the objects, about which the data were stored in many locations. Considering the above issues, it seems justified to analyze a larger number of registers to unify them and indicate the principles or rules that should be obeyed when next registers or records are created, or when working on implementation or modernization of the IT tools supporting the use of the already existing registers and records. Due to rapid development of IT technology and the necessity of modifying the already existing solutions, the introduction and implementation of some new rules in the process of creating uniform registers and records seems indispensable.

Study [A_66] includes a proposition to apply biometric technologies for both identification of people (ID documents) and maintenance of an appropriate level of security of data that are contained in identification documents. The identification of persons starts with the issuance of birth certificate and ends with death certificate. During such period, a person holds many documents, which include the identification data - a health certificate, school card, ID card, student card, passport, driving license, service card, work badge, access card, name membership card, residence card (...) - generally, we may state that the above refers to all documents containing data such as names, last names, dates of birth and

photographs. Both the ID card and the passport are documents establishing someone's identity. It mainly refers to persons aged over 18, in case of whom the issuance of the above-mentioned documents is mandatory, but children and adolescents (under the age of 18) may also obtain an ID card or passport upon request. Other documents are used more as a confirmation of someone's identity (it is often a case when a given person confirms his/her identity by producing more or two documents, containing a photograph of that person). Therefore, the ID card and the passport are treated in a special way. The identification data included in the ID card or passport are strictly protected. To this end, the security measures of "blank" forms (e.g. type of materials they are made of, protection against any attempts to modify their content), security measures related to the process of collecting and including such identification data in the forms (i.e. personalization) and security measures connected with the distribution and use of ID cards and passports are used. The authors also described various biometric technologies, which may be used to secure identification documents (both physical and behavioral characteristics), and pointed to the opportunities and limitations connected with their mass application. An opportunity, and in some cases – the necessity to use biometric data – results from broader application of IT technologies (in particular, online) in daily life and more frequent attempts to steal identity from persons using such technologies. A biometric document is a kind of "connector", which allows to associate a "natural person" ("a man of flesh and blood") with a "digital person" ("an electronic person composed of zeros and ones") that is present only in the IT system.

In publications [A_88], [A_9] and [A_14], the authors presented a concept of practical application of IT technologies using the general data model for combating all types of crimes. Article [A_14] outlines a concept of applying the methodology for identifying patterns to detect documents (proofs) suggesting the execution of some criminal financial transactions. The analogies of diagnostic processes for disease classification in medicine were used in the method. The detection of criminal financial transactions (financial crimes, supporting of terrorism, money laundering) is a difficult and complex issue. The total number of financial transactions in the national financial market reaches several millions of operations per day. The scope of diversity of financial transactions is really extensive. The financial transactions are executed in different transactional environments: physical environments, local networks, postal networks and global networks such as the Internet. To "fish out" criminal transactions is, therefore, a really complex, but also important process, as it may lead to quick and efficient identification of criminal groups and prediction of financial crimes, hence, allowing their earlier detection and prevention. Therefore, particular countries (including the whole European Union) introduce a number of regulations (including regulations equivalent to Acts of Parliament) imposing certain obligations (procedures) on financial institutions to ensure the undertaking of efficient actions preventing such events. In compliance with the provisions of relevant Acts, the financial institutions shall, as part of applying financial security measures, undertake the following actions: "monitor economic relations on an ongoing basis, including the inspection of transactions executed during such relations to ensure that the transactions are in accordance with the knowledge of a given institution regarding the client, business profile and the risk, including, where possible, the sources of funds, and to ensure that the documents, data or information held by the institutions are being updated regularly" ()[5]. Due to the scope and complexity of the financial flow system and, above all, due to the special role of detecting criminal financial transactions, it has become necessary to use appropriately designed IT systems supporting such activities. The appropriately designed and implemented IT systems may turn out to be an efficient tool supporting the detection of criminal financial transactions. The main module of such systems is the subsystem for detecting patterns of transactional documents used in criminal

[5] S. Acid, L.M. Campos, *A comparison of learning algorithms for Bayesian Networks: a case study based on data from an emergency medical service*, Artificial Intelligence in Medicine, vol. 30, pp. 215–232, 2004.

financial activities, which includes the multi-criteria module for the similarity analysis ()[6]. The automatically selected set of "suspicious financial documents" may be then "manually" verified by experts and used for subsequent operational activities.

Study [A_88] includes analysis of the available data resources within the scope of their feasible application for the purpose of detecting and combating crimes (mainly financial). The analyzed aspects were mainly related to: legal basis for the functioning of a given resource, bodies keeping registers/records, scope of collected data, method of processing and existing links and correlations between other data resources. Among other things, the following registers and data resources were taken into consideration: Central Population Register (register of personal identification numbers, PESEL), data collected by Registry Offices, Social Insurance Company, National Court Register, National Business Registry (REGON), National Criminal Records, New Land and Mortgage Register, Register of Pledges, data resources collected by the General Inspector of Financial Information, Court and Commercial Gazette, Business Activity Central Register and Information Record, National Taxpayer Register, Central Register of Vehicles and Drivers, resources of Tax Offices and Treasury Control Offices, Schengen Information System and Visa Information System, databases of Customs Service. The analysis concerned a possibility of using the available data resources for detecting and combating financial crimes. The contents of the presented data resources were limited from the financial and ownership point of view. The registers are made available by the institutions responsible for their maintenance. The above-mentioned analysis covered the data that may be used to detect and combat financial crimes (i.a. their information content, methods of processing, access methods and modes of access) and a description of their actual and current use by the institutions established to prosecute such crimes. The authors also pointed to certain limitations of access to the analyzed resources, including security elements related to data protection and processing. The conducted analysis may also allow to describe and recommend the application of the available thematic models in the future, e.g. ontology or object models used by identification and monitoring tools, e.g. financial operations. The models shall be useful to automate activities of the bodies responsible for the prosecution of financial crimes and establishment of collaboration in that respect (including mutual exchange of information, not only institutional as resulting from the legal regulations). The characteristics include the analysis of data resources and sets, which seemingly do not concern any ownership relations, but in fact may constitute significant output information, i.e. the information allowing to obtain such data (e.g. identification of a person). The analysis of data collected in particular sets and registers includes, among other things, the information contents (current data, historic data), structure (attributes, estimated percentage of data completeness), dynamics of changes in contents (volume, how much more/less it gets over time), connections with other registers/records, methods of processing (centrally or locally, electronically or traditionally/in paper form).

On the other hand, study [A_9] presents a new look on the use of existing data resources in combination with modern methods applied for the purpose of data processing. Modern ICT technologies allow efficient operations run against large amounts of data. The creation of dedicated analytical models allows to efficiently combat and prevent crimes, e.g. crimes committed against people, including child abuse. The article also characterized a possibility of using long existing data registers and records to

[6] A. Ameljańczyk, *Metryki Minkowskiego w tworzeniu uniwersalnych algorytmów rankingowych*, WAT Newsletter, Vol. LXIII, No. 2, pp. 324–336, 2014.
A. Ameljańczyk, *Analiza wpływu przyjętej koncepcji modelowania systemu wspomagania decyzji medycznych na sposób generowania ścieżek klinicznych*, Newsletter of the Institute of IT Systems, No. 4, p. 1-6, 2009.
A. Ameljańczyk, *Wielokryterialne mechanizmy wspomagania podejmowania decyzji klinicznych w modelu repozytorium w oparciu o wzorce*, Newsletter of the Institute of IT Systems, No.5, p. 2-8, 2010.
A. Ameljańczyk, *Metoda podziału zbioru obiektów na wielokryterialne klastry jakościowe*, Newsletter of the Institute of IT Systems, No. 12, p. 1–7, 2013.

prevent such crimes. The use of modern IT methods and tools in combination with the well-defined and integrated data sources (not only national) allows to increase detectability of certain types of crimes, without the necessity of involving additional efforts or means. Furthermore, the examples given may be applicable in many places worldwide even though they refer to data sources in specific countries. Such approach is also justified due to the fact that modern criminal activities are of international character.

Details and clarification of the issues described in [A_67], [A_68], [A_66], [A_88], [A_9] and [A_14] may be found in [B_3], [B_8], [B_10], [B_17], [B_38], [B_39] and [B_60] – mainly within the areas related to combating economic crimes.

The concept of using the general data model to design modern ICT tools, supporting the bodies and institutions combating economic crimes, may be outlined as in figure no. 1. The technology developed as part of the IAFEC project, described in [P_1], explicitly shows all the advantages of applying such concept.

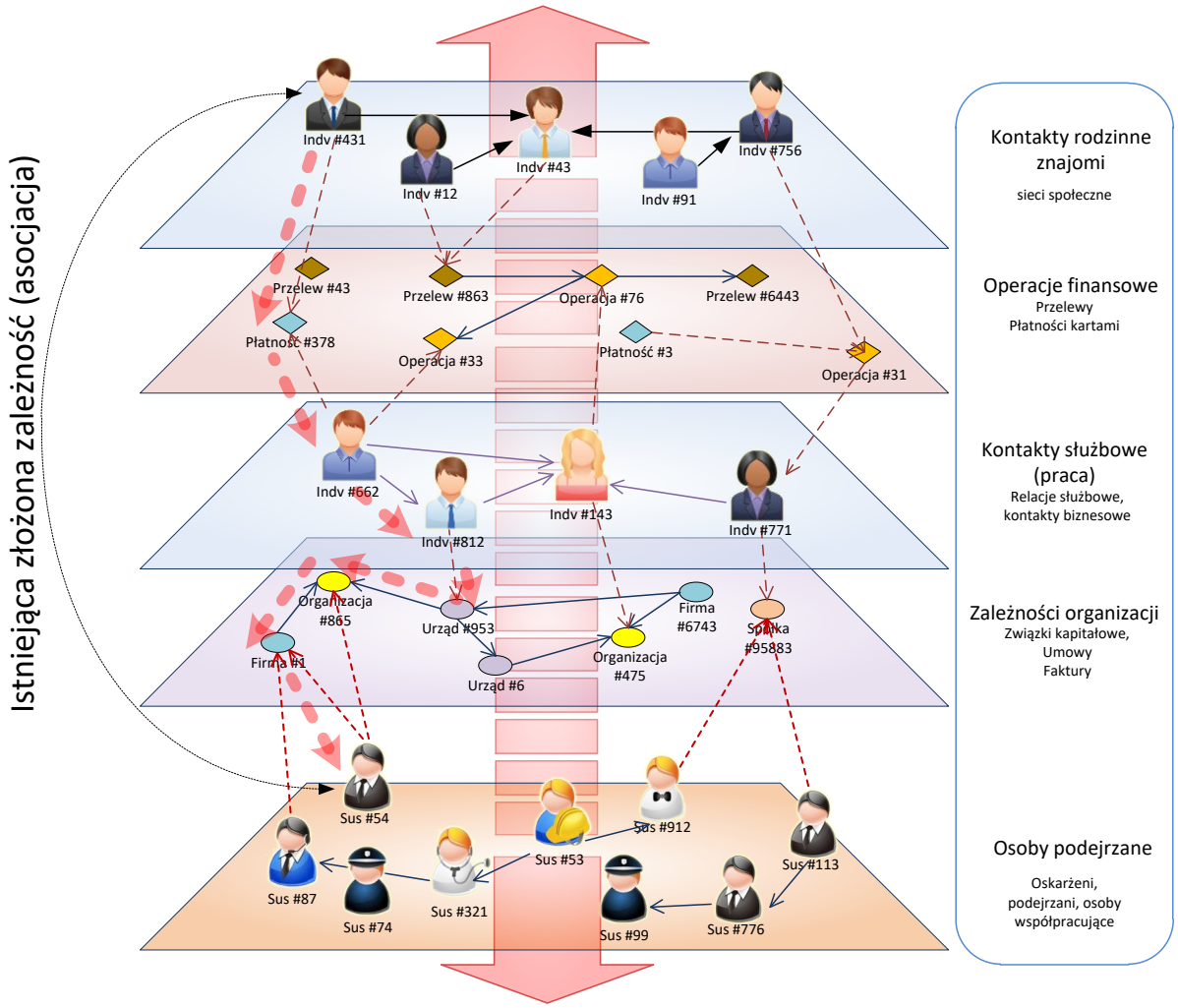

Figure 1. Correlations between entities/persons.

The concept was, among other things, characterized in monograph [B_3]. The integrated system of access and analysis of data from registers/records described therein constitutes a development project of national defense and security. The priority area of research, in which the project was submitted, are modern technologies and innovative solutions related to the use of sensitive data, detection and prevention of financial crimes. In compliance with the terms and conditions of the contest, the project referred to national defense and security, as this is the field, in which financial crimes may be observed.

Financial crimes, often understood as economic crimes and referred to as the "white-collar crimes", constitute a multi-dimensional phenomenon, whose one aspect is the national security. To ensure military and non-military security is the fundamental obligation of every state. The Act on Internal Security Agency and the Intelligence Agency stipulates that the Internal Security Agency shall be responsible for: recognizing, preventing and combating threats to Poland's internal security and its constitutional order, including in particular its sovereignty and international position, independence and integrity of its territory as well as public defense. In compliance with the above-mentioned Act, the Internal Security Agency is responsible for recognizing, preventing and detecting crimes threatening economic foundations of the country. In their analysis of crimes threatening economic foundations of the country, mentioned in the Act on Internal Security Agency and the Intelligence Agency, Grzemski and Krześ ()[7] observed that neither the aforesaid Act nor the previous Act on the Office for State Protection provides any definition of the term "economic foundations of the country". At a more general level, it may be surely ascertained that economic security of the country is one of the components of the national security, which is due to the fact that the country has implemented a specific social and economic policy. Significant protection of the fundamental economic interests of the country has direct impact on its functioning as a whole as well as on the operations of individual institutions responsible for re-distribution of goods among citizens.

Study [B_8] contains a description of tools and methods for detecting and assessing financial frauds based on the stream of transactional data from financial institutions. The presented original approach is aimed at processing the data that include the context and are derived on the basis of ontology and logical thinking using DL and FOL ()[8]. The domain terminology defines basic terms, correlations and rules of classification, which provide a possibility of semantic processing. The article contains grounds for implementing the concept of a set of tools used to identify frauds on the basis of the problem-solving ontology set. Methods, algorithms and software constitute a good source for the IAFEC analytical tools showing the analysis of semantic links. What is innovative in this approach is the inclusion of heterogeneous data analysis, which connects different data layers, extending the scope of available links between persons, organizations and entities on the financial market. Extensive descriptions of domains provide many methods for showing links in families, social groups, organizations, financial transactions and other correlations. Progress in automatic analysis and availability of tools for semantic processing may help analysts to extend the already existing methods of link analysis into the contextual processing of knowledge. The discussed research provides a broader insight into the analytical method and algorithms, which are based on logical thinking as well as identification and evaluation of associations present in the financial transactions supplemented with intelligence data. The developed method was provided as an independent computer application integrated with appropriate controllers and data integration services (as part of the implementation of tasks resulting from the scope of the project described in [P_1]).

The development of ICT methods and technologies in combination with the evolution of data models open up entirely new possibilities of their application in different areas of human activities. In particular, the above refers to such areas, which have been neglected so far, for example, due to large amounts of data or absence of analytical tools that could be used for efficient and effective data processing and analysis. The interest in using substantial data sources (Data Warehouse, Big Data, noSQL Databases, stream DB) largely boils down to the processing of more and more amounts of data

[7] J. Grzemski, A. Krześ, Analiza pojęcia „*przestępstwa godzące w podstawy ekonomiczne państwa*" in the Act of May 24, 2002 on Internal Security Agency and the Intelligence Agency, in: *Przegląd Bezpieczeństwa Wewnętrznego*, No. 2 (2012), p. 150–153.

[8] F. Baader, D. McGuinness, D. Nardi, P. Patel-Schneider, The Description Logic Handbook: Theory, Implementation, and applications, Cambridge University Press, ISBN 0521876257, 2007.

S. Staab, R. Studer, Handbook on Ontologies, Springer, ISBN 3540408347, 2004.

and larger data volumes. The same refers to social networks. The emergence of still more innovative data (information) solutions usually triggers the emergence of still more innovative ICT tools designed to handle such solutions. It appears that "old", well-structured databases for processing data in a traditional manner have been forgotten. The article [B_10] includes an attempt to look at these "old" data sources by using the cutting-edge IT techniques and methods for their analysis. The presented approach refers to the so-called public registers and records, which cover the whole population of a given country (region) or include data about all objects of a certain type (e.g. real estate records). Their basic feature is that they have been kept for several dozen years (even if initially maintained in a traditional, i.e. paper, manner), they are public (which not always means that everybody can use them) and usually managed by government or public administration units. A clear-cut advantage of such traditional databases is also the fact that the data contained therein are in most cases "cleaned" and complete. The presented examples mainly refer to Polish registers and records, but it was shown that they may also be applied in other non-European countries. The examples include issues connected with the analysis of seemingly unrelated registers and records as well as links between different persons (entities), with special emphasis on a possibility of using the results to combat and detect illegal activities, including analyses of crimes against people.

The subsequent three publications [B_38], [B_39] and [B_17] outline the concept of the IAFEC system (*Information Analysis of Financial and Economic Crime*), which was created as the result of R&D activities commissioned by the National Center for Research and Development [P_1]. The purpose of article [B_28] was to outline the concept of the IT system for combating economic crimes, including all the necessary modifications of the organizational and legal environment. The concept of the IAFEC system was created as a result of the activities aimed at verifying the possibilities of using different data resources for combating economic crimes (mainly in the field of finance). Due to the amount of such resources and their variability, current tools and methods for data analysis turn out to be too simple and do not meet the assumed expectations. The described propositions indicate to other ways of application of the known methods and other methods and techniques, which have not been used so far or have been used to a lesser extent for the purpose of analysis in the area of broad data resources. Attention was also drawn to formal and legal conditions, which - in many cases - create far-reaching limitations and make it impossible to conduct efficient analyses and undertake preventive measures. The study describes basic concepts related to the designed system treated as a set of tools for detecting and combating adverse economic phenomena. On the other hand, the purpose of article [B_39] was to present the modern architecture and system for supporting data analysis based on heterogeneous resources, using the SOA approach (Service Oriented Architecture) for various data analysis methods based on diverse analysis methods and algorithms (methods of graph and network analyses for searching paths on homogeneous and multi-layer graphs) to support combating economic crimes. The proposed architecture was presented from the point of view of the “Analyst” responsible for preparing data for analysis, conducting the analysis and presenting the results thereof for further proceedings. Due to the amount of such data resources and their variability, current tools and methods for data analysis prove insufficient. From the perspective of decision-makers, a possibility of obtaining the information based on analyzing all potential premises of specific actions makes it possible to take much better quality decisions in terms of further procedure (the risk of a wrong decision is mitigated). While developing the concept [B_38] and system architecture [B_39], one of the adopted assumptions was to obtain satisfactory results from the research before a financial crime “materializes” so that it is possible to mitigate or event eliminate potential (negative) effects of such undertaking. Study [B_17] supplementing the two above-mentioned articles presents the developed and implemented elements of the system for detecting and combating financial crimes – IAFEC. The concept of the IAFEC system elaborated on the basis thereof also uses the network model databases for the purpose of analysis. The

article describes the general architecture of the system and its information resources, including a method for obtaining data for the adopted data model. Every year, the country observes the increasingly higher losses to public finances caused by financial crimes, in particular money laundering. The model for detecting and combating such crimes, which has been implemented in Poland, is of a distributed nature, since it is based on the operations of many independent bodies and institutions. Furthermore, the development of technologies hinders efficient detection of financial crimes and the present methods use only manual analysis. Automation of the processes for obtaining and analyzing data increases the chance of efficient detection of money laundering. The aforementioned issue has formed grounds for undertaking appropriate activities and hence developing the IAFEC system intended for data analysis in terms of detecting and combating financial crimes.

The above-mentioned studies had to be based on the legal framework in broad context. The analysis of legal conditions is included, among other things, in study [B_60]. Recent years have seen a significant increase in economic crimes related to the application of modern ICT technologies. On the other hand, the same technologies allow to efficiently combat such crimes, in particular those related to money laundering. The effects of such technology development are the changes and extension of legal regulations concerning the issues of economic crimes and use of IT tools and methods used for their prevention. In particular, the legal regulations on the protection of information and data sets, among other things, in the field of bank, treasury, tax, ICT confidentiality and protection of personal data, were subject to the aforementioned changes. Publication [B_60] tackles basic issues related to the possibility of processing the data from that area. The scope of the collected and processed data was described and discussed in terms of the possibility and necessity of making such data available. A special emphasis was placed on making the data available to the authorities responsible for combating and detecting economic crimes related to money laundering. Special attention was paid to legal restrictions resulting from the necessity to comply with the confidentiality clause (i.a. bank, treasury, customs, tax advisor, ICT, insurance, doctor/patient, statistical, correspondence confidentiality as well as trade and official secrets). The presented analysis is mainly related to the possibilities of making the data available and potential scope of the processed and accessed data. The aforementioned examples show that – in compliance with the binding provisions of law – it is possible to clearly connect the IT solutions with access to relevant databases and efficiently combat economic crimes. Naturally, the presented examples were anonymized and narrowed to basic facts useful for the purpose of the aforesaid analysis. The last part of the article points to the necessity of ensuring an appropriate level of security while processing and accessing the data on financial crimes.

One of the innovative technological applications, which are aimed at confirming a possibility of using the RFID technology for safe processing of data (and other media) containing sensitive information, was to implement the project: “Electronic system for management of lifecycle of documents at varying sensitivity levels”, whose characteristics may be found in [P_2]. The main purpose of the project was to “develop innovative system of readers and IT services”, as part of the priority research area - “ Modern and innovative technologies and solutions for detecting, combating and neutralizing threats”. To achieve this objective, a system for tagging electronic media and paper documents with RFID tags was developed along with appropriate devices, which were designed or upgraded for that purpose. The final effect of the project implementation is a prototype of the modern secret office, where the latest RFID technological achievements are used and the manner of its operations and management are adapted to such technology, which allows to work with the documents at different levels of sensitivity.

As part of the project implementation, a model of unified processes for management of lifecycle of the documents at different level of sensitivity was developed. Prior to the system development and implementation, in compliance with the requirements of the administrator, unusual processes requiring customized services had to be re-defined. The main objective was achieved in stages by implementing

particular detailed goals. The development of the modern system for tagging electronic media and paper documents with RFID tags as well as design or upgrade of appropriate devices for completing such task required completion of the following detailed tasks: (1) development of the system for remote identification of public and non-public media tagged for the purpose of radio reading in places of storage and real time work; (2) development of the system for automatic stocktaking of public and non-public documents put into piles and kept in folders, including automatic detection of changes in their location; (3) development of the system for controlling media and public and non-public documents flowing between various risk zones, including an authentication module to allow access to public and non-public documents; (4) development of the system for electronic protection of media and documents against unauthorized dislocation; (5) automatic identification of media and documents not only in the area of storage, but also at work stations; (6) development of the technology of security measures protecting against multiple copying of public and non-public documents, limiting the number of possible copies; and (8) identification of location of a single public and non-public document, with accuracy to a predefined location of a folder or volume.

A list of titles of basic and supplementary publications used for the discussed issue appears below. The details of a given publication may be found in the list of the published academic papers.

[A_9] *Application possibilities of Advanced Analysis of Public Data Sources in the Fight Against Child Maltreatment.*

[A_14] *Multicriteria Methods for Identifying Patterns in the Analysis of the Flow of "Dangerous Financial Documents".*

[A_66] *Use of biometric data in identification documents.*

[A_67] *Location with the use of the RFID and GPS technologies - opportunities and threats.*

[A_68] *Objects identification in the information models used by information systems.*

[A_88] *Rejestry i zasoby informacyjne wykorzystywane przez organy odpowiedzialne za wykrywanie i przeciwdziałanie przestępczości.*

[P_1] *Projekt IAFEC.*

[P_2] *Projekt RFID.*

[B_3] *Zintegrowany system dostępu i analizy danych rejestrowych i ewidencyjnych* –w przygotowaniu

[B_8] *Financial fraud recognition and identification method using reasoning and quantitative association evaluation.*

[B_10] *Przestrzenne uwarunkowania wykorzystania zaawansowanej analizy danych w przeciwdziałaniu przestępczości.*

[B_17] *Wykrywanie i przeciwdziałanie przestępstwom finansowym z wykorzystaniem sieciowych baz danych - system IAFEC.*

[B_38] *Koncepcja systemu informatycznego wspomagającego zwalczanie przestępczości gospodarczej na przykładzie systemu IAFEC.*

[B_39] *Architektura systemu informatycznego wspomagającego zwalczanie przestępczości gospodarczej na przykładzie systemu IAFEC.*

[B_60] *Gromadzenie i przetwarzanie danych mających związek ze zwalczaniem przestępczości finansowej: Zasady dostępu, ograniczenia prawne.*

Summary

The development of ICT technologies calls for adequate changes in the manner of perceiving their impact on the present and the future. The issues discussed in the above-mentioned publications allow to assume that they significantly contribute to the development of the whole discipline, such as the information technology, in particular while treating the data and information as its basic elements.

The presented publications including both theoretical deliberations and practical applications of the research results explicitly show that the development of the information technology (as part of the technical sciences) is not possible without considering variability of the environment, which in turn reflects the issues taken from other disciplines (or areas). Such correlations are getting more and more complex. Since broader areas of human activity are under the influence of new technologies, the larger parts thereof become the areas of the operations of the information technology discipline. In the studies provided for evaluation, the thesis author attempted to find correlations and mutual impact between the environment determining "**which information shall be needed**" and the environment, in which it is decided "**what kind of data shall be processed**" so that the information is made available. In his work, the author also described practical solutions related to the development and application of ICT technologies, which to a large extent make it possible to consider the aforesaid correlations. It should be stressed that the presented deliberations are each time in accordance with the provisions on **need for maintaining the security** of data/information and **legal conditions**.

The results obtained during many years of R&D work concerning the discussed issues were divided into three thematic groups:

- General and thematic data models with respect to public administration repositories and registers; information resources of public administration.
- Selected aspects of security in the processing of information resources of public administration; process-oriented approach based on risk analysis.
- Application of proposed models for combating economic and financial crimes; legislative conditions.

indicate possibility of perceiving certain phenomena in broader context, often against initial assumptions resulting from tool limitations. The application of the advanced mathematical models by the thesis author confirmed such possibility. Additionally, when presenting the selected aspects of security while processing the information resources of public administration, the thesis author proved that the analysis of data resources (both quantitative and qualitative) may be conducted based on heterogeneous data sources with similar semantics.

The analysis of the available literature showed that there are no publications covering such diverse areas. The available national and international publications only refer to the selected single elements described herein. The referenced sources show that the presented range of publications may significantly contribute to a broader perspective on the discussed issues and extend the achievements in the field the information technology and technical sciences.

Discussion of other scientific and research achievements.

Thematic scope	number	in total
Group "A" – publications covering the aforementioned academic achievements (including 2 reports on project implementation)	**17** (+2)	
Group "B" – publications supplementing academic achievements	31	
Group "C" – other publications	68	116+2
Type of publication		
Monographs	5	
Articles in journals	49	
Chapters in monographs	44	
Scholarly editing of monographs	7 (+2)	
Published conference materials	11	116+2
Authorship		
Author (independently)	**37**	
Co-author (two authors)	28	
Co-author (three authors)	22	
Co-author (four authors and more)	29 (+2)	116+2

Table 2. Aggregated data on the number of publications in the period by 2000.

The thesis author participated in **8 R&D projects**, **in 2 of which acted as the Project Manager**. Two of the above-mentioned projects included collaboration with international academic centers, one of which included collaboration with academic centers in the United States, whereas the other - in the European Union.

The thesis author participated in **17 foreign** (international) academic conferences, where he was **a speaker** (or co-speaker) **42 times**. The topics of such conferences were closely related to the topics tackled in the publications mentioned herein as academic achievements. Some of the speeches were later published in the conference journals or other materials. Furthermore, the thesis author participated in **29 national** academic conferences, where he was a speaker **36 times**. He actively took part in thematic seminars to promote science.

His active participation in the academic conferences meant, among other things, **chairing 7** thematic (special) **sessions** during **4 international conferences** and one national. The thesis author was a **member of Academic Committees or Steering Committees at 6 international conference**s. He was also a member of the Organizational Committee at a national conference. He participated in 5 consortia (mainly to implement R&D projects).

He was a thesis supervisor of around **150 diploma projects** (postgraduate courses – 5, uniform studies – 47, first and second cycle degree programs – 93). He provided didactic care for individual students. He also prepared a number of expert opinions and scholarly publications in the field covered by the academic achievements (|i.a. Reviews of R&D projects). He has been a member of many expert teams in that area.

The thesis author received many medals and distinctions, including the Medal of the Commission of National Education awarded by the Minister of National Education.

It should be also mentioned that the thesis author – apart from the work in the aforementioned academic units – was also engaged in public administration units and commercial enterprises. His employment and work for the above-mentioned entities constitute a very good example of combining the concepts and solutions emerging as part of the R&D activities with the actual application of effects while creating IT systems that are supposed to operate in practice. Examples of the systems that have been designed and implemented in different areas of human life explicitly show the right direction and development of the academic achievements being the subject hereof. On the other hand, practical experience of the thesis author was useful in terms of developing the issues described in the presented publications.

The experience of the thesis author results, among other things, from his work in such institutions as:

1. PKO BP, 1991-2001. Data analyst. ERP systems for management reporting.
2. Ministry of Justice, 2003-2005. Implementation and supervision of projects of the systems used in the Ministry of Justice. Including: registration systems (National Court Register, Register of Pledges, Electronic Land and Mortgage Register), systems supporting the work of courts, IT systems in the Prosecutor's Office, projects related to the use of aid measures (i.a. PHARE, Transition Facility, SIS II VIS).
3. Ministry of Interior Affairs and Administration, 2005-2008. Implementation and supervision of projects of the registration systems used by the Ministry of Interior Affairs and Administration (PESEL System, National Records of Issued and Lost ID Cards, Central Records of Issued and Invalid Passports). Implementation and supervision of projects related to the incorporation of biometric data into passports and travel documents of aliens. Preparation of a project of new biometric ID card. Concept and implementation of a project of a new biometric passport – implementation of the system, including the issuance of biometric passports.
4. Editorial section of "Polityka", 1994-2004: project, implementation and maintenance of the system for financial settlements and subscription.
5. "Office Depot", 1998-2002: project, implementation and maintenance of the system for operating a store chain.
6. "STROP" Housing Cooperative, 1991-1994. Design and programming of financial applications and settlement of home loans.

The tasks completed as part of the work in the aforementioned institutions were closely related to the scope of the R&D activities performed by the thesis author. They allowed to connected the theoretical results with practice in a creative and innovative manner. On one hand, they offered a possibility of verifying in practice the assumptions made during the theoretical deliberations, and on the other – using the experiences gained during the implementation of IT projects at a later stage of development of the theoretical studies.

The details concerning other R&D achievements indicated in this point are in appendix "Z.3. List of academic projects and achievements …".

……
Maciej Kiedrowicz