V.I. VERNADSKY TAURIDA NATIONAL UNIVERSITY

COMPUTER SYSTEMS, TECHNOLOGIES AND CYBER SECURITY ASPECTS

Collective monograph

Lviv-Toruń
Liha-Pres
2019

Reviewers:

Dr inż. ***Michał Sójka****, Dean of the Faculty of Mechanical Engineering of Cuiavian University in Wloclawek (Republic of Poland);*

Dr ***Zbigniew Brenda****, Director of Logistics and Technology Institute of Cuiavian University in Wloclawek (Republic of Poland);*

Prof. dr hab. ***Ryszard Strzelecki****, Politechnika Gdańska / Gdansk University of Technology (Republic of Poland).*

Computer systems, technologies and cyber security aspects : collective monograph / M. H. Medvediev, V. B. Kyselov, V. I. Domnich, O. M. Muliava. – Lviv-Toruń : Liha-Pres, 2019. – 164 s.

ISBN 978-966-397-104-9

Liha-Pres is an international publishing house which belongs to the category „C" according to the classification of Research School for Socio-Economic and Natural Sciences of the Environment (SENSE) [isn: 3943, 1705, 1704, 1703, 1702, 1701; prefixMetCode: 978966397]. Official website – www.sense.nl.

Here we deal with the modern computer systems and technologies, levels of the organization of the computer integrated production, systems of intelligent data analysis, geographic information systems, preparation support and decision-making systems. Separate aspects of information security of information systems and networks of a modern company (organization) are considered.

ISBN 978-966-397-104-9

CONTENTS

INTRODUCTION

Modern production and life are no longer possible without the use of computer technology and associated technologies that accompany it. Especially strikingly it “breaks” into the agrarian sector of the economy of Ukraine, where not so long ago manual labor provided the final result. Today, poultry farms, hothouse combines, factories for the production and processing of mushroom production, woodworking enterprises effectively use technical means capable of implementing intelligent control algorithms as separate technological processes, as well as production in general.

This became possible due to the use of computer-integrated systems and technologies, which largely unload the personnel from the adoption and implementation of decisions aimed at maximizing profits of production, and so on.

In the modern world, the transfer of information takes place in public networks. To develop the own infrastructure for the transfer of information in conditions of rapid technological change is too costly and hopeless. Therefore, the tasks of security and protection of modern information networks of large companies and organizations are relevant.

In the local computer systems, the threats of disclosure and integrity of information are most common, and in the global, the first is the threat of denial of service.

In this regard, the aspects of information security of information systems and networks of modern companies (organizations), the basic mechanisms of organization of attacks on information networks, as well as the basic means and methods of protection of complex information systems are considered. The main modern cryptographic algorithms are presented and the approximate estimation of reliability and degree of vulnerability of standard algorithms of information encryption is presented here.

DOI https://doi.org/10.36059/978-966-397-104-9/5-28

COMPUTER SYSTEMS AND TECHNOLOGIES

Medvediev M. H.

1. The emergence of information technology

The notion of "information technology" arose in the last decades of the XX century in the process of formation of computer science. The peculiarity of information technology is that in it both the subject and the product of work are information, and instruments of labor – the means of computer technology and communication. Information technology as a science of information production arose precisely because information was considered to be a completely real production resource, along with other material resources. At the same time, the production of information and its top-level – knowledge – has a decisive influence on the modification and creation of new industrial technologies. By information technologies means the whole set of forms, methods and means of automation of information activities in various spheres. To date, the general theory of information technology (IT) as a system of integral interconnected techniques, methods and means of information processing has not been developed, the basic concepts of IT are not defined. However, it is enough to understand the essence of IT, as well as explain its scientific and practical importance. Moreover, the design and creation of specific IT intertwines many tasks from various scientific disciplines[1].

As a science, IT includes methodological and methodological provisions, organizational settings, methods of using instrumental and technical means – all that regulates and supports the information production and activities of people involved in this production. The transformation of new scientific knowledge into specific information technology is the main task of IT as a science.

In view of the discussion of the subject of discussion, we give a few notions of IT: a set of scientific methods and techniques for the production of information products and services with the use of all the diversity of computing facilities and communications; it is a border area that covers

[1] Vitkup M.E. Informatics and computer engineering (MSOffice in examples and problems with methods of their solution): Tutorial / M.E. Vitkup, V.V. Petrenko. K.: Центр «Методика-информ», 2002. 351 c.

both computing technology and a specific social information practice that rationalized it at the expense of widespread use of computer technology; This is a collection of fundamentally new tools and methods that provide creation, processing, transmission, display and storage of information.

A huge impetus to the development of information technology brought the development of multimedia. From this point of view, information technology – a set of methods and methods for receiving, processing, presenting information aimed at changing its state, properties, form, content and carried out in the interests of users.

According to the definition of IT adopted by UNESCO, information technology is a complex of interrelated scientific, technological, engineering disciplines studying methods of efficient organization of labor of people engaged in the processing and storage of information; computer technology and methods of organization and interaction with people and industrial equipment, their practical applications, as well as all social, economic and cultural problems associated with them.

IT require complex training, large primary costs and high technology. Their introduction should begin with the creation of mathematical support, the formation of information flows in the training systems of specialists. Recently, the following terms have become widespread: paperless technology, interactive technology, programming technology, database design technology, CALS-technology (Continuous Acquisition and Lifecycle Sourror), network technology, Internet technology, technology for analysis and reengineering of business processes, etc. All of them assume the use of information, any kind of information about the objects, facts, concepts of the subject area.

There are three levels of information technology review: the first level is the theoretical. The main task – the creation of a complex of interrelated models of information processes, compatible with parameters and criteria. The second level is research. The main task – the development of methods that allow automated design of optimal concrete information technology; The third level is applied, which is divided into two parts: instrumental and substantive.

Instrumental part (analogue – equipment, machine tools) determines ways and means of realization of information technologies, which can be divided into: methodical; informational; mathematical; algorithmic; technical; software.

The subject is connected with the specifics of a specific subject area and is reflected in specialized information technologies, for example, organizational management, technological process management, automated design, training and others.

Information technology provides a transition from routine to industrial methods and tools of work with information in various areas of human activity, providing the opportunity to use it rationally and effectively.

1.1 Concept and components (structure) of information technologies

Under information technology is understood a set of methods, production and software and technological tools, integrated into the technological chain, which provides for the collection, storage, processing, output and dissemination of information. Information technologies are designed to reduce the complexity of processes of using information resources.

Computer information technologies mean the use of computer facilities and network technologies for the implementation of a wide range of tasks: the preparation of text documents; creation of data banks, their processing and use; automation of financial and scientific calculations; making of books, newspapers, magazines; creating and editing graphic and photo images; creation of cartoons; creation of electronic encyclopedias and electronic versions of other books; creation and computer processing of sound; creation and computer processing of television and video; creation and use of telecommunication computer networks; computer design of various mechanisms, architectural structures, creation of geographic maps, etc.; modeling of natural, technical and other processes.

IT is an integral system that functions in a single information space due to the consistent work of all its components. Implementation of the system and its deployment in time provides the dynamics of information technology development, its modification, restructuring, joining of new components of the system and modernization. IT consists of interconnected components, which are grouped into three groups: basic technologies, specific technologies of AE (Application Environment) (enterprise, corporation, office, firm, etc.) and knowledge base of AE[2].

AE displays in the database a collection of objects of the real world with their connections belonging to a certain field of knowledge and of

[2] Марк Спортак, Френк Паппас и др. Компьютерные сети и сетевые технологии. Platinum Edition: Пер. с англ./ СПб.: ООО «ДиаСофтЮП», 2005. 720 с.

practical value to users. The subject area exists independently of both the creator of the IS and the IS itself.

The AE model is a certain system that mimics the structure and functioning of the research subject area and meets the basic requirements – to be adequate to this area. The value of such models, such as reference ones, is that they reliably convey the specifics of the subject area, while the template model represents a solution to the problem in a defined context, but allows for use in other contexts.

Basic technologies – a set of hardware automation, system and application software, which implement the subsystem of storage and processing of information.

Knowledge Base (KB) is a formal representation of a coherent, consistent compendium of judgments reflecting the knowledge of AE. KB contains both a database (scheduled tasks, accounting, production, scientific, legislative, auxiliary information), as well as the user interface. The main form of organizing information on carriers is a database.

Data Base (DB) is a named set of structured data that reflects the state of objects and their relationships with such minimal redundancy, which allows it to be used for one or more applications in a certain AE.

1.2 Information processes

The notion of information is inseparable from the notion of information processes. Information processes include: information transfer; receiving information; storage of information; processing of information and its representation for use; use of information.

Information technologies can practically be implemented in non-automated (traditional or, in other words, "paper"), and in an automated form.

The hardware components are a personal computer, office equipment, communication lines, network equipment. The software is directly dependent on the hardware and information support and implements the functions of accumulation, processing, analysis, storage, interface with the computer.

Infoware – a set of data presented in a certain form for computer processing. Data – information obtained by measurement, observation, logical or arithmetic operations, are presented in a form suitable for storage, transmission and processing. Organizational and methodical

support is a set of measures aimed at the functioning of the computer and software for obtaining the desired result.

There is another approach to considering the structure of automated IT, according to which any IT can be divided into three interdependent and equivalent components that make up its core: hardware; software; brainware. In addition to the above mentioned core of the IT, there is another, very important component – the IT support network, Infrastructure – the necessary physical, administrative and organizational structures, cultural schemes, standards and criteria, and so on. The advocates of this approach believe that the merger or merger of information technology into larger structures – technology systems (using the term "information technology and systems" – IT/S) should be considered in practice.

However, the mere availability of the necessary components that make up IT (complexes of technical and software tools, as well as information and organizational and methodological support) is not enough to "revitalize" the technology. Implementation of IT is possible in a specific environment – the information system.

1.3 Properties and classification of information technologies

Among the properties of IT should indicate the following: expediency – increasing the efficiency of production based on the use of modern DEC, distributed information processing, distributed databases, various information networks (ICN) through the circulation of information and processing; the presence of components (specific content of processes of circulation and processing of information) and structures (internal organization, which are the interconnections of the components that make it, are grouped into two large groups: reference technology and knowledge base); interaction with the environment; integrity; development in time.

The classification of IT depends on the classification criterion. The criterion may be the indicator or a set of features that affect the choice of one IT or another. Different schemes of IT classification are possible. Each of them is based on certain classification characteristics.

The first sign of classification is the absence or availability of automation. In this case, here are traditional and automated technologies. Providing and functional information technology.

Providing technologies can be used as tools in various subject areas for solving various problems. They can be classified according to the types of tasks that they solve. Examples of technology providing are text processing technologies, database management systems. Usually these technologies can be performed on different computers and in different software environments. The main task is combining these technologies into a single information system. Functional technologies are a set of providing technologies for the automation of some task, function. The technology of processing information on a computer can consist of a predefined sequence of operations and does not require the user to interfere in the processing process. In this case, the dialog with the user is null and the information will be processed in batch processing mode.

Tasks solved in batch mode, are characterized by the following: the algorithm for solving the problem is formalized, the process of its solution does not require human intervention; There is a large amount of incoming and outgoing data, much of which is stored on electronic media; the calculation is performed for most entries of the input files; big time solution to the problem due to large volumes of data; tasks are solved with a given periodicity. If you need a direct user interaction with a computer, where the user receives instantaneous computer actions for each of his actions, the dialogue mode of information processing is used.

Dialogue mode is the evolution of batch processing mode. Dialogue mode provides for the absence of a rigorous security operation with operational data, unless it is conditioned by the subject matter technology.

Next classification mark is the type of processed information.

Information is a set of known properties of an object or process, which are subjects of knowledge.

Information is a set of signals of physical processes, which are perceived by the subject through the organs of his senses.

All the information that a person uses, can be divided into the following types: mathematical is any information associated with numbers and formulas. In addition, in fact, mathematical, it can be both physical and statistical information. Mathematical information can be processed using various counting machines and apparatuses and stored on paper in the form of records and books; textual – this information can be written on paper by hand or by means of a PC and stored on paper (manuscripts, documents, books, newspapers, etc.) or electronic media; graphic – this information

can be processed using various visual means and methods (fine arts, photography) or special graphic editors and stored in the form of paintings, drawings, sculptures, photographs, etc.; sound – this information can be processed with a tape recorder or special sound editors and stored on magnetic tapes, recorders and audio CDs and electronic media; video information – this information can be processed with motion picture and video equipment or video editing software and stored on film, video tapes and electronic media.

All these types of information existed before the computer appeared. A modern personal computer has allowed processing all these types of information and greatly facilitated their sharing.

Today, it is possible to combine different forms of information representation on a single media, thanks to multimedia technologies.

2. History of CT development

Automation of the processes of work naturally goes through several stages: partial mechanization, complex mechanization, partial automation and complex or complete automation. At present, CTs are divided to: CT 1 generation (1965–1975) – elemental base, discrete semiconductors, programmable media – magnetic tape (unitary code BCK-5), devices K-4MI, K2P (ZP), KPT; CT 2 generation (1966–1982) – an elemental base of chips of series 155, 176, a programmer – an eight-track punch tape (ISO-7 bit), devices N22, series P; CT 3 generation (1977–1989) – element base VIS of series 589 (software implementation of control algorithms, storage of programs in memory, expansion of technological functions), software – eight-track punch tape; KT 4 generation (1985–1990) – block multiprocessor implementation, specialized VIS, high-level languages for technological functions programming, electroautomatics, dialogue, programming – eight-track pistol (ISO-7 bit code), the ability to add a communication program to the computer; 5 generations (1990–...) – industrial PCs, multiprocessor systems.

At each stage of the development of science and production, a certain approach was applied, appropriate design solutions and elements were proposed. From the user's point of view, each improvement was directed, first of all, to the following: increasing the level of mechanization and automation of the implementation of frequently repeated technical

operations; creation of new input and output tools; increase a memory space; the development of new data storage devices, etc.

Management of technological processes based on SCADA-systems began to be implemented in the leading western countries in the 80's of the twentieth century. In the 90 years of the last century began to appear software systems, through which any employee can observe the work of an arbitrary unit of equipment. These include the Factory Suite (Industrial Set) of the company "Wonderware" (USA) and Genesis (Revival) firm "Iconics" (USA). So, the Factory Suite consolidates the MES levels.

MRP – DBA Manufacturing, MRP Design Group, Ascent company, etc.

MES – Lighthouse Systems, KIS «Omega Production», Oracle E-Business Suite (OEBS)

SCADA – In Touch (Wonderware, USA), iFIX (Intellution, USA), SIMATIC WinCC (Siemens, Germany), Citect (Ci technologies, Australia), RTAP / plus (HP, Canada), Wizcon (PC Soft International, Israel- USA), Sitex and Phocus (Jade SoftWare, UK), Real Flex (BJ Software Systems, USA), Factory Link (US Data Corp., USA), View Star 750 (AEG, Germany), PlantScape (SCAN 3000) Honeywell, USA), Schneider Electric (France).

3. Application and main purpose of computer technology (CT)

CTs are best suited for automation of continuous and discrete processes, and are used in the following areas: production management; transmission and distribution of electricity; industrial production; water purification and water separation; management of space objects; transport management (all types of transport: air transportation, metro, railway, automobile, water); telecommunications; military industry.

In addition, the introduction of CT in medicine is perspective. In the world, there are more than a dozen companies that are actively engaged in the development and implementation of computer-integrated technologies in the medical sector, and software products of some of these companies are represented on the Ukrainian market.

The main objective of computer technologies is the creation and operation of computer integrated management systems that provide the solution of tasks of coordinating the operation of subsystems, the use of

intelligent subsystems of decision support on the basis of databases and knowledge and management systems.

This kind of activity requires the knowledge of special software. At the same time, computer-integrated technologies are closely linked to systems of automatic control and automation of processes in various industries and production.

3.1 Levels of computer-integrated production organization

Computer-integrated production contains five levels of automation:

I/O (Input/Output) – the level of communication with the equipment. Here the coordination of external elements with the control device is provided.

Control – At the control level, the control devices built into the equipment control the signals of state-of-the-art sensors by producing control commands for actuators – drives, valves, lights and sound signals[3].

I/O and Control levels are sufficient to control the process equipment.

In the process of development of automation, the level of control of technological equipment and the level of organization of production became closer to each other. Now, simultaneously with the management information on the operation of equipment in real time is transmitted to the level of generalized control and SCADA data collection.

SCADA (Supervisory Control and Data Acquisition) – at the SCADA level, they sort, transform and store current data, as well as their mapping in the process mnemonic. For the controller, the behavior of all units of equipment is displayed: the current state and performance of machines, the movement of material flows, generalized information.

SCADA systems allow you to observe the process as a whole, track emergency information, time trends and statistical characteristics of the process. If necessary, the controller transfers generalized control commands to the equipment and can remotely reprogram the remote automation systems.

MRP (Manufactory Resources Planning) – resource planning level. This is a well-known version of office activities automation for the purpose of accounting, financial management and logistics, organization of document circulation. At this level, production managers analyze the

[3] В.С. Билоусько, Т.И. Чуждан Вычислительные машины и программирование: Практикум / В.Е. Антипенский, К.: Вища шк. Головное изд-во, 1987. 245 с.

market-oriented strategy: the dynamics of market prices for manufactured products, the level of profit for different types of products, and predict demand.

MES (Manufacturing Execution System) – an additional level of execution of tasks that connects top managers with current production. Here information from SCADA is converted into information for the MRP, the database is updated, the sequence of operations is monitored, the scheduling of inspection and repair of the equipment is formed depending on the duration of actual operation. After analyzing this information from the position of production and business policy of the enterprise strategic manager decisions are executed at lower levels.

In the 1990s, software systems that could receive information from any of the five levels of computer-integrated production began to emerge. The MRP top level manager can go to a lower level of automation to analyze the work of any unit of equipment. On the other hand, the debugger of the equipment at a lower level can, by going to the Internet through the upper level, get from the manufacturer from anywhere on the planet a troubleshooting instruction.

3.2 Information systems (IS)

Simultaneously with the widespread use of new information technologies, the concept "information system" (IS) appeared. Information System – (Computer-Based Information System) is a complex of computing and communication equipment, software, linguistic resources and information resources that provides for their collection, storage, updating, distribution and processing in order to support any kind of activity.

Consequently, IS is understood as a set of interconnected components that work together to achieve a certain goal. To describe the system, the following concepts are used: structure (set of elements and relationships between them); inputs and outputs (material, financial and information flows entering and outputting the system); laws of behavior (functions connecting inputs and outputs of the system); goals and constraints (the processes of the system being described by a number of variables, usually limited to individual variables).

Until now, the processing of economic information has been isolated in a separate independent scientific and technical direction, which is characterized by a huge variety of ideas and methods. At the same time,

individual elements of the information processing process have reached a high level of organization and interconnection, which allows combining all means of information processing on a particular economic object with the notion of "Economic Information System".

An economic information system is a system whose functioning consists in collecting, storing, processing and disseminating information about the activities of any real economic object.

The main role of the economic information system is to organize the storage and transmission of information. Consequently, the implementation of the functions of the information system is impossible without an information technology oriented to it.

The economic information system is based on two components: system and information.

A system can be defined as a set of interconnected elements acting as a unit.

Information can be defined as a variety of new information that allows you to improve the processes associated with the transformation of matter, energy and information itself.

Management is a change in the state of the system, which leads to the achievement of the goal.

The process of control of the system is determined by the objectives of management, the environment and internal conditions.

From the standpoint of cybernetics, this process is interpreted as a directed action on the elements of the system to achieve the goal, and can be represented as an information process that relates the external environment, object and control switch.

The information exchange that underlies the process of managing the system consists in the cyclic implementation of the following procedures: collecting information about the current state of the controlled object; analysis of the received information and comparison of the current state of the object with the desired; developing a control action to convert the controlled object to the desired state; transmission of the control to the object.

The organizational structure of an economic object regulates the scheme of information flows of the management system, decision-making levels. Typical organizational structures are: 1) management information – a set of planning, regulatory and policy information,

which is formed by the control switch (subject of management) in accordance with the purpose of management and information about the environment; 2) accounting and reporting information, which is formed by the object of management and reflects the internal state and degree of influence on the object of the environment; 3) information on the external environment – regulatory and legislative information created by government agencies, information on market conditions created by competitors, suppliers, consumers.

Flows of control information are sent from the subject to the object of management. The effectiveness of management is achieved through feedback – obtaining information about the current state of the controlled object. Based on the analysis of information flows, appropriate management decisions are made. Output information is intended for other objects of the economy, higher standing organizations: reporting financial information – for government agencies, investors, creditors, and so on; marketing information – for potential consumers. The basic elements on which the management system of the organization is based include: goals and strategies; business processes; organizational structure (management structure); ways of interaction (flows and communication); regulations and motivation (employees).

The task of developing a management system, improving its efficiency and the whole business in general, is to support each of its elements in the required state. An interconnected set of tools, methods, personnel used to store, process, and issue information in order to achieve the goal is the information system (IS).

With the development of computer technology, the meaning of information system changed . The modern information system is a set of information technologies aimed at supporting the lifecycle of information and includes three main processes: data processing, information management and knowledge management. In the context of a sharp increase in the volume of information, the transition to working with knowledge on the basis of artificial intelligence is probably the only alternative to the information society.

Thus, the information system is an organized, interconnected set of IT tools and techniques that are used to store, process, and issue information to achieve a specific goal.

Implementation of IS improves the efficiency of production and economic activity of the enterprise due to not only processing and storage of information, automation of routine work, but also fundamentally new methods of management.

New methods of management are based on modeling the actions of specialists in decision making (methods of artificial intelligence, expert systems, etc.), using modern telecommunication facilities (e-mail, teleconferencing), global and local area computer networks.

The main ways of building an IS:

- development of the custom design system;
- use of prototypes – instead of a complete system, a prototype is created that meets the basic needs of users: the definition of basic queries; creating a working prototype; use a working prototype; view and improve the prototype; work with the final version of the prototype; use of ready-made solutions – it is recommended to maximize the use of standard business automation technologies; use of third-party services to transfer control functions – an IS organization uses a specialized firm that performs control functions for the operation and development of an IS company.

Benefits: – guaranteed quality of service; – saving money; <t0 /> <t1 /> human resources.

Gaps: – information leakage; dependence; loss of IT control.

In the field of application, information systems are classified as follows: IS for research; IS of automated design; IS of organizational management.

Scientific ICs are used for automation of scientific activity, analysis of statistical information, experimental management. IS of automated designing is used for: development of new products and technologies for their production; various engineering calculations; creation of graphic documentation (drawings, diagrams, charts, etc.); simulation of projected objects.

The IS of organizational management is intended for automation of the functions of the administrative apparatus. These include the IP management of both industrial enterprises and non-industrial objects (banks, exchanges, insurance companies, hotels, etc.) and separate offices (office systems).

IS control processes are created to automate various technological processes.

3.3 Structural IS analysis technologies

In the 70's and 80's. Twentieth century In the development of IS, a structured methodology was developed that provides developers with the strict formalized methods for describing IS and accepted technical solutions. It is based on visual graphic techniques: diagrams and charts are used to describe different types of IS models.

Under the structural analysis, it is common ground to refer to the method of research of a system, which begins with its general review, and then is detailed, providing for a hierarchical structure with an increasing number of levels. Its essence consists in partitioning the system into functional subsystems, which, in turn, are divided into subfunctions that are assigned to tasks, and so on. The process of breaking up continues to specific procedures. At the same time, the automated system retains a holistic view, in which all components are interconnected. When developing the system "bottom-up" from individual tasks to the whole system of integrity is lost, there are problems with the information compression of individual components. For such methods, a breakdown at the level of abstraction with a limitation of the number of elements at each of the levels is characteristic; limited context, which includes only essential parts at each level; the use of strict formal recording rules; consistent approximation to the final result.

All structural analysis methodologies are based on a number of general principles, the basic ones of which are the following: the principle of decomposition of the system, which is the principle of solving complex problems by breaking them down into a set of smaller, independent tasks that are easy to resolve; the principle of hierarchical ordering, which consists in the organization of the components of the task in the hierarchical structure. In addition, the important principles are: the principle of abstraction – is to allocate the essential aspects of the system and the separation from the non-essential; the principle of formalization – lies in the need for a strict methodological approach to the problem of the principle of consistency – lies in the validity and consistency of the elements; the principle of structuring data – is that the data must be structured and hierarchically organized.

In the structural analysis, mainly two groups of tools are used, which illustrate the functions performed by the system, and the relationships

between the data. The listed funds together give a complete description of the IS regardless of whether it exists or is being developed.

Visibility and clarity of structural analysis tools allowed developers and future users of the system to informally participate in its creation from the outset, to discuss and consolidate understanding of key technical solutions. However, the widespread use of this methodology and the imitation of its recommendations in the development of specific IS has been quite rare, as it is practically impossible for non-automated (manual) development. Indeed, manually it is very difficult to manually design and graphically present clear formal system specifications, check them for completeness and consistency, and moreover, to change. If you still manage to create a rigorous system of project documents, then their processing in the event of serious changes is practically impossible. Manual development usually caused the following problems: inadequate specification requirements; failure to detect errors in design decisions; low quality of documentation, which reduces performance; protracted cycle and unsatisfactory test results. On the other hand, IP developers historically have always been the last in a number of those who used computer technology to improve quality, reliability and productivity in their own work (the phenomenon of "The cobbler's children have no shoes").

These factors contributed to the emergence of software-technological tools of the special class – CASE-tools (Computer Aided Software Engineering), implementing CASE-technology for creating and maintaining IS.

CASE technology is an IS design methodology, as well as a set of tools that allow you to visualize the subject area, analyze this model at all stages of IS development and maintenance, and develop applications in accordance with the information needs of users. Most existing CASE-based tools are based on structured (mostly) or object-oriented analysis and design methodologies that use charts or text-based specifications to describe external requirements, relationships between system models, system behavior dynamics, and software architectures .

Each group of tools corresponds to certain types of models (diagrams), the most common of which are the following: SADT (Structured Analysis and Design Technique) models and corresponding functional charts; DFD (Data Flow Diagrams) of data flow diagrams; ERD (Entity – Relationship Diagrams) of the essence of the diagram.

The SADT model provides a complete, accurate, and adequate description of a system that has a specific purpose. This purpose, which is called the model's purpose, stems from the formal definition of the model in SADT. SADT models use both natural and graphic languages. For the transfer of information about a particular system, the source of the natural language is the people who describe the system, and the source of the graphic language is the SADT method itself. The SADT graphical language provides the structure and exact semantics of the natural language model. The SADT graphic language organizes a natural language in a well defined and unambiguous way.

In terms of SADT, the model can describe either the functions of the system or its objects. Functional-oriented SADT models are called functional models, but object-oriented systems – data models. The functional model with the necessary degree of detail represents a system of functions, which, in turn, reflect their interconnections through the objects of the system.

Data models are dual to functional models and are a detailed description of system objects associated with system functions. The full SADT methodology supports the creation of multiple models for a more precise description of a complex system. Data Flow Diagrams (DFDs) are the main means of functional simulation of a projected system. For the DFD image, two different notations are traditionally used: Yourdon and Gane-Sarson. In accordance with the methodology, the system model is defined as a hierarchy of data flow diagrams that describe the process of transforming information from its input into the system before being issued to the user. With these diagrams, the system is divided into functional components (processes) and presented as a network linked by data flows. The main purpose of such tools is to demonstrate how each process converts incoming data on the output, as well as to identify the interactions between these processes.

Top-level hierarchy diagrams (contextual charts) define the main processes or subsystems of the IS with external inputs and outputs. They are detailed using lower-level charts. By creating a multilevel hierarchy of diagrams, this decomposition continues until such a level of decomposition is reached, on which processes become elementary and it is impossible to further elaborate them.

When creating a data flow diagram, four basic concepts are used: data streams – abstractions used to model the transmission of information (or physical components) from one part of the system to another; processes of converting input data streams into output, the purpose of which is to produce output streams from the inputs in accordance with the action that specifies the process name; external nature (storage, storage) – is a material object outside the context of the system that is the source or data receiver and allows to specify on the specified areas data which will be stored in memory between processes; data storage (repository).

The task of the DFD set is to make the correct decomposition of the system in order to show the functioning of the system is clear and understandable at each level of detail. The process of building a model is divided into the following stages: the dismemberment of many requirements and their organization into the main functional groups; Identification of external objects with which the system should be connected; Identification of the main types of information circulating between the system and external objects; formation of the first level DFD based on the processes of the previous contextual diagram; DFD primary level requirements check. After decomposition of the main process for each subprocess, a similar table of internal events is constructed. The next step after defining a complete event table is to allocate data flows that are exchanged between processes and external entities. The easiest way to allocate them is to analyze the event tables. Events are converted into data streams from the event initiator to the requested process, and the reactions are in the reverse flow of events. After constructing input and output streams, internal flows are constructed in a similar way. For their selection for each of the internal processes are allocated suppliers and consumers of information. If the supplier or consumer of the information represents the process of storing or requesting information, then the data store for which the given process is an interface is entered. After constructing data flows, the diagram should be checked for completeness and consistency.

Entity-relationship model (ERD) are designed to develop data models and provide a standard way to identify data and interconnections between them. With ERD, the details of the data warehouses of the projected system are carried out, as well as the essence of the system and methods of their interaction, including identification of objects important for the subject

domain of objects, properties of these objects (attributes) and their interrelations with other objects are documented.

An important place in the development of automated control systems are object-oriented methodologies, based on the object object decomposition, represented in the form of a set of objects that interact with each other through the transmission of messages. Authors of well-known methodologies Booch, Rumbaugh, and Jacobson have teamed up to develop a unified methodology called Unified Modeling Language (UML). When creating UML its authors were guided by the purpose of accelerating the evolution of the most popular methodologies in the direction of converging them with each other, summarizing the accumulated experience of their use, ensuring the stability of projects based on a single holistic method.

Heuristic methods have been widely used in automated control systems, and further progress in this direction is associated with the development and implementation of expert systems. Expert systems allow you to accumulate knowledge bases about the production process, about effective management solutions, and, on this basis, offer rational solutions to tasks that are inadequately formalized. The range of economics and mathematical models and methods is extremely wide. Their application is restrained by the complication of an adequate description of the production process, the receipt of solutions in the conditions of high dimensional tasks, as well as the lack of necessary for this case, the qualifications of managerial staff.

Below are models and methods for solving private tasks of enterprise management included in basic systems such as ERP: for solving strategic planning tasks, linear programming models are used; operational planning is usually built on the basis of network models. In this case, methods are used to calculate the critical path of the PERT; for solving the problems of forecasting demand and other economic processes, methods of regression analysis, analysis of time series, procedures for processing expert assessments are used; when solving tasks of planning sales volumes and production, methods of linear programming are used; the problem of forming the schedule of output can be formulated as a task of minimizing the total production cycle with restrictions on capacities, where the variables are the terms of launch (release). In basic systems such as ERP (Enterprise Resource Planning) there are procedures that solve this

problem by generating, analyzing and screening options with simultaneous reductions in the number of variables in each iteration; the task of calculating the material needs for ensuring the timetable of output is solved on the basis of a model of disintegration, during which the calculation of the network structure describing the composition of the product. Operational production management in ERP is based on the application of priorities and heuristic methods for constructing work schedules. Normative base can be formed using statistical methods.

3.4 Concept and models of life cycle (LC) of the IS

The basis for the creation and use of software (SW) is the concept of its life cycle (LC). LC of IS – is the period of creation and use of IS, from the moment of the emergence of the need for IS and ending with the moment of its complete disengagement. LC is a model for creating and using software that reflects its different states, from the time the need arises in this software product and ending with the moment of its complete withdrawal from use among all users.

Traditionally, the following main stages of LC of software are distinguished: requirements analysis; designing; coding (programming); testing and debugging; operation and maintenance. Among the stages of the LC of IS, the following are distinguished: pre-project survey – collection of materials for design, which involves the formulation of requirements, study of the object of automation, pre-presentation of the pre-project version of the IS, as well as analysis of materials and development of documentation, during which it is required to be given technically -economic substantiation with a technical task for the design of IS; design – preliminary design, which includes the choice of design decisions on aspects of the development of IS, description of the real components of IP, design and approval of a technical project (TP), detailed design, which includes the choice or development of mathematical methods or program algorithms, adjustment of database structures, creation of documentation for the delivery and installation of software products, the choice of a set of technical equipment with documentation for its installation, the development of a technical working project of IS (TWP), as well as the development of a methodology for the implementation of functions management by means of IS and description of the operating regulations of the management apparatus; development

of IS, consisting of obtaining and installing technical and software tools, testing and proofing of software and development of instructions for the exploitation of software and hardware; the introduction of IS into operation – the introduction of technical means, the introduction of software tools, training and certification of personnel, experimental exploitation, the handing over and signing of acceptance-delivery acts; IS operation – daily operation, general maintenance of the entire project. The LC is formed in accordance with the principle of downstream design and, as a rule, is an iterative nature: the stages implemented, starting with the earliest, are cyclically repeated in accordance with changes in requirements and external conditions, the introduction of restrictions, etc. At each stage of the LC a certain set of documents and technical solutions is generated; At the same time, for each stage, the documents and decisions obtained in the previous step are initial. Each stage ends with the verification of the created documents and decisions in order to verify their compliance with the original.

The main regulatory document regulating the LC of the software is the international standard ISO/IEC 12207 (ISO – International Organization of Standardization, IEC – International Electrotechnical Commission). It defines the structure of the LC, which contains the processes, actions and tasks that must be performed during the creation of the software.

The structure of the LC of software according to the ISO/IEC 12207 standard is based on three groups of processes: the main processes of the LC of software (acquisition, supply, development, operation, maintenance); auxiliary processes that ensure implementation of the main processes (documentation, configuration management, quality assurance, verification, certification, evaluation, audit, problem solving); organizational processes (project management, project infrastructure, definition, evaluation and improvement of the LC itself, training).

The development includes all work on the creation of software and its components in accordance with the requirements. This includes the design and operational documentation, the preparation of materials necessary for testing the performance and quality of software products, materials necessary for the organization of training personnel, etc. Software development usually includes analysis, design and implementation (programming).

Operation includes work on the implementation of components of software in operation. This process includes configuration of the database and user's workplaces, maintenance of operational documentation, training of personnel, and direct operation, including localization of problems and elimination of the causes of their occurrence, software modification within the established rules, preparation of proposals for improvement, development and modernization systems.

Project management involves planning and organizing work, creating teams of developers and monitoring the timing and quality of work performed. The technical and organizational support of the project includes the selection of methods and tools for the implementation of the project, the definition of methods for describing the intermediate state of development, the development of software methods and tools testing, personnel training, etc. Project quality assurance is associated with verification, testing, and testing problems.

Verification is the process of determining whether the current state of development, achieved at this stage, meets the requirements of this stage. The check allows you to evaluate the compliance of the development parameters with the initial requirements. The test partially matches the test, which involves identifying the differences between actual and expected results and evaluating the compliance of the characteristics with the initial requirements. In the process of implementation of the project, an important place is the identification, description and control of the configuration of individual components and the whole system as a whole.

Configuration management is one of the auxiliary processes that support the core processes of the software lifecycle, first of all, the processes of development and maintenance of software. When creating complex IC projects, consisting of many components, each of which can be varieties or versions, there is a problem accounting for their links and functions, the creation of a unified structure and the development of the entire system. Configuration management allows you to organize, systematically take into account and control the introduction of software changes at all stages of the LC. Currently, the general principles and recommendations for configuring, scheduling and managing software configurations are reflected in the draft ISO 12207-2.

Each process is characterized by certain tasks and methods of their solution, the initial data obtained in the previous stage, and the results.

The results of the analysis, in particular, are functional models, information models and charts corresponding to them. The software LC is iterative: the results of the next stage often cause changes in design decisions made at earlier stages.

Existing LC models determine the order in which the stages are implemented during development, as well as the criteria for transition from stage to stage. Accordingly, cascading and spiral LC models were the most widespread.

Cascade model (70-80g.r.) – involves the transition to the next stage after the complete end of work of the previous stage.

Spiral model (86-90g.r.) – focuses on the initial stages of the LC: requirements analysis, design specifications, preliminary and detailed design. Each spiral round corresponds to a step-by-step model for creating a fragment or version of a software product, it specifies the purpose and characteristics of the project, determines its quality, the work of the next round of the spiral is planned. In this way, the details of the project are deepened and consistently specified, and as a result a valid option is selected that is to be implemented.

Experts note the following advantages of a spiral model: accumulation and reuse of software tools, models and prototypes; orientation on the development and modification of software in the process of its design; risk and cost analysis in the design process.

The main feature of the software industry is the concentration of complexity at the initial stages of the LC (analysis, design) with relatively low complexity and labor intensity of the subsequent stages. Moreover, unresolved issues and mistakes made at the stages of analysis and design, generate, at a later stage, difficult, often insoluble problems, and, ultimately, lead to the failure of the whole project. Consider these steps in more detail.

Requirements analysis is the first phase of software development, on which customer's requirements are specified, formalized and documented. In fact, at this stage, the answer is to the question: "What should the future system do?". It is here that the key to the success of the whole project lies. In the practice of creating large software systems, many examples of unsuccessful implementation of the project are known due to the incompleteness and uncertainty of the definition of system requirements.

The list of requirements for the system being developed should include: a set of conditions under which the future system is intended to be operated (hardware and software resources provided to the system; external conditions of its operation; composition of people and works related to it); description of functions performed by the system; constraints in the design process (policy deadlines for completion of individual stages, available resources, organizational procedures and measures to protect information).

The purpose of the analysis is to transform the general, fuzzy knowledge about the requirements of the future system into as accurately as possible. At this stage, the following are determined: the architecture of the system, its functions, external conditions, the distribution of functions between hardware and software; interfaces and distribution of functions between a person and a system; requirements to the software and information components of the software, necessary hardware resources, requirements to the database, physical characteristics of the components of the software, their interfaces.

The main objective of computer-integrated technologies is the creation and operation of computer-integrated control systems that provide the solution of tasks for the coordination of the functioning of subsystems, the use of intelligent subsystems of decision support on the basis of databases and knowledge and management systems.

This kind of activity requires the knowledge of special software. At the same time, computer-integrated technologies are closely linked to systems of automatic control and automation of processes in various industries and production.

REFERENCES

1. Vitkup M.E., Petrenko V.V. Informatics and computer engineering (MSOffice in examples and problems with methods of their solution): Tutorial. Київ: Центр «Методика-информ», 2002. 351 с.

2. Марк Спортак, Френк Паппас и др- Компьютерные сети и сетевые технологии. PlatinumEdition: Пер. с англ. Санкт-Питербург.: ООО «ДиаСофтЮП», 2005. 720 с.

3. Билоусько В.С., Чуждан Т.И., Антипенский В.Е. Вычислительные машины и программирование: Практикум. Київ: Вища шк. Головное изд-во, 1987. 245 с.

Information about the author:
Medvediev M. H.
Doctor of Technical Sciences, Professor,
Head at the General Engineering
and Thermal Power Engineering Department
of the V. I. Vernadsky Taurida National University
33, John McCain str., Kyiv, 02000, Ukraine

DOI https://doi.org/10.36059/978-966-397-104-9/29-51

INFORMATION TECHNOLOGIES IN ECONOMY

Medvediev M. H.

INTRODUCTION

Information technology in the economy is a virtual economy tool. The virtual economy is an environment, a special economic space in which the e-business is implemented, that is, an economy based on the use of interactive capabilities. This space is characterized by specific features that distinguish the virtual economy from the ordinary, non-virtual, offline economy. The virtual economy is often referred to as a new economy to emphasize its distinction from the old, traditional economy.

Let's consider the details of the new economy. The basis of economic activity is business. In the virtual economy, there is the concept of e-business.

An e-business is a revenue-generating company based on digital technology and the benefits that it provides. Areas of application of e-business: e-commerce; mobile trade; financial transactions; purchase and sale of an information product; buying and selling through vending machines; banking operations; buying and selling through a virtual store; household services market; insurance operations; stock market transactions; operations with foreign currency.

The concept of "e-business" includes many different information technology concepts: technology e-commerce; technology of electronic auctions; electronic banks; IP telephony; Internet telephony; electronic pointers technology; electronic research and development; electronic franchising; Email; e-marketing; electronic resource management (ORM); electronic supply management; electronic brokerage services; information technologies of acquaintances.

Let's consider more these concepts. E-Commerce Technologies. E-commerce (e-commerce) is one way of doing business with e-commerce. Considering the problems of e-commerce, one should pay attention to the double interpretation of the term. Sometimes, speaking of e-commerce, it refers solely to the commercial activities of Internet Service Providers (ISP), but much more often, e-commerce has a wider interpretation and is

seen as a set of all possible ways to use the Web for commercial purposes. Internet Service Provider is a commercial firm that provides access to the Internet by supporting it for a fee and carries out some related services on demand of customers. The term "e-commerce" combines many different technologies: EDI (Electronic Data Interchange Protocol); Email; Internet; Intranet (information exchange within the company); Extranet (sharing information with the outside world)[1].

The most advanced information technology on which electronic commerce can be based is Electronic Data Interchange (EDI), which is a method for encoding and processing sequential transactions in on-line mode. Technologies of electronic auctions. Electronic auctions are part of a new type of markets – electronic trading markets (ETM) whose purpose is to build buyers and sellers. The main means for the implementation of electronic auctions – the Internet[2].

At electronic auctions the price is not fixed. Online revenue sources, that is, electronic auctions – transaction fees and advertising. This is a very promising field of e-commerce. Many companies use electronic auctions as a marketing assessment tool that allows you to determine the primary demand and market price of a relatively new product. On the Internet auctions can be exhibited any goods that are most suitable for auction trade: computers and accessories, as well as new high-tech products for the market; reduced prices of goods; non-market goods; recent sales leaders; collectible goods.

Online auctions are categorized based on their division in the direction of growth or decline.

Bet may increase from the minimum to the maximum or, conversely, decrease from the first maximum to a certain winning minimum determined by the method.

In connection with the promise of auctioning on the Internet is now particularly popular among the various auction theories, which are becoming one of the most fashionable sections of economics.

Electronic banks. Electronic banking is carried out in two forms: services provided by electronic banks, and services provided by traditional banks, but online.

[1] Игер Б. Работа в Internet. Под ред. А. Тихонова; Пер. с англ. – Москва: БИНОМ, 1996. 313 с.

[2] Крол Эд. Все об Internet: Руководство и каталог. Пер. с англ. С.М. Тимачева. Киев: BNV, 1995. 591 с.

The basis of the emergence and development of Internet banking (Internet-banking) are the types of remote banking, the existence of banking, used at the earliest stages:

- banking – access to a bank account using a personal computer, which is carried out by means of direct dial-up connection to the banking network;
- telephone banking – account servicing by phone;
- video banking – the system of interactive communication of the client with the bank staff.

Internet banking can be defined as management of bank accounts via the Internet.

Online banks have a great future. These forecasts are due to the number of advantages that electronic banks provide to their customers. Smart Cards create the following conveniences for customers who previously seemed unattainable: round-the-clock mode of operation, uninterrupted service availability.

Internet banking involves customer service through the Internet by providing them with a wide range of services:

- open deposits;
- purchase and sale of currency and securities;
- translation;
- receiving an account statement and much more.

Customers can check the status of their accounts without leaving the office or home from any geographical point of the world and at any time of the day. Thus, there is a significant savings on the maintenance of private clients as a result of automation of this process, especially in the case of an integrated approach to the use of electronic capabilities:

- the formation of a home bank;
- creation of an electronic trading market (ETM);
- promotion of payment schemes for e-commerce, etc.

However, as long as the banking sector is concerned not with the transition to the online regime, but rather on the parallel use of traditional business practices and the opportunities provided by new information technologies. It should be borne in mind that besides purely commercial effect, electronic services in the banking sector affect the image of the bank.

Internet banking gives customers the opportunity to get a full range of services in one system: pure banking services (access to accounts, financial transactions, etc.), insurance services, corporate finance management services, etc.

IP telephony. VoIP is the most powerful communicative information technology.

In recent years, the rapid growth of data transmission systems has led to the fact that many of the usual consumer services are now provided in a new way: e-mail has replaced traditional, electronic commerce allows you to order and pay for goods without leaving the house, etc. Today, VoIP is already beginning to compete with traditional telephony operators. One of the significant advantages of VoIP is the significantly lower cost of voice traffic compared with the cost of public telephone network services. VoIP enhances the efficiency of everyday activities of companies, introducing into the telephone all that useful, which has become familiar to users of computer networks – the ability to work with e-mail messages, obtain operational data from ERP-system production applications, as well as summaries, reports and news from the Internet / Intranet.

With the introduction of integrated voice, graphics, video and data systems, it has become possible to create fundamentally new, contemporary, user-friendly applications that convert an IP phone to a fully functional office computer. Such a phone that implements a wide range of services is a small computer with a built-in XML browser for performing various XML applications. IP telephones, in addition to supporting traditional telephone functions, provide access to the corporate directory of subscribers with search and dialing capabilities. The built-in service menu allows an IP-phone user to access textual or graphical information located on Web-servers.

Operational access to the entire volume of corporate and other data through an IP phone is usually provided through the Enterprise Information Portal (EIP). An IP phone in this case is considered as a "super-thin" client. From the user's point of view, this is a unique opportunity to gather all the information that is needed for him at the moment to perform his official duties on one screen.

IP-telephony (Internet-Phone telephony) is a technology used on the Internet to transmit speech signals. When talking, voice signals (pronounced words) will be converted into compressed data packets. These

data packets are then sent to the other party over the Internet. When the data packets reach the destination, they are decoded in the voice signals of the original.

IP telephony is a way to organize a corporate telephone network, without investing significant funds in the creation of lines and reducing the cost of paying for telephone services.

There are two basic types of IP telephone calls: from computer to computer or from computer to phone.

IP telephony uses the dedicated digital channels as lines of telephone traffic transmission.

The Internet fundamentally changes our perceptions of both telephony and ways of communication. Although telephone networks and data networks have coexisted for decades, they have evolved independently of each other. IP telephony unites them into a single communication network, which offers a powerful and economical means of communication. Dozens of companies around the world offer commercial solutions for IP telephony. All major telecommunications companies have begun research to better understand emerging prospects. VoIP combines voice and data in one network and offers cheap long distance and international calls and a range of communications services to any user.

The general principle of IP telephony servers is as follows: on the one hand, the server is connected to telephone lines and can connect to any phone in the world. On the other hand, there is an Internet-based server that can connect with any computer in the world. The server accepts a standard telephone signal, digitizes it (if it is not digitized before), it compresses, breaks down into packets and sends them over the Internet using its Internet Protocol (TCP/IP).

For packets that come from the Web to the phone server and go to the telephone line, the operation is in reverse order. Both components of the operation (signal input to the telephone network and its exit from the telephone network) occur almost simultaneously.

Based on these basic operations, you can build many different configurations. Therefore, in the market of telephone services, a new category of operator-providers – ITSP (Internet Telephone Service Provider) – has been introduced, offering services for interacting Internet users with subscribers of telephone networks.

Internet-telephony. Internet telephony is a special case of IP telephony. In this system, ordinary channels of the Internet are used as transmission lines. Internet telephony is partly based on the existing network of fixed telephone lines.

The concept of voice over the network using a personal computer originated at the University of Illinois (USA) in 1993. Already a year have become quite common connections over the Internet of two telephone subscribers, located in completely different places on the planet. And for only two years, until 1995, an alternative way of telephony was developed.

Technology of electronic pointers. With the help of electronic pointers, Internet customers are able to search for products and services on the Web.

Digital RW and RDW. RW – research works is a series of research that is conducted with the aim of obtaining new knowledge, finding new ideas, principles, methods and ways of creating new or upgraded products. RDW – research and development work is a set of interconnected processes for the creation of new or modernizations of existing structures, products in accordance with the requirements of customers, the manufacture and testing of their research or master samples.

Electronic franchising – this agreement on the conditions of joint activity between the company and the dealer, according to which the dealer obtains the right to operate with the use of the trademark of the company, its know-how, marketing techniques, technologies, promotional opportunities, semi-finished products, etc., paying for this deduction of a certain Percentage of turnover or profit.

According to the New Economic Dictionary, the term "franchising" has gone from the English "franchise" – privilege. Franchising is a form of economic integration of large and small businesses, which is to give a large company (franchisor) the right to act under its trademark of a small company that is an independent legal entity. At the same time, the franchisor can give a loan, be a surety when receiving a loan. Franchising is widely used in trade, hotel business and consumer services.

Franchising can be divided into three parts:

- franchising as a form of replication of business technology (a striking example – the McDonald's network);
- e-shops (for example, Porta-shop that sells microelectronics and much more, Ozon, etc.) that use the Internet as a means of electronic

communications, in particular for the transmission and execution of orders and electronic payments;

- network forms of product promotion – network of shops, network of promoters (multi-level organizations being built to promote products and services from the manufacturer to the consumer, using a direct human contact with a person, that is, multi-level network marketing).

The active part of electronic franchising remains a person specially trained to own a computer, including Internet technologies. This specialist becomes the director of the virtual e-shop and performs the functions of the manager in the organization of information flows.

Email. The Internet has opened fundamentally new business opportunities. Computer systems have begun to be used as a medium for communication between humans since the mid-1970s. At that time, experiments on the study of the possibilities of computer communication between people on the basis of electronic information exchange systems began. Systems for transporting messages between people using computers are called e-mail systems.

E-mail is a postal service in which messages are delivered electronically via computers.

E-mail is the basis of any business. E-mail is a powerful and convenient means of communication that essentially outperforms traditional mail by speed and facsimile connection at the cost of information transfer. E-mail facilitates business negotiations.

Significant difference in e-mail from the usual is that the "local branch of communication" is very small and serves only the user's computer, it (as a personal "mailbox" for sent messages) is always "at hand" – in the computer. More details on email will be discussed further.

E-marketing. The main function of e-marketing is the study of demand, pricing issues, advertising, sales promotion, product range planning, and more. Advertising, goods, strategy, price – all depends on the needs of customers. At the moment, individual marketing on the Internet began to develop.

The development of Internet marketing is associated with the opportunities that the Internet provides to various companies:

- carrying out of advertising actions of firm, goods, services, organizational measures;
- marketing market research;

- analysis of competitors' activity, demand for products and advertising effectiveness;
- establishment of business relations with partners;
- search for new customers and partners.

The basis of any marketing company on the Internet is the corporate Web site of the company or company around which the entire marketing system is built. In order to attract visitors to their Web-server, the company should advertise it through registration in search engines, Web-directories, links to other Web sites, banners, thematic mailing lists.

Also, the effectiveness of marketing activities on the Internet is ensured by the advantages of e-mail (e-mail marketing):

- E-mail is practically available to all Internet users;
- Possibility of personifying messages and actions on the target audience;
- modern mail clients support the html-format of letters, which allows you to place not only text ads, but also graphic ads in the letters.

Electronic Operational Resources Management (ORM). ORM carries out advertising, sale, delivery of non-manufactured goods.

Electronic Supply Management. Electronic supply management delivers offers, goods, services, information on the Web.

Electronic brokerage services. Electronic brokerage services – services in the securities market, providing a sales agreement between a potential seller and buyer.

The Internet provides new opportunities for brokerage activities. Big banks, equity houses and investment firms are actively involved in the online brokerage market, with the volume of such services becoming more and more extensive. Brokers also compete by providing customers with bank accounts and money market services online.

The volume of electronic brokerage operations is directly related to the possibility of access to the Internet, which, in turn, depends on many factors and, above all, on the level of income per capita.

1. CRM-care for the consumer

Over the past few years, we are experiencing a real boom in customer relationship management (CRM). This concept today has become an important tool in the hands of a businessman or owner of his own business, who cares about the future of his company. The concept

itself is simple – instead of caring for consumers, caring for the Consumer. Moreover, about each of them, individually. The collected and processed customer information (history of purchases, tastes, needs and preferences) is used to more precisely specify the offers of a particular client, which he will accept with a high degree of probability. Naturally, in the presence of an ever-increasing number of "benevolent" clients, this approach can only be realized on the basis of the use of modern information technologies. In traditional marketing oriented consumerism, which implements the classical formula "product – positioning – promotion – value / price", there is no need for interaction with a particular buyer, the differentiation of specific groups of consumers, the identification of the individual needs of customers. It could be argued that for the concept of CRM, the introduction of new technologies is not mandatory. Here are examples that show the opposite.

The implementation of the CRM-concept should involve the majority of corporate services and departments – marketing, production planning, customer support, territorial sales divisions and service services. Contacts with the client should be carried out continuously in a direct or indirect form. A special notion of "Point of Contact" ("Point of Contact") has been introduced in the CRM concept to illustrate ways of engaging with the client.

Customer Relationship Management System – the target corporate information CRM system or subsystem included in the ERP system is designed to improve customer service by maintaining customer information, customer relationship history, establishment and improvement of business procedures on the basis of stored information and subsequent assess their effectiveness.

The basic principles of building a CRM system are the following:

- having one repository of information that contains all available information about all cases of customer interaction;
- synchronization of control of interaction channels;
- collection and continuous analysis of customer information.

Thus, this approach implies that with any interaction with the client through any channel, the employee of the organization is available full information about all customer relationships and the decision is made on its basis, information about which, in turn, is also stored and is available for all future interactions.

Table 1

Comparison of different marketing approaches

Concept	Identification	Differentiation	Interaction	Personalization
Goal	Customer identification	Assessment of the client and his needs	Creating long-term relationships	Realization of client's needs
Traditional marketing	Unrealizable	Cluster differentiation	Telephone Call center	Sales / services
CRM concept	Profiling a customer's identity	Analysis of the personal level	Automated Call Center	Sales and marketing automation
Technological solutions	Cookies and personalization of the Web client profile	Intelligence and analytics	Internet applications and WAP telephony	ERP and e-commerce

Classify the capabilities (modules) of the CRM system by functionality and levels of information processing.

Functionality can be grouped into process blocks: marketing, processing requests and wishes, sales, service.

Call-centers – inbound call processing centers (originally telephone calls, most recently all channels of communication) are usually distinguished as separate components.

Classification by information processing functions:

- operational function – registration and immediate access to primary information on the sections of the database: Events, Companies, Projects, Contacts, Documents, etc.;
- analytical function – reporting on primary data and, most importantly, in-depth analysis of information in different sections (sales funnel, analysis of results of marketing activities, analysis of sales performance in the context of products, customer segments, regions, etc.);
- cooperative function – organization of close interaction with end consumers and customers up to the influence of the client on the internal processes of the company (surveys to change the quality of the product or the order of service, Web-pages for tracking customers of the order status, SMS notification about the conducted transactions in a bank account, an opportunity for customer to independently assemble and order in real time, for example, a car or a computer with available blocks and options, etc.).

Prior to 1993, the CRM market consisted of two main areas – Sales Force Automation (SFA) and Customer Service (CS). The primary purpose of automated territorial sales management systems was to allow sales reps to manage their customers' "points of contact" and to work with a sales plan agreed with the calendar. Over time, such systems have been enriched by the introduction of a feature management capability, which in practice has meant maintaining the tactics and methodology of sales adopted within the company, as well as being able to communicate with other units of the company, such as customer support or customer service.

Until the year 2000, CRM systems were usually "one-sided" – the so-called "contact managers", marketing support systems, or service automation systems.

The period from 2000 to 2005 is connected with the first wave of formation of joint business of companies with consumers – joint commerce (Collaborative Commerce). It is characterized by the establishment of interactive interaction of companies with their regular partners through the Internet.

Such interaction implies giving outsiders much greater access to corporate information and should therefore be based on the principles of safeguarding and trust in the partner, as well as agreed rules of operation.

2005–2007 is the time of the second wave of Collaborative Commerce, based on the even greater openness of ERP systems. Leading manufacturers have started creating interfaces for their user-friendly ERP systems, B2C e-commerce platforms have emerged, and new business infrastructure is being formed (for example, on the basis of corporate Web services in the .Net architecture). In this case, unlike the first wave, it is a matter of many-to-many interactions, that is, enterprises will cooperate not only with permanent partners, but also with all members of the business community.

Almost all modern CRM systems have more or less received the above capabilities and levels of information processing and presentation: data processing and storage in collective repositories, development of knowledge bases, Internet-based solutions for interactive interaction with the client through corporate portals, etc. An example is the Corporate Portal module of Axapta (Microsoft Business Solutions) software.

MS Axapta is a scalable system for medium to large enterprises, corporations and holding companies, providing a single integrated solution

aimed at improving manageability and business optimization. Axapta is a powerful technology platform: its modules are open source, include integrated development environment (Morph X) and its own object-oriented programming language (X ++), optimized for writing business applications. These tools can both modify your existing business logic and build new features.

This multifunctional ERP solution covers the business of the company as a whole, including manufacturing and distribution, supply chain management (SCM) and projects, financial management and business analysis tools, customer relationship management (CRM) and personnel management. The powerful functionality of the system greatly reduces the time and cost of creating, deploying and operating the solution.

1.1 Concept functionality

According to the classification of the Center for the Study of Information Technology and Organizations of the University of California, CRM systems may include the following set of functions:

- contact management – support for customer information and contact history, may include information on points of sale or periodic replenishment of customer inventory with their products;
- activity management – provides a calendar and business diary for sales representatives working in the field;
- communication management – is expressed in a standalone software module that is responsible for transmitting information using a modem or mobile phone, storing and replicating it;
- forecasting – provides information on prospective sales plans, as well as forecasts of research organizations or marketing research data of company divisions;
- Opportunity Management – Managing motivating factors for attracting leads;
- order management – obtaining information about the availability of goods in the warehouse and placing orders for the delivery or production of products online;
- documentation management – development and implementation of customizable standards and reports and promotional material;
- sales analysis – providing analytical capabilities to sales databases;

- product configuration – storage of information about alternative products and their price characteristics;
- Encyclopedia of Marketing – Provides up-to-date information on products, prices, promotional activities, research findings (e.g., factors that influence purchasing decisions) and competitors.

Customer service acts as a factor in the after-sales relationship with the customer. Its purpose is the fast and effective solution of external and internal problems of the client.

By providing fast and accurate scenarios for solving customer problems, the company can save costs and increase the customer's sense of satisfaction and loyalty to the chosen supplier and, as a consequence, their revenue.

The following management subsystems are used to specify the directions of customer service of the CRM-system:

a) management of the customer service center: provides automated processing of the received request; collects, summarizes, analyzes customer feedback to evaluate performance, quality control and product improvement;

б) field service management: distributes, appoints and controls people with the appropriate skills and materials to serve the customer's needs; records materials, costs and time associated with customer service; provides a history of client relationships; offers valid and proven solutions by building and maintaining a knowledge base; c) management of current (Hot Line) support: solves problems by searching in the existing knowledge base; compiles, processes and maintains a problem report; informs customers about updates, new additions and models appearing in the company assortment.

Modern CRM systems integrate all the tools related to customer contact and are supported by information technologies: territorial sales management system; customer support system; marketing and sales management system; contacts and activity management.

1.2 The main components of CRM-systems

Software solutions aimed at improving management processes in the implementation of the CRM concept, as a rule, include the following modules: interacting CRM subsystems of individual territorial units of a distributed company; analytical and marketing software modules; electronic directories and management; an online ordering system with relevant Web services, online invoicing and the ability to pay by credit card or e-wallet.

Since these software solutions, which are embedded in the ERP-system and continue it in the external environment, are quite complex, there are quite natural questions: "How effective is the system?", "Is the big return on a complex and expensive information system?", "What about her time, effort and money?" It can be pointed out again that the focus of the CRM concept is the consumer. The fight for the client is the essence of the market, and it will continue as long as there are market relationships. In terms of economic benefits, it is much cheaper to maintain a relationship with a regular buyer than to find a few new ones: according to the Pareto principle and based on the processing of client orders and requests, it can be shown that about 80% of the company's revenue is provided by 20% of its regular customers; sales of manufactured goods require, on average, more than ten indirect (advertising) hits to new leads to sell a unit of goods, and only 2-3 direct hits to existing loyal customers; a 5% increase in the number of repeat customers is expressed in total by more than 25% increase in sales; making an agreement with an existing customer is easier and cheaper than reaching the same agreement with a new buyer; the average customer, frustrated at their supplier, tells about his adventures to ten acquaintances.

One of the main problems in creating and maintaining such a system of relationships is the task of maintaining the integrity and security of customer information. A company that seeks to engage with the customer more effectively while collecting the maximum amount of information about the client should take care of the non-disclosure of this information (Client Information Privacy).

The issue of collecting private information is not as simple as it might seem at first glance. There is still no consensus as to what information can be used for business purposes and which information is inadmissible, even if the client has provided it. The basic procedures that a company must implement to protect private client information include: notifying the client of the purpose of collecting information about him and its further use; the refusal of the client to establish a relationship of this nature does not mean a decrease in its value to the company in the case of long and fruitful relationship with him; an opportunity for the client to view information about him and to correct information that is not related to the internal procedures of the company (rating system, comments of contact persons, etc.); real protection against access by third parties to private information.

Measures taken to protect private information about a customer increase the level of trust between the company and its clientele.

The CRM implementation process takes a long time on the part of the Information Technology Department. Indeed, CRM implementation is a continuous process, so IT staff must work closely with business units (planning, marketing, ordering, sales, delivery), be prepared for ongoing system support, and direct their efforts to ensure the smooth running of software applications and data structures.

Table 2

Types of CRM products

CRM product format	Cost	Disadvantages	Benefits	User profile
Box solutions	$200 – $400 per workplace	Weak integration with other applications, low customi-zability, finishing writing	Low cost; ease of implementation and learning	Small business company. Number of managers no more than 5-10, small amount of information, no need to connect to other systems
Integrated solution	$600 – $2000 per workplace	Thinly represented in the market	Integration into the entire IT structure of the company, powerful functionality; flexible setup for business processes	Medium Business Company. Number of managers 10-500, large flows of customer information, one of the requirements is the integration of the IT structure
Module in ERP-system	from $2000 and above	High cost and timing of implementation of the CRM module	No need to integrate with other applications; initially a single information environment for all business units	Large manufacturing companies and holdings. The number of managers is thousands. Requires automation of all processes, trans-parency of the whole enterprise as a whole.

When purchasing a ready-made solution, you should always consider which software of the class will provide the most rational "continuation" of the existing ERP-system in the client environment.

Investing in CRM is an investment in a long-term relationship with your customers and, therefore, the process of reimbursement of the investment will depend on how effective the supplier-client relationship model you create. It should be understood that CRM is not a cheap, easy and fast, but always promising solution.

1.3 Enterprise Resource Planning, synchronized with customer requirements and expectations

Today, the globalization of the economy, the erasure of national borders, the free movement of goods, the increasing competition, the emergence of legislative foundations in the field of product quality have led to the emergence of new requirements to meet demand and the realization of the required quality. The business is facing fundamentally new questions: "On what criteria will a buyer base his purchase decision?"; "What can be done to reduce the unproductive costs of today's competition?".

The competition formula has led manufacturers over the past decade to first and foremost focus on improving product quality and reducing its value. In the 1990s, fierce competition was concentrated around production in a short supply and just in time (JIT), and its intensification forced manufacturers to seek solutions to improve and accelerate the production process. They directed their resources to improve production efficiency, tried to produce products better, cheaper and faster.

Many changes have taken place. To adequately answer the question "Do you know the buyer?" and "Do you know exactly what the buyer wants?" requires careful consideration of the buyers – their needs and benefits. The most successful manufacturers of the last decade of the last century have found that information about a particular buyer and the realities of the market is not easy to bring together and not easy to use to increase business efficiency. The main difficulty, as it turned out, was that production efficiency could be determined, modeled, measured and achieved, and market trends were so complex and dynamic that they were difficult to measure and even more difficult to adequately predict. Production efficiency has been the result of the theory, practice and

experience of business management over the last decade. The fastest and most predictable way to improve production performance is to increase the value of the product to the consumer (new science, new technical solutions) and reduce the value of the product by reducing costs or transforming production (using new resource-saving and information technologies) to create new product value[3].

Experience has shown that production efficiency can provide short-term benefits, but in the long run, production methods and technologies can be quickly picked up and repeated by competitors. Improved production, the widespread use of technology and more efficient business organization practices make any technological advantage a temporary factor in competitiveness. The essence of competition has changed due to the growth of business dynamics – production efficiency no longer determines long-term success in the market. But the goal remains the same – to attract new and retain a contingent of interested buyers.

The selection criterion has changed, the previously effective factors – price and quality – no longer determine the choice. The buyer is not just looking for a product – he is looking for a product that meets a specific set of requirements at a particular time. New tools are needed to meet the changed requirements. As a result, a new business model has emerged – Customer Synchronized Resources Planning (CSRP), which largely defines the enterprise's efforts to create a specific product needed "here and now" by a particular consumer. New relationships have emerged: a focus on the customer, not the product.

The use of ERP-systems becomes a standard approach to improving the enterprise management system. Manufacturers hoping to succeed in the growing competition in the market should actively use ERP simply to match competitors' production performance.

More and more manufacturers are introducing MRP/ERP class management systems, but as stated above, they are no longer providing pure and lasting competitive advantage. Production efficiency is always an important factor in competitiveness, but it is clearly not enough now.

The use of ERP is always focused on virtually internal processes. ERP technologies optimize enterprise management, order reception, production planning, purchase of raw materials and components, production,

[3] Крайников А.В., Курдиков В.А., Лебедев А.Н. и др- Вероятностные методы в вычислительной технике: Учеб. пособие для вузов по спец. ЭВМ.; Под ред. А.Н. Лебедева и Е.А. Чернявского. Москва: Высш. шк., 1986. 312 с.

delivery – that is, in most cases, internal operations. But if competitive advantage is already determined by the dynamic creation and delivery of purchasing value, then the current ERP model is not enough. Manufacturers should extend the game rules to include a new player – buyer – throughout the product life cycle.

Three key business questions are: "What products will the buyer require in the near future?", "Which product improvement will create competitive advantages?" and "If the fashion, tastes, and preferences of shoppers are changing at an ever-increasing rate, how can you get critical information about the market?" require increasingly effective consumer engagement technologies.

The answer is simple – integrate customer requirements and expectations with your business planning and real-time business support system.

Now the most powerful production management tools are built on the basis of the ERP kernel, but necessarily focus on integration with customers.

The system of effective production planning has two focuses – on production efficiency and on the creation of new purchasing value. This value is created through a CSRP methodology that includes a complete lifecycle – from defining the required functionality and designing a future product to meet customer requirements, to after-sales warranty and after-sales service. This new scheduling paradigm is CSRP's "synchronized resource planning".

The CSRP methodology utilizes the proven, integrated functionality of ERP systems and redirects production planning from production to customer. CSRP provides effective methods and applications for creating value-added products for the buyer. All this amounts to CSRP technology.

To implement the technology, it is necessary to: optimize production activities (operations) by building an efficient ERP-based production infrastructure; integrate buyer and customer-focused organizational units with major planning and production units; implement open technology to create a technology infrastructure that can support the integration of customers, suppliers and production management applications.

The first step in CSRP is to achieve production efficiency through the introduction of production planning technology that takes into account consumer preferences. This is especially important in areas where fashion and consumer tastes, as well as the advancement of science and the rapid

development of technology, dictate the need for frequent changes in models and product nomenclature. Examples are the automotive industry, microelectronics, communications systems, software development, advances in nanotechnology, etc. Why not abandon the practice of using standardized ERP for other, new business practices? There are two reasons.

The first reason. ERP-based production management approaches are working – and in a number of industries, they work well. Enterprise Resource Planning is a proven methodology that utilizes a robust set of application tools that has been successfully applied in the last two decades. ERP works because it links the execution of basic operations to business logic and provides a consistent set of policies and procedures. Order processing is linked to production planning, and scheduled needs are automatically transferred to the procurement process and back. The cost of production and financial accounting are automatically changed, and critical information about operations, profitability, results of operations of units and so on become available in real time. A systematic, measurable methodology is established. Following the implementation of such a business methodology, the process of improving it can be determined, executed and repeated on a predictable basis. *The second reason*. An ERP-based approach is action-based. The activity of the enterprise is determined by the production process. This is a good starting point for combining customer activity. This is especially true if the manufacturer has ERP applications and processes that are focused on custom production techniques. An enterprise unable to manage customer orders has a small number of orders at a time, and they are not too different. This is critical if, with the help of CSRP, we hope to provide products that meet the customer's needs and are cost effective.

The synchronization of the requests and interests of the buyer and the departments of the customer-oriented organization with the company's executive and planning center provides the ability to identify favorable opportunities for creating differences that support competition.

The requirement to flexibly adjust production by adding real-time customer requirements to day-to-day planning and production forces business executives to pay attention not only to how critical product and market factors are to be taken into account, but to whom to do it. CSRP redefines business practices by focusing on market activity and changes in demand rather than production activity, which is planned a month or more ago.

At the same time business processes are synchronized not only with the requirements but also with the expectations of the customers. Manufacturers that focus on customer engagement, not just production, can create benefits by developing a systematic approach to evaluation: what products to do; what services to offer; what new markets to target.

CSRP is a business methodology that moves that part of a customer-focused business to the center of a business management system. The CSRP concept establishes a methodology for doing business based on current customer information (requirements) and projected activity (expectations). CSRP shifts the enterprise focus from planning from production to planning from customer orders. Customer information and services produced are integrated into the organization's information framework.

Production planning activities are not just expanding, but are being reorganized to include customer requests transmitted from customer-focused units of the organization. For example, the order processing process is overridden. Order processing is expanding, and instead of a simple order entry feature, marketing and sales functions are integrated. The process of "ordering" now does not begin with your own order – it begins with the prospects of sale:

- Sales managers do not form overall orders. They, together with buyers and in their workplace, formulate orders, identifying the needs of the buyer, which are dynamically translated into specific requirements for the products and their production at the moment. Order Configuration Technology allows you to test their suitability for completion before they are placed.
- Order processing is expanding to include prospect information. Working contact management systems integrate with the order creation and production planning process to provide information about the resources needed before the order is placed. Market trends, product demand and information about competitors' offers are linked to key business processes of the company.
- Static pricing models are being replaced by a target pricing tool that allows you to determine the value of each product for each buyer, as needed. The accuracy and profitability of the products are increasing.

CSRP technology redefines customer service and extends beyond ordinary telephone support and invoicing. When using the CSRP model, the policy of selling products and services to meet general and specific

purchasing preferences becomes the core policy of the enterprise. The Customer Support Center is responsible for bringing critical customer information to the organization's executive centers. In the general case, the interaction algorithm below is valid.

- Customer support applications integrate with key planning, production, and management applications. Critical information about buyers and goods is delivered in advance to the units responsible for production, sales, research and development, as well as to other units.
- Modern technologies for developing targeted Web services are expanding customer support, including remote, round-the-clock, self-configuring, a help and consultation system that operates through a corporate portal. The associated execution systems automatically integrate and account for requests, increasing the ability to provide buyers with faster answers to requests and services.
- Sales Centers also become Customer Support Centers with ongoing feedback.

Integration of planning with order processing, sales and management provides the knowledge and infrastructure to transform customer support into effective sales activities, providing a channel to promote new and related products and services.

The CSRP methodology provides effective methods and tools for creating customized products. The main mechanisms behind this technological solution are the presence of a module called Product Configurator and advanced adjustable production schedule management at limited capacity and time intervals (Advanced Planning and Scheduling – APS).

The configurator includes not only business logic and rules of order specifications formation, but also equipment composition and possible technological routes depending on different conditions. All operations are provided with several variants of time and cost of reconfiguring the equipment and its own execution, depending on the formation of a certain technological route. The data is prepared by managers of the appropriate level and is entered into the system when it is set up. It is possible to trace not only linear relations of type "if, then", but also more complex relations and logical relationships, which are calculated using the apparatus of statistical and approximating functions.

The configurator allows you to quickly and accurately estimate the cost of an order for a specific product for a particular consumer, and taking

into account not only the individual options, but also the features of the technological process specially designed to fulfill this order. It is important that the module allows the product to be put into production immediately after completion of the configuration process, specification and price agreement with the customer.

The requesting sales manager may not be aware of all the technological relationships between production procedures, materials, and components used in the order configuration. However, it is within his competence to accept the order as soon as possible and to estimate its real cost.

The implementation of the customer's original configuration requires the ability to control production technology much more flexibly than before. In particular, the implementation of the CSRP approach requires the transition to the creation and modification of production plans immediately after the formation of each new specification. This approach cannot be implemented using the MRP/ERP systems standard (as already stated, this methodology is based on mandatory multi-stage planning – and layering plans are difficult to change because they are tied with all production and resource support processes).

To implement instantaneous modification of production plans in the CSRP methodology, the product configurator is directly linked to the Advanced Planning and Dispatcher Management (ASP) module, which uses a fundamentally new "math" to calculate and optimize production schedules and optimize equipment utilization. Unlike the MRPII-based methodology, in which the calculation of agreed production schedules is performed in off-line mode, the CSRP methodology based on the configurator and ASP module allows to calculate several variants of the on-line production schedule at the time of order acceptance with an estimate of possible costs for specific resources and re-equipment.

Thus, the planning of production and all activities is redefined and becomes the planning of customer orders for the organization of dynamic production.

The success of CSRP is to improve the quality of goods, reduce delivery times, increase the value of products for the buyer, etc. The result is a reduction in production costs, the creation of an infrastructure that is tailored to create products that meet the needs of the buyer, improve customer feedback and provide better customer service.

A prime example is a computer sales company that offers buyers to configure their own computer system at will. After that, delivery to any specified place is made within 24 hours. Another example is the layout of a car, a yacht, an airplane from a set of components, which can be found in the catalogs of companies and on-line to form an order. The automated system calculates the necessary moment and at the right time will submit the necessary part to the assembly line.

When using the CSRP business model, traditional business processes are reviewed to serve customers and create products that meet their needs. Implementing CSRP applications pushes business leaders to change. The internal focus of traditional production structures, segmented by departments and functionality, shifts to the consumer. It is not a traditionally evaluated production efficiency that provides temporary competitive advantage; rather, it is the ability to create products that meet the customer's current needs and better service. The ability to create instantaneous purchasing value by shifting the focus from planned impersonal production to the satisfaction of a particular consumer leads to an increase in sustainable competitive advantage.

REFERENCES

1. Игер Б. Работа в Internet. Под ред. А. Тихонова; Пер. с англ. Москва: БИНОМ, 1996. 313 с.

2. Крол Эд. Все об Internet: Руководство и каталог. Пер. с англ. С.М. Тимачева. Киев: BNV, 1995. 591 с.

3. Крайников А.В., Курдиков В.А., Лебедев А.Н. и др. Вероятностные методы в вычислительной технике: Учеб. пособие для вузов по спец. ЭВМ.; Под ред. А.Н. Лебедева и Е.А. Чернявского. Москва: Высш. шк., 1986. 312 с.

Information about the author:
Medvediev M. H.
Doctor of Technical Sciences, Professor,
Head at the General Engineering
and Thermal Power Engineering Department
of the V. I. Vernadsky Taurida National University
33, John McCain str., Kyiv, 02000, Ukraine

DOI https://doi.org/10.36059/978-966-397-104-9/52-74

USE OF OPEN TECHNOLOGIES

Kyselov V. B.

INTRODUCTION

The presence of modern open technologies and thirty years of experience in the development of complex information systems make CSRP projects feasible and practical. Manufacturing, management, sales, customer service, maintenance, and other customer-oriented, business functions can be performed by appropriate units using software specifically designed for these units.

CSRP software applications can provide and retrieve business-critical information from a central ERP-based system used by other organizational units. Software solutions from IBM, Microsoft, Oracle, SAP, PeopleSoft and other software vendors, based on a modern computing architecture that utilizes powerful Intel multi-core processors, allow you to create integrated flexible infrastructures for the needs of specific enterprises for Business On Demand implementation.

The following is a list, including some manufacturers of modern CRM and CSRP systems:

- Applix Inc. – http://www.applix.com;
- Interact Commerce Corporation – http://www.saleslogix.com;
- Nortel Networks – http://www.nortelnetworks.com;
- Oncontact Software – http://www.oncontact.com;
- ONYX Software – http://www.onyx.com;
- PeopleSoft Inc. – http://www.peoplesoft.com;
- Pivotal Corporation – http://www.pivotal.com;
- Point InformationSystems – http://www.pointinfo.com;
- Remedy Corporation – http://www.remedy.com;
- SAP AG – http://www.sap.com;
- Siebel System, Inc. – http://www.siebel.com;
- Staffware – http://www.staffware.com;
- Software AG – http://www.update – marketing.com;
- Worldtrak Corporation – http://www.worldtrak.com;
- YOUcentric, Inc. – http://www.youcentric.com.

The dynamics of modern business, the growing supply of markets and the "discernment" of consumers have led the management of companies to understand the need to increase the consumer value of the product at the expense of a significant reduction in non-production costs. In addition, as experience in mathematical modeling of production processes, the real reserve for reducing total costs is the optimal organization of movement of raw materials and components for processing and assembly.

In this regard, traditional logistics and management operations for ordering, delivery, warehousing, production release (inventory management), supplemented by the requirements of technology "Order In Time" and "Kanban" at the heart of the Just In Time methodology.

Production and registration cards of the orders of "Kanban" absolutely accurately stipulate and offer quantity of the ordered completing products on the assembly ladder, the point of the production cycle at which these products are needed and the point of time to which the products should be delivered.

The implementation of the "Just in Time" technology is focused on the following key points: accurate planning of the required volume of inventory; achieving the optimum level of inventories at all production sites; reduction or complete elimination of downtime; reduction in batch size (purchase or production) of products and increased batch maneuverability; reduction of time of transfer, processing, delivery of production; minimizing warehouse space and operations.

When implementing this technology, it is necessary to anticipate the irregularity of deliveries due to the fault of suppliers, the possibility of equipment breakage, changes in staff composition, etc. To do this, the production process includes: detailed inspection and maintenance of machines and equipment; interchangeability of workers – workers must be able to work in several workplaces and perform several production operations; Requirements for Suppliers of Guaranteed Supplies, Requirements for Defective Supplies and Fees; use of simple and clear accounting systems (so-called "kanban cards").

These technologies were developed in the mid 80's and were applied mainly in compact enterprises with a clear technological cycle. Automation of production cycle management on the basis of MRP / ERP systems has filled the technology "Just in time" with new content and allowed to apply it to distributed enterprises of a wide range of activities. The process of

automated management of complex logistics processes based on mathematical models describing the interaction algorithms of external and internal suppliers, schemes and trajectories of the movement of material values, called Supply Chain Management.

The information systems by which management is performed have become known as SCM systems. Supplies that are "tied" into complex chains should not only increase the cost at the chain nodes, but add real value at each stage of the movement. In this regard, the SCM strategy is bidirectional – it covers both the supply of raw materials and components to the enterprise, and the delivery of the finished product "Just In Time" to the market.

There are seven basic principles of the SCM concept:

- monitor market demand closely and plan based on them;
- observe the spatio-temporal distribution of sales and segment consumers based on the need for goods and services;
- equally target the logistics network to the supplier and the customer;
- strategically plan deliveries;
- to develop strategy of chains of movement of material resources;
- actively use methods of attracting new distribution channels;
- use linear programming, mathematical modeling and information technology to increase forecasting accuracy and develop network delivery schedules and optimal traffic routes.

SCM systems, as well as CRM and CSRP systems, "extend" the standard enterprise ERP system into the external environment, forming, in the aggregate, an expanded ERP II enterprise management system. This integrated system makes it possible to implement the baseline of the SCM strategy: "deliver the right product – at the right place – exactly in time – at low cost – with the right customer service." Technological and software SCM solutions are very diverse, but the most in demand nowadays are complex solutions, built on the principle of open systems for interfacing with the standard ERP-core. For example, consider the following solution implemented by Lowson Software on the IBM System platform.

This solution includes the following specialized modules:

- Supply Chain Planner – SCP;
- Demand Planner – DMP;
- Multi-Site Planner – MSP;

- Yield Optimizer – YOP;
- Advanced Production Planner – APP.

Some of the modules are embedded because they implement direct-to-many (many-to-many) operations of goods and resources to different user groups.

Microsoft Dynamics NAV Supply Chain Management System (formerly Axapta) is a suite of integrated applications including warehouse management, distribution, manufacturing, automated data acquisition (ADCS), and has pricing and e-commerce. The main characteristics of the solution:

- a comprehensive approach to supply chain management – integration of distribution and production units, automated data collection, pricing and e-commerce functionality;
- optimization and improvement of warehouse logistics and all warehouse processes;
- support for discrete production – volume-scheduling and production forecasting, flexible definition of production policy;
- modeling of effective business processes and various parameters of production process;
- increased profitability through cost reduction and effective collaboration with partners, including through the Internet.

Effective supply chain management allows you to increase revenue by maintaining inventory levels at the level you need to meet demand, resulting in increased sales, reducing the need for inventory reductions. This also leads to lower transportation costs, storage of goods, additional labor costs through optimal planning of operating facilities and inventories.

Proper supply management is, first and foremost, a cost savings, which means that you can make additional investments from the turnover of the company itself. SCM systems help to reduce the amount of working capital "frozen" in inventory, while improving the level of service provided.

Supply and demand forecasting and supply chain planning tools provide the really necessary level of inventory, taking into account the cost and effective collaboration with partners, including through the Internet.

Effective supply chain management allows you to increase revenue by maintaining inventory levels at the level you need to meet demand, resulting in increased sales, reducing the need for inventory reductions.

This also leads to lower transportation costs, storage of goods, additional labor costs through optimal planning of operating facilities and inventories.

Demand forecasting and supply chain planning tools provide the really necessary level of inventory, take into account the availability of slow and fast rotating goods, justify advertising activity, seasonal increase / decrease in demand, calculate optimal delivery times, etc. And finally, they make better use of the assets of manufacturing enterprises, as well as retail and network marketing companies through the optimal planning and placement of goods in the available warehouse and store space.

Globalization and internationalization of the economy, fast-growing business dynamics, fierce competition and the struggle for raw materials have increasingly led to situations where, in times of scarcity, only the right business decision is needed. To do this, the manager needs to analyze the situation, formulate Decision Tree, assess risks, and take responsibility for making and implementing the decision in a very short time.

To do all this using only the "hand" tools or Decision Support System modules built into standard ERP systems was quite difficult, and as a result, the risk of making the wrong decision was high. In this regard, formalized decision-making methods under uncertainty, which are described by fuzzy logic, began to develop, and specialized information systems were created using the theory and methods of artificial intelligence.

1. Systems of teamwork

The intensive development of computer and communication technologies opens up fundamentally new opportunities for the construction and development of information systems to solve management problems in large, territorially distributed and virtual organizations.

The development vector shifts towards the creation of Informational Multimedia Networks – IMN. A prerequisite for building such a network is a single technology solution for all applications running on this network, and the use of open standards and specifications – that is, you must make extensive use of open systems technology. These are, first of all, H.120, H.261, H.263 audio and video compression standards, H.320, H.323, H.324 multi-protocol standards, operating on both IP and ISDN networks, as well as widely used today is the H.264 video stream compression standard.

The ITU-T and ISO / IECMoving Picture Experts Group (MPEG) created the MJPEG standard for compression of a separate graphic image, then MPEG-1 and MPEG-2. These standards were broadband-oriented and were used mainly in digital television and for interactive video applications, without intersecting with video conferencing. But with the start of work on MPEG-4, working groups have joined forces. As a result, the H.264 standard, also known as MPEG-4 Part 10 or AVC (Advanced Video Coding), is now used by most video conferencing equipment (VCS) companies.

Groupware is a generic term for information systems (subsystems) that enable a group of people to implement Joint Actoins. For example, prepare and make decisions, peer-review new ideas, manage business units, processes, projects and staff, create software for computers, write project implementation reports, interact with the external environment (government, social organizations, suppliers, partners, customers, competitors).

Much of Groupware arose from the development of messaging tools (the first such tool was a product called PLATO Group Notes, which appeared in 1976). Such systems, usually implemented in local or distributed networks, form Integrated Collaborative Environments – ICE and are intended not only for collaboration, but also for the acquisition and formation of knowledge. In this case, they are defined by the term "Computer Aided Network Groupware". They can also be seen as an evolving technology that studies the impact of computer and communication technologies on the behavior and performance of a group, as well as the implementation processes of complex software and information systems. This discipline is based on computer science, psychology, sociology, management information systems and more. With the development of this technology, many synonyms for the term "computer networking tools" have emerged.

Commonly used in the literature are the terms "computer-based collaboration", "shared software", "team work software", "technology support for workgroup activity", "collective decision support systems", "collective automated work", "collaborative automated work", "computer-assisted communication", "flexible interactive technologies for teamwork", and even an "advanced knowledge workshop". In principle, all this means

the availability of software and hardware that implements the electronic space in which:

- collecting and processing information necessary for decision-making;
- management of teams and production of projects;
- formation and reproduction of knowledge – from finding the necessary sources to discussing results and publishing works.

Shared-use software allows a team of employees to take joint actions to accomplish tasks, use shared data and information, and improve corporate communication decision-making.

The software is classified according to the functions performed:

- to support decision making;
- to ensure the process of using general information and generating knowledge;
- to manage collaborative processes;
- to manage communications.

Doug Engelbart, one of the founders of the theory and methods of teamwork, predicted in the 1960s that computers would be able to expand the boundaries of human intelligence in the near future "due to the complexity of software systems and collaboration based on and beyond using new technologies. " His Augmented Knowledge Workshop worked on some fundamental issues that proved to be very important to understanding the implementation of computer collaboration support systems. These include the Dialog Mapping Ware technique, teleconferences, co-creation of electronic documentation, advanced planning, shared databases, organizing contacts between managers and contractors using multimedia tools. Not without the influence of his ideas, in the 1970s, two of the most widely used components of shared software appeared – email and teleconferencing.

In the 80's, the basic terms and ideas in the field of computer-based collaboration appeared and came into constant use: collective software, collective decision support systems, computer-based collaboration, teleconferences.

Currently, group support systems and electronic meeting organization systems are considered to be the most important components of decision support and enterprise management systems.

It is hard to imagine a successful company that does not take advantage of the benefits of modern IT. Such technologies, of course, should include those without which it is impossible to organize effective work – technology and systems of team (group) work. The realities of today's business are that the decision-making paradigm has changed – a system of group and distributed work, where middle-level managers are able to receive and analyze any information they need in their workplace, wherever they may be, allow them to delegate some of the decision-making authority middle management solutions. It follows that to implement this paradigm, it is necessary to develop and implement appropriate elements of the information infrastructure at the corporate level.

The actual practice of companies shows that the IT infrastructure of an enterprise, which by its nature belongs to the security subsystems, has a significant, and in some cases, decisive impact on the activities of the company as a whole, as well as on individual business decisions and operations. In particular, successful or unsuccessful implementation of business decisions directly depends on how fully, qualitatively and timely they are backed by adequate information, which is the result of teamwork and managers, IT specialists, analysts.

The activities to be provided with the relevant IT infrastructure are quite diverse. In the general case, there are:

- managing the activities of a large, geographically distributed or virtual company;
- managing complex projects, some of which are outsourced or subcontracted;
- coordination with suppliers and partners;
- managing the portfolio of investments in OnLine mode, participation in electronic stock exchanges;
- knowledge management and distance learning of company employees;
- remote control and management of equipment and technological processes;
- remote participation in scientific experiments, environmental monitoring with the participation of representatives of different countries;
- formation and provision of services using network technologies – conducting interactive interviews, conferences, telemridges, etc.

What is needed to organize such work? Simply the tools for collecting, processing, analyzing, structuring, archiving information and delivering it to the end user – that is, those standard tools that are part of any medium-sized corporate information system are not enough today. Requires specialized technologies and equipment (Groupware) to form Integrated Collaborative Environments – ICE.

1.1 Video conferencing

One of the effective types of teamwork is conferences organized on television channels or carried out on the basis of computer and network technologies.

There are currently many varieties of conferencing systems available, including computer conferences (e-mail meetings), mobile caller meetings, desktops, multimedia, TV and video conferencing.

Video conferencing is a kind of simultaneous connection between a number of participants (subscribers) who can see and hear each other, no matter where they are, provided with the use of appropriate telecommunications. For the organization of videoconferences use modern technology, called – VCS. Videoconferencing Session is a video call in real time. Videoconferencing is used as one of the technologies to reduce the costs of preparation, coordination and adoption of a business decision, reducing organizational, temporary, transportation and other costs in territorially distributed organizations, as well as one of the elements of technology "telemedicine", "distance learning" and "communication power representatives with the people".

Experience in the use of such technologies has shown their effectiveness – according to studies by psychologists, the level of perception of information and trust is increased in the interlocutors, if non-verbal language (gestures, facial expressions, body position) is added when communicating with the interlocutors.

Videoconferencing and ongoing video networks for ongoing monitoring of mission-critical processes are increasingly used in corporate governance, regardless of the company profile and type of business. Such technologies not only save time and resources for organizing and holding eye-to-eye meetings, but also provide previously unavailable opportunities. This is a remote monitoring of previously closed processes, managing such

processes, conducting distance learning directly during real work without active intervention in it, etc.

Video conferences are usually held in the Videoconference Room, equipped with appropriate computer and multimedia equipment, large monitors (plasma panels) with multi-screen image output, television or Web cameras, an electronic board, telecommunication devices. In this case, specialized software is used to compress and decrypt the information, as well as to secure its transmission over open communication channels or over the Internet.

Various modifications of videoconferencing systems allow to take into account the ergonomics of workplaces of personal subscribers, to create optimal conditions for "subscribers-audiences" taking into account lighting, acoustic environment, convenience of transmission and display of video information.

For the organization of videoconferencing between three or more subscribers the technology of multipoint VCS is used, which can be implemented on a specialized video server (Multipoint Conference Unit – MCU) or on firmware terminals of VCS.

During the videoconference, its participants can exchange fax images and electronic copies of documents, jointly view presentations and videos. They can send files of various formats, broadcast telemetry data (video sessions with spacecraft), store static and dynamic fragments, and request and retrieve information from remote databases of these information systems.

Professional video conferencing opportunities to discuss analytical materials, scientific ideas, political discussions, and discuss different cultural and artistic fields, create opportunities for engaging in discussions that could not have been attracted earlier because of their remoteness.

To communicate in video conferencing, the subscriber must have a complete VCS terminal, which typically includes: microphones, camcorders, a large screen, arrangement of information display and sound reproduction, as well as a codec providing encoding/decoding of the stream.

As a codec, a computer with appropriate software or software may be used to adapt the VCS systems to different bandwidths and the quality of the transmitted video, namely: use H.261/H.263 standards, MJPEG, MPEG2, MPEG4. In particular, encoding video information using

MPEG 2/4 codecs allows you to achieve a higher transmission rate, and encoding using the MJPEG codec allows for greater resistance to interference in the communication channel.

One of the Internet Protocol – IP or Integrated Services Digital Network – ISDN is used to connect the VCS to the data network.

In the course of preparation for participation in videoconferencing, a contact book is usually formed in advance of the VCS system, which contains the contact addresses of potential participants. Once agreed with all participants in the videoconference, the address book is approved and used by the organizer (administrator) of the WCC as a basic document for the identification of participants and their connection. There is an opportunity for both personal and group calls. Once the call is acknowledged, voice and video communications are established automatically.

At the request of the subscriber, a voice-only connection may be made initially, with subsequent video connection. If the VCS is made in Point to Point Mode, the call is transmitted directly to the calling party's workplace, and if the communication is to occur in Multipoint Mode, the call first arrives at the video server, which then calls (notifies) other participants in the video conference. The process of video conferencing consists of the following stages: hardware and software initialization of the VCS; establishing a connection, calling a subscriber (s) or video server; identification of subscribers, registration and approval of additional participants; call or disconnect additional subscribers; duplex audio-visual communication; challenge of remote information resources, exchange of materials, record keeping, preparation and adoption of resolutions, final voting, conclusion of the video conference by the chairman or moderator, agreed with all participants having the decisive vote;

Each videoconference subscriber has equal rights and responsibilities. Within the corporate data network, several video conferences can be held simultaneously with the presence of a powerful video server. The need for full CCTV video recording is generally agreed upon in advance – except in the case of recording videoconferencing with subsequent selective editing for media or for archiving important events. Any participant in a video conference can pre-opt out or terminate its participation directly in its process. These actions are determined solely by the participant and the overall situation of the VC.

The modern communication technologies used in professional VC systems (Digital Videoconferencing System – DVS) make it possible to use them with virtually any communication channels: analog and digital wire telephone channels; radio channels; radio relay lines; fiber optic channels; dedicated telephone and VPN channels; satellite channels; local and Internet networks; GSM/CDMA/GPRS cellular communication channels and so on.

The main communication parameters under which the use of professional VC systems are possible are shown in Table 1.

You can control some important parameters directly in a VCS session: the number of frames that come per second, the real speed of outgoing and incoming IP packets, all and through the channels individually (data, sound, video), the number of lost or distorted IP processes. packages – all and by channels separately (data, sound, video). You can also control and change the basic parameters of both your own system and the remote subscriber system: communication parameters; settings of input and output devices; parameters for digitization and compression of video, sound and data; user interface settings.

Table 1

Basic communication parameters

№	Parameter type	Amount
1	Minimum data rate (Kbps) – "video/audio + video/text"	19/2/4
2	Maximum data rate (Mbps)	100,0
3	Channel error probability	not more than 5-8% (without special coding)
4	Channel delays (recommended)	not more than 1 sec.
5	IP Packet Delivery Timeout (Recommended)	not more than 100 msec.
6	Channel Signal Fluctuations (Recommended)	not more than 10% (preferably)

We will note that the price range for modern VCS is very wide – from 500 to 2500 dollars for the Desktop System for work in a local area network, and from 5000 to 50000 dollars for the Videoconference Room System, operating both in local and and in external networks. The choice of a particular VCS is determined by the company's business objectives and capabilities.

1.2 Office automation and document management systems

Office Automation Systems is based on office automation and records management automation programs that cover all types of office-related issues that need to be studied and accepted and require approval from the hierarchy of managers[1].

Modern document management systems have advanced means of creating and sending documents in an automated manner, allowing you to track the routes and correctness of filling the document at all stages of its creation or processing.

In today's market are presented dozens of available software products of domestic and foreign companies in a wide price range, on the Internet you can find different versions of Open Source products for office management.

1.3 Group Activity Planning

The task of Group Activity Planning systems is to simplify the agenda planning process of working groups, their daily, weekly and long-term activities. By working with a shared database and scheduler, an organization can minimize overlays in team members' schedules. Such Outlook modules are now embedded in virtually all office applications, and MS Project and Primavera software packages are used for quick planning and reliable execution control.

1.4 Collective design of textual documentation and graphic materials

Group documentation development is the creation of a set of documentation at a time by a group of employees, some of whom can work together on a single document (identifying and formulating requirements, developing specifications, drawing up a plan, report, instructions, preparing the text of a brochure or article).

Using a system for collecting documentation collectively allows each member of the workgroup to create and edit their own sections of documents, which may include text, graphics, spreadsheets etc. The hardware for this system includes a file server with databases, which is one of the nodes on the LAN and with which the workgroup personal computers are connected.

[1] Мирошник И.В. Теория автоматического управления. Линейные системы. Санкт-Питербург, 2005. 336 с.

It focuses on all group documentation, text editors, and graphics packages (if the interaction is built on a client-server scheme).

For the group to create documents together, specialized software is used to identify, locate, track, move and maintain documents, and configure and control complex multi-page documents containing text, tables, and graphs.

1.5 Text Database Systems for Open Working Groups

The use of such databases (DBs) is a very effective way of accessing unstructured textual data that stores a variety of organization materials – a body of textual data obtained from emails, electronic message boards and collective free access resources. It is an important corporate resource that can be used to solve internal tasks, work with clients and in many other cases[2].

When storing text data, an effective way to systematize large amounts of information is to use link technology and hypertext. Using hypertext provides users with quick and convenient access to information contained in large documents. Hypertext sharing allows people to conduct a distributed work session in real time, for example, simultaneously viewing and editing different sections of text. User actions are immediately displayed on the displays of all participants who have opted for the high-coupling interaction mode.

If the user chooses the weak-link interaction mode, he or she may take some actions that will not be immediately visible to others, but the Source Safe System will always capture and save any changes made.

Note that in the 80s and 90s of the XX century, the leader among Lotus Notes / Domino Lotus products was a leader among low-cost software products that implement open source teamwork on the organization's LAN. This product has many important features.

Lotus Notes databases store documents containing graphical data, spreadsheets, text information, etc. in the form of a single entry. What's more, this software is compatible with many popular text editors, spreadsheet applications, and graphics packages for the PC.

Lotus Notes can work with different operating systems and with different hardware. It can be used on any computer running Windows or

[2] Цыпкин Я.З. Основы теории автоматических систем. Главная редакция физико-математической литературы изд-ва «Наука», Москва, 1977, 56 с.

Unix, as well as some popular network operating systems, including Novell, Banyan, and IBM. This interoperability simplifies the process of sharing information and user collaboration across large distributed systems.

1.6 Database management systems for workgroups

Placing, storing, securing and issuing information on request are fundamental functions of automated IS. Data storage is performed on secondary storage devices, using a hierarchical system of data levels: bits, bytes, fields, records, files and databases. Each record in the database contains specific fields of a given length, the record set is a file.

Data Base Management System – DBMS provides the user with the necessary data, hiding technologies for their placement, storage and maintenance[3].

Workgroup DBMS is software for managing (entering, updating, organizing, querying, reporting, etc.) databases. Such popular databases as Microsoft Access, Progress, MySQL can be used by one person and a group of executors. The difference between DBMS for workgroups and individual DBMS is that DBMS for workgroups control access and sharing of data and ensure their integrity in teamwork.

Modern DBMS, implemented, for example, technologies and tools Microsoft and Oracle, provide many flexible functions for teamwork with complex and distributed databases. Note that products such as Apache Web servers, MySQL databases, or PostreSQL are currently available.

1.7 Support systems for preparation and decision making

Since the mid-1980s, when the focus of IP began to shift from reporting to the use of IP to support business implementation, systems were being developed and increasingly used to enable teams of professionals to effectively prepare for business decision-making. Such a teamwork system is an "interactive automated system" that facilitates decision-making on unstructured issues by the team members of Decision Support Systems.

In the early 1990s, there was a generalized system of requirements for technological support of such groups and the necessary communications. Each member of such a group has a personal computer or workstation that

[3] Попович М.Г., Ковальчук О.В. Теорія автоматичного керування: підручник. 2-ге вид., переробл. і допов. Київ.: Либідь, 2007. 656 с.

is connected on a local or Internet network to the computers of the other members of the group, as well as to one or more large screens or electronic boards for each participant groups could see information entered by others.

Software for group decision-making systems should support specialized functions such as anonymous input of ideas and user comments, list of user input, voting, ranking of alternative solutions and their display (Dialog Mapping System).

The human component includes either several experts, analysts, representatives of interested project teams, and a moderator who conducts the session and mediates between the group and the computer system. The group's tasks include establishing personal communications, discussing and systematically analyzing problems, resolving emerging issues, negotiating, resolving conflicts, designing solutions, preparing documents, and sharing them.

Based on the application of IT Integrated Collaborative Environments – ICE, which includes audio and video equipment, procedures, techniques, aids and data required for the work, provides support for group meetings, which can be distributed over time and in space.

Shared software is incorporating an increasing number of Internet protocols. Such products include, for example, Lotus Development's Domino or Microsoft Exchange. It is no longer a question of securing certain areas of teamwork.

There are many products on the market from leading foreign software manufacturers Microsoft, IBM, Intel, Sun Microsystems, Borland, Novell, some domestic companies that implement a full-featured environment (IT infrastructure) to manage the company's activities and effective IT support of these activities to solve the major business tasks

2. IT based on the concept of artificial intelligence

What is the difference between Crisp Logic and Fuzzy Logic? In Crisp Logic, the expected consequence always unambiguously follows the stated reference, if clear rules of the condition are fulfilled – for example, "if A, then B", or, "if A and B, then C". When the Fuzzy Logic, the boundaries of the condition are not defined or clearly defined: "if A, then in the time interval [T1, T2] B may be much greater than B, and may be almost equal to B" – it all depends on the initial and current conditions, which can change rapidly even within a fixed period of time [T1, T2].

Algorithms for analyzing such situations, as a rule, implement scenario scenarios for the risk assessment of each variant. Accordingly, the information system in this case, in addition to the standard functions of data collection, storage and transmission, should contain modules that implement the processing and multivariate analysis of information. Since the development of a business situation can be determined by several parameters, and models describing such situations are rarely linear, the real problem is often reduced to the tasks of multivariate estimation and nonlinear optimization[4].

In this context, Decision Support System (DSS), Expert Information System (EIS), Executive Support System (ESS), Diagnostic Information System (DIS), Image Recognition System (IRS) and Searching System modules are typically built using the principles that are called "principles of artificial intelligence".

Artificial Intelligence is a section of computer linguistics and informatics that deals with formalizing problems and tasks that resemble human tasks. In most cases, the algorithm for solving the problem is unknown in advance. There is no precise definition of this science, since philosophy does not address the nature and status of human intelligence. There is also no exact criterion for achieving "intelligence" by the computer, although a number of hypotheses, such as the Turing test or the Newell-Simon hypothesis, have been proposed before artificial intelligence. There are now many approaches to understanding the tasks of artificial intelligence and to creating intelligent systems.

In addition, artificial intelligence can be defined as "a set of theoretical methods and physical computing devices whose task is to reproduce reasonable considerations and actions aimed at achieving the expected or new result".

One of the classifications identifies two approaches to the development of artificial intelligence: descending, semiotic – the creation of symbolic systems that model high-level mental processes: thinking, judgment, language, emotions, creativity, etc.; ascending, biological – the study of artificial neural networks and evolutionary computations that model intellectual behavior on the basis of smaller "non-intellectual" elements.

[4] Иващенко Н.Н. Автоматическое регулирование. Теория и элементы систем. Учебн. для вузов. Изд. 4-е, перераб. и доп. Москва: «Машиностроение», 1978. 236 с.

This science is related to psychology, neurophysiology, transhumanism and others. Like all computer science, it uses a mathematical apparatus. Of particular importance to her are philosophy and robotics.

Artificial intelligence is a very young field of research, started in 1956. Its historical path is reminiscent of a sine wave, each "take-off" of which was initiated by some new idea. In the 1950s, Wiener, Newell, Simon, and Shaw appeared, exploring the essence of different tasks. The results are algorithms and computer programs "Theoretical Logic", designed to prove theorems in numerous statements, and "General Problem Solver". These works initiated the first stage of research in the field of artificial intelligence related to the development of algorithms and programs for solving problems based on the use of various heuristic methods.

Unlike algorithmic methods that allow for formal verification of correctness, heuristic methods of solving the problem are considered as inherent in human thinking in general, which is characterized by the emergence of intuitive assumptions about the way to solve the problem.

Thus, the overall task of using artificial intelligence is to build a computer-based intellectual system that would have a level of effectiveness in solving informal tasks that is comparable to human or superior. As a high-level criterion for the intelligence of systems based on artificial intelligence technology, an imaginary experiment known as the "Turing test" proposed by Alan Turing in 1950 was proposed. in the article "Computers and Mind" to see if a computer is "intelligent" in the human sense of the word.

Today, the position on the sine wave is on the decline, inferior to the application of already achieved results in other fields of science, industry, business and even in everyday life.

Although far-reaching artificial intelligence is far, some progress has been made in the formation of so-called expert systems and neural networks.

Modern expert systems use the knowledge and intuition of experts – people who are deeply versed in solving a range of tasks (specialists in this subject area). Expert systems are a computing structure that independently generates an algorithm for solving a possible set of logic subsystems and computational operations designed by experts. The choice of certain

subsystems of operators is made according to the estimates and comparisons formulated earlier by experts.

Neural networks are also interesting. Previously, it was called the neural network "perseptio", because the main task in their formation was pattern recognition.

Neural networks use non-linear mathematical models of neurons as elements, of which there may be many in the network. Most neurons can be tuned by changing their response to the input signal. If there are a sufficient number of tasks in the required and broad class of tasks whose solution is known in advance, you can start learning a neural network – a neurocomputer. The network is set up – trained, passing through it all the known decisions and seeking the necessary answers on the way out. The setting is to select the parameters of the neurons. Once set up, the network is able to correctly answer questions from the same series of tasks.

It is not without reason that mathematicians believe that the mechanism for solving problems in expert systems and neural networks is almost similar. But if, in the case of a neural network, even its adjuster does not understand how knowledge (ie, the network is a so-called "black box") is formed in its structure, then its creators must put that knowledge into the expert system. some form (using a certain formalism). Usually, when working with an expert system, it creates new knowledge, which it then uses. By the way, you can always review this knowledge of the expert system and check the solution of each problem at all its stages. But the problem is hidden in the obvious shortcomings of formalism, invented by man, the very structure of the representation of knowledge, which may simply not meet the required level of description of real tasks. The neural network does not use formalisms and largely behaves like natural intelligence.

There is no single answer to what artificial intelligence (AI) deals with. Almost every author who writes a book on artificial intelligence is repelled by any definition, considering in his light the achievements of this science. Usually, these definitions are as follows: Artificial intelligence studies methods of solving problems that require human understanding. Roughly speaking, this is about teaching AI to solve intelligence tests. This involves developing ways to solve problems by analogy, methods of deduction and induction, the accumulation of basic knowledge and the ability to use them; artificial intelligence studies methods of solving problems for which there are no ways of solving or which are not correct (due to limitations in time, memory, etc.). Due to this definition, intellectual algorithms are often used to

solve NP-complete tasks, such as traveling salesman tasks; artificial intelligence is involved in modeling the human higher nervous activity; Artificial intelligence is systems that can operate with knowledge, and most importantly, learn. First of all, it is about recognizing the class of expert systems (the name comes from the fact that they are capable of replacing expert people) with intellectual systems.

It follows that the scientific aspect of the problem of artificial intelligence concerns attempts to explain its work and explores the possibility of constructing common algorithms for its functioning. An applied aspect of AI involves the computer solution of a variety of problems that do not have a clear algorithmic solution, or multivariate "What if" tasks, that is, tasks with fuzzy goals and fuzzy logic. It uses "human" ways to solve such problems, that is, to simulate the situation when such a problem is solved by a person.

The latter approach, which began to develop since the 1990s, is called the agent-oriented approach. This approach focuses on the methods and algorithms that will help the intelligent agent to survive in the environment while performing their task. Therefore, search and decision algorithms are much more often studied here.

The fields of application of artificial intelligence methods are extremely wide: the proofs of informal theorems and the solution of problems with fuzzy logic; game theory, study of game situations and possibilities of synthesis of decisions (theory and practice of computer chess); recognition of images (symbols, texts, language, images) for the purpose of search, processing and adaptation; adaptive programming; imitation of creative activity – a work of literary texts, poems, music; data processing and transformation in natural languages, machine translation; machine vision, virtual reality building; learning systems based on neural networks; control systems and robotics (automotive, aviation, aerospace, humanoid multifunctional works, etc.); building specialized information systems to support business decision-making.

2.1 Data mining systems

A class of technologies and systems created on the basis of artificial intelligence principles and intended to support business decision-making under uncertainty, became widely used in business and was called "Business Intelligence (BI)".

For the first time, the term "Business Intelligence" was introduced by Gartner analysts in the late 1980s as "a central user process that includes access to information and its exploration, analysis, intuition and understanding that lead to improved and informal decision making" .

Later, in 1996, refinements were made – tools for analyzing data, building reports and queries that could help business users overcome the complexities of processing, interpreting and presenting data in order to synthesize meaningful information from them. These tools collectively fall into a category called Business Intelligence Toolware.

Today, BI product categories include: BI tools and BI applications. BI tools can be divided into the following types: Query / ReportGenerator (QRG); advanced BI tools – first of all, Online Analytical

Processing – OLAP; Enterprise BISuites – EBIS of various configurations built into ERP systems; BI platform.

Multidimensional OLAP servers, as well as relational OLAP mechanisms, are BI tools and infrastructure for BI platforms, on the basis of which various applications with "custom" interfaces are being developed. These tools are used to access data, multidimensional and multivariate analysis, and generate reports based on data that is most often housed in various storefronts, warehouses, databases, or data warehouses. Executive Support System (ES) is as an example of BI-application. BI applications are usually focused on specific important functions of the organization, such as analysis of market trends, risk analysis, analysis and forecasting of sales, budget planning, etc. They can be used more widely – to build a Balanced Scorecard System or Enterprise Perfomance Management. Methods and systems of data mining, built on the basis of neural self-learning networks, are widely used in the creation of modern information systems. This is a large class of systems whose architecture has some analogy to the construction of neural tissue from neurons.

In one of the most common architectures – the multilayer perceptron with reverse error propagation – it simulates the work of neurons in the hierarchical network, where each higher-level neuron is connected by its inputs to the outputs of the layer below the neurons.

The neurons of the lowest layer are given the values of the input parameters, on the basis of which it is necessary to make some decisions, predict the development of the situation, etc. These values are regarded as signals transmitted to the next layer, weakening or amplifying depending

on the numerical values (weights) attributed to the inter-neural relationships. As a result, the output of the neuron of the upper layer produces some value, which is considered as the response-response of the entire network to the input values of the input parameters. In order for the network to continue to be used, it must first be "trained" on previously obtained data, for which both the values of the input parameters and the correct answers are known. "Training" is the selection of weights of inter-neural connections, which provide the closest closeness of network responses to the known correct answers.

There is a scheme of "intelligent self-learning subsystem" that can be used as part of expert, diagnostic, retrieval and other such systems. The work program "launches" a set of initial data, boundary conditions and approximate exit conditions from the iterative chain. These options are related to sets of known situations and known solutions.

The neural network analyzes the data, identifies the correlations, and then selects the sets of the most likely solutions. This set forms the initial model. The parameters are further varied and new data and rules added. When a set of probable values does not improve the model, the condition for issuing a final prediction is triggered. Recently, evolutionary algorithms are actively developing, which involve the creation of a population of programs, their training, mutations, crossing (exchange of parts of programs) and testing for the fulfillment of a target task.

The programs that work best survive – and after many generations, the most effective program comes out. Very effective methods of creating intelligent search and information systems using Multi Agent System, which operate in the information space, interpreting the task, depending on the conditions and search results. Agent means a software or hardware entity capable of acting in the interest of achieving the goals set by the user. An agent's level of intelligence can be assessed as his ability to use the "old" and build "new" knowledge to accomplish the task in previously unknown situations and problem areas where the evaluated agent is used as an active problem solver.

REFERENCES

1. Мирошник И.В. Теория автоматического управления. Линейные системы. Санкт-Питербург, 2005. 336 с.

2. Цыпкин Я.З. Основы теории автоматических систем. Главная редакция физико-математической литературы изд-ва «Наука», Москва, 1977, 56 с.

3. Попович М.Г., Ковальчук О.В. Теорія автоматичного керування: підручник. 2-ге вид., переробл. і допов. Київ: Либідь, 2007. 656 с.

4. Иващенко Н.Н. Автоматическое регулирование. Теория и элементы систем. Учебн. для вузов. Изд. 4-е, перераб. и доп. Москва: «Машиностроение», 1978. 236 с.

Information about the author:
Kyselov V. B.
Doctor of Technical Sciences, Professor,
Director of the Institute of Municipal Administration
and Urban Economics
of the V. I. Vernadsky Taurida National University

DOI https://doi.org/10.36059/978-966-397-104-9/75-95

GEOINFORMATION SYSTEMS

Kyselov V. B.

INTRODUCTION

Globalization and internationalization of the economy, the destruction of trade barriers between a large number of countries in Europe and Asia, the widespread use of IT and IS in the activities of government and commercial entities, the emergence and rapid development of the global Internet led to the emergence of IS in the mid-1980s., which allowed the organization of On Line mode of work of multinational corporations located on different continents. Distances have ceased to be an obstacle to the efficient operation of distributed companies, providing virtually instant communication and delivering information to analyze and make a business decision, implementing the well-known 7x24 principle (7 days a week, 24 hours a day)[1].

Much of this information is available in almost every field of activity in the form of drawings, maps, plans, diagrams and explanatory texts. These could be gas or oil pipelines from Siberia to Western Europe, submarines and combat patrols along borders, circuits on a country or subway scale across the city, building plans or interconnections between company offices, environmental monitoring map territories, atlas of land cadastre or map of natural resources, etc.

Choosing a location for a company affiliate abroad, marketing and recruiting in another country, coordinating the "binding" of production to the area where it is most advantageous from the point of view of the most efficient use of resources in most cases ceased to be a difficult task.

There was an urgent need to present geographic and related information in a convenient graphical form, combining several sheets of map image on the monitor screen.

The rapid development of specialized systems and technologies, known as Geographical Information Systems (GIS), enabled the successful completion of such tasks by the end of the twentieth century.

[1] Марк Спортак, Френк Паппас и др- Компьютерные сети и сетевые технологии. PlatinumEdition: Пер. сангл. Санкт-Питербург.: ООО «ДиаСофтЮП», 2005. 720 с.

GIS technologies are widespread and used in science, technology, and business. Time-bound objects are used in geodesy, cartography, geology, navigation. Processing and consolidation into a single system of photographic images from space for scientific and military purposes, processing of data of geophysics and geodynamics, use in the national economy (compilation of urban, regional and federal land cadastres) and many other things are done with the use of GIS technologies. Numerous definitions of "Geoinformation system" and "geoinformation technology" reflect the multifaceted nature of the concepts.

Table 1

GIS definitions chronology

Author	Definition of GIS	Source
Langeforce B.	A system that includes components for collecting, transmitting, storing, processing and issuing territorial information.	Theoretical Analysis of Information Systems. Lund, 1966.
Degani A.	Dynamically organized set of data (dynamic database) connected to a set of models implemented on a computer for the computational, graphic and mapping of this data into spatial information in order to meet the specific needs of certain users within the structure of well-defined concepts and technologies .	Methodological observation on the state of geo cartographic analysis in the context of automated spatial information systems. – Map Data Process. – Proc. NATO Adv. Study Inst. Maratea, June 18–29, 1979, Acad. Press. 1980x 207-220.
Vitek J.D., Walsh St.J., Gregory M.S.	An information system that can provide input, manipulation and analysis of geographically defined data to support decision making.	Accuracy in geographic information systems: an assessment of inherent and operational errors. – Record 9th Symp. Spat. Technol. Remote Sens. Today and Tomorrow. Sioux Falls, S.D., 2-4 Oct. 1984. [нечеткое совпадение] – Proc. Silver Spring, 1984, pp. 296–302.

Table 1 (continuance)

Author	Definition of GIS	Source
Star J.L., Cosentino M.J., Foresman T.W.	Spatially defined system for collecting, storing, searching and manipulating data, as well as a means of analyzing and managing this data.	Geographic information systems: question to ask before it`s to late. – Machine Processing of Remotely ended Data with Special emphasis on Thematic Mapping Data and Geographic Information Systems, 1984, pp. 194–197.
Trofimov A.M., Panasyuk M.V.	Implemented with the help of automatic means (DEC) repository of the system of knowledge about the territorial aspect of the interaction of nature and society, as well as software that simulates the functions of search, input, etc.	Geoinformation systems and problems of environmental management. Kazan, pub. house of Kazan University, 1984, 142 pp.
Clarce K.	A special case of an information system where a database consists of observations of spatially distributed phenomena, processes, or events that can be defined as points, lines, and contours.	Geographic information systems: definitions and prospects. – Bull. Geogr. and Map Div. Spec. Libr. Assoc., 1985, № 142, pp. 12–17.
Konecny M.	A system consisting of humans, as well as the technical and organizational means that collect, transmit, enter and process data for the production of information that is convenient for later use in geographical research and for its practical application.	Geograficke informacni systemy. – Folia prirodoved. fak. UJEP v Brne, 1985, t. 26, № 13, 196 s.
Mac-Donald C.L., Crain I.K.	A system that is implemented to collect, store, manipulate, search and display specific geographical data.	Applied computer graphics in a geographic information system: problems and successes. – Computer graphics and app, 1985, vol. [нечеткое совпадение] 1980x 34–39.
Reisinger T.W., Davis C.J.	A system that manipulates and manages data stored in the form of thematic layers, geographically defined relative to the map base.	A map-based decision support system for operational planning of timber harvests. – Winter Meet. Amer. Soc. Arg. Eng., Ayatt Regency, Chicago, Decem ber 17–20, 1985. Paper N 1604. – St. Joseph: ASAE, 1985, 12 p.

Table 1 (continuance)

Abler R.	A complex of hardware and software and human activities for storing, manipulating and displaying geographically (spatially correlated) data.	The National Science Foundation National Center for Geographic Information and Analysis – International Journal of Geographical Information Systems, 1987, v. 1, № 4, pp. 302–306.
Berry J.	Internally positioned automated spatial information system designed to manage and map data.	Fundamental operations in computer-assisted map analysis – International Journal of Geographical Information Systems, 1987, v. 1, № 4, pp. 119–136.
Lillesand T., Liefer R. W.	A system that includes a database, hardware, specialized mathematical software, and software packages to expand the database, manipulate data, visualize them in the form of maps or tables, and ultimately make decisions about a particular business activity	Remote session and image interpretation. N.Y., John Willey and Sons, 1987, 722 p.
Tikunov V.S.	Interactive systems capable of realizing the collection, systematization, storage, processing, evaluation and means of obtaining new information and knowledge about spatial-temporal phenomena on their basis.	Modern means of research of the system "social and industrial environment". – Izvestiya Vsesojuzn. Geograf. obshestva, 1989. 121p. 4, p. 299–306”.
Koshkarev A.V.	A hardware-software human-machine complex that provides the collection, processing, display and dissemination of spatial-coordinated data, integration of data and knowledge about territories for their effective use in solving scientific and applied geographic problems related to inventory, analysis, modeling, forecasting and management of the environment and territorial organization of the company.	Cartography and geoinformatics: ways of interaction. Izv. AN USSR, geographic series, 1990, № 1, p. 32.

Table 1 (ending)

Serbenyuk S. N.	Scientific and technical complexes of automated collection, systematization, processing and presentation (delivery) of geographic information in a new quality with the condition of increasing knowledge about the study of spatial systems.	Cartography and geoinformatics – their interaction. M., 1990, 159p.
Simonov A.V.	A system of hardware and algorithmic procedures designed for digital support, replenishment, control, manipulation, analysis, mathematical and cartographic modeling and figurative display of geographically coordinated data.	Agroecological cartography. – Chisinau, publishing house "Stiinets", 1991 – 127 p.

By analyzing these definitions and omitting repetitions, you can identify the main keywords of GIS technologies. These are "information system", "geographical information", "software-hardware", "interactive systems", "mathematical static and dynamic models", "spatial-coordinated data", "control, analysis, data manipulation", "visualization of data in the form of maps or tables","thematic map layers","mapping databases".

And finally, let's give the definition of 1997, taken from GOST (State Standard), which largely integrates the above definitions and uses almost all of the above keywords.

"Geographic Information System (GIS) is a set of technical, software, communication and information tools that provide input, processing, storage, mathematical and cartographic modeling and imaginative integrated representation (visualization) of spatial and related attribute data to solve problems of territorial planning and Management (OST HSE 02.001-97).

Thus, GIS technologies are, first and foremost, computer technologies and systems that allow to work effectively with dynamic data on spatial-distributed objects, supplementing their clarity of representation and ability to build models and solve problems of spatio-temporal analysis.

GIS, like any information system, is equipped with data collection and processing tools, allows you to accumulate and analyze such information, quickly find and process the necessary geographical information and display them in a user-friendly way.

The use of GIS technologies can dramatically increase the efficiency and quality of work with spatial-distributed information in comparison with traditional "paper" cartographic methods.

Geographic Spatial Distributed Data means information that identifies the geographical location and properties of natural or artificially created objects, as well as their boundaries on earth, above and below ground, on water, above and under water, in outer space. This information can be obtained through remote sensing, mapping and various types of imagery, including space photography.

The data contains four integrated components: the location and spatial relationships of the objects, the time at which these components are fixed, and the rate of change of the specified parameters. In other words, geographical data describes:

- the geographical spatial position of physical or simulated objects is represented by 2-dimensional (X, Y coordinates on the plane), 3-dimensional (latitude, longitude, height above the level of the geoid) and 4-dimensional coordinates (latitude, longitude, height above geoid level, time in seconds) in the coordinate system assigned to the middle pole of the Earth and the position of the middle equator;
- the properties of objects or models may contain information that does not explicitly indicate spatial orientation and is descriptive, however, such information is important and is also included in geographic data;
- spatial relations determine the relative location of objects or models, for example, the position of object A with respect to object B on a plane, in space or in time, the motion of A relative to B, the nesting of A in B and so on;
- time parameters can characterize both the relationship of objects (models) and the life cycle of geographical data.

Areas of GIS are extremely diverse today: land management, resource control, ecology, municipal government, transport, economics, social tasks and more.

The first work on GIS technology began more than 25 years ago in Canada and the United States, where it was originally used primarily for land management in the southern and western United States and the mapping of Canadian areas of the Arctic by computer processing of satellite photographs.

Nowadays, GISs of mass use are becoming more widely used – for general electronic plans of cities, plans for the development of mineral deposits and offshore oil exploration, engineering communications schemes, transport traffic schemes, etc.

It is estimated that up to 80–90% of the information we usually deal with can be presented as GIS for various purposes. To support critical areas of activity – nuclear power, oil and gas extraction and transportation, disaster relief, and defense activities – specialized Web resources are now being increasingly developed and deployed to implement distributed GIS and GIS portals. The development of such portals is now carried out on the basis of international standards, created by well-known international organizations for standardization – ISO (International Organization for Standardization) and OGC (Open Geospatial Consortium). These are standards such as ISO 19115 Meta Data, ISO 19139 Meta Data – XML Schema Implementation, Catalog Interfaces, Geography Markup Language and Web Map Service.

GIS is currently one of the fastest growing segments of the market for high-tech computing with a large number of large firms. These include: Intergraph (http://www.intergraph.com/gis), ESRI (http://www.esri.com), MapInfo (http://www. mapinfo.com), Autodesk (http: //www.autodesk.com), CalComp, Space Imaging (http://www.geoeye.com) and many others.

Non-professional users have high-quality Web resources, such as GoogleMap (http://maps.google.com) and Geography NetWork (http://www.geographynetwork.com).

1. GIS Classification

A variety of existing GIS technologies fit into different types of classifications.

GISs differ in the subject area of information modeling – Urban GIS (UGIS), Environmental (GIS), Manufacturing FacilitiesGIS – (MFGIS) and so on.

The problematic orientation of GIS is determined by the scientific and applied tasks it solves – inventory of resources, analysis, evaluation, monitoring, management and planning, decision support.

Integrated GIS (IGIS) combines the functionality of GIS and digital imaging systems (remote sensing data) in a single integrated environment.

Multiscale GIS (MSGIS) is based on multiple representations of spatial objects, providing graphical or cartographic reproduction of data at any zoom level based on the data set that provides the largest spatial resolution.

Spatio-temporal GIS (STGIS) operates with spatial-temporal data. Implementation of geoinformation projects (GISProject) includes the usual life cycle stages:

- Feasibility Study, including the study of user requirements and functionality of GIS software used;
- technical and economic feasibility study for a GIS development;
- Costs/Benefits;
- GIS Designing, including the GIS Pilot Project stage;
- GIS Development;
- testing in a small territorial fragment or test area;
- Prototyping;
- GIS Implementation;
- Setting Into Operation.

Scientific, technical, technological and applied aspects of the design, creation and use of GIS are the subject of study of the branch of rapidly developing informatics – geoinformatics.

In the history of GIS development, geoinformatics identifies four main periods:

- 60's – mid 70's – exploration of the principal possibilities of using large computers of that time for the accumulation, processing, analysis and construction of banks and geographic databases; theoretical work in the field of analysis and construction of banks and geographic databases; theoretical work in the field of processing such data, accumulation of experience;
- mid 70's – mid 80's – the emergence of automated control systems (ACS), including the first specialized GIS, the development of large state GIS projects in the field of control of nuclear energy and hydropower, defense, etc.;
- mid 80's – late 90's – the emergence of the concept of GIS, the emergence of a market for software that implements various GIS based on personal computers, powerful servers and network communications; expanding the scope of GIS based on integrated databases and powerful

DBMS, including tools for processing and necessary visualization of geographical and descriptive data;

- the emergence of application GIS for non-professional users, as well as specialized distributed GIS, such that support state and corporate databases of such data;
- the beginning of the twentieth century – today – increased need for geographical data in connection with the globalization of many sectors of the economy, strong competition in the GIS market, the emergence of large groups of users interested in specific application software GIS-tools, the use of artificial intelligence and intellectual networks in GIS design, application of mobile agent software technology for gathering specialized information in expert GIS, formation of world GIS infrastructure.

These stages of development showed all new requirements for the functionality of different GIS, but these requirements were outlined in the third stage in the 80's – 90's. Let's note at once that GIS is not just a geographical map, transferred to a computer.

Geoinformation systems store information in the form of sets of thematic electronic layers, which can be combined by any necessary attribute. Therefore, GIS technologies integrate operations to work with layers, databases, analysis tools and layer virtualization that contain the right data in the right combinations.

For example, building a large supermarket in a metropolitan area requires a common data analysis. The transformation (merging, splitting, scaling, and so on) of layers and conversion of data from one format to another is done by methods of mathematical mapping and data management in the GIS database.

2. GIS functionality

In GIS, there are five basic functional procedures with data: input, manipulation, control, query and analysis, visualization.

Geographic data (numbers, text, images) for use in GIS are entered in vector or bitmap format, if such data already exists in the appropriate digital format, or pre-digitized using a digitizer or scanner. Each element or object in the image has a coordinate binding. Thus, any properties and characteristics of real objects (models) or their elements are "tied" to the location of the object in the coordinate grid. It should always be borne in mind that digitization or data entry technologies in a specific thematic

layer, as well as overlay and erection of layers, can be accompanied by significant errors, which will further lead to significant mapping of the mapping data and visualization of the result.

Manipulators are various ways of highlighting, grouping and converting data, such as bringing all geoinformation to a single scale and projecting it onto a specific thematic layer for ease of co-processing.

For storing, structuring and managing GIS data, relational databases with elements of OLAP technologies (On Line Analytical Processing) and report generation technologies (Report Creation) are most commonly used. Query and analysis can be performed at different levels of complexity – from the simplest questions of "where an object is and what its descriptive properties" to searching and compiling data on complex templates and "And what if ..." scenarios.

Modern GIS has advanced means of analyzing the proximity and overlay of objects belonging to different thematic layers. The first tool is related to the allocation of buffer zones around specified objects by a combination of different parameters (for example, "Select settlements located not more than two kilometers from a specific airport" or "Calculate the areas of damage in the event of an accident at the NPP and select settlements that fall into these zones"). The second allows you to calculate the intersection, merging, exclusion and other combinations of two or more distributed objects (overlay operations) in the construction of layers.

The results of various operations can be simply displayed on the screen or create (draw) new objects with any set of attribute characteristics. Advanced visualization tools and methods allow GIS to easily control the display of data. The traditional result of processing, analyzing and displaying spatial geographic data is a map, supplemented by accounting documents, embossed color images of real and simulated objects, photographs, tables, diagrams, video clips of the situation development and other multimedia tools.

In addition to these basic operations, modern GIS have a number of special groups of functions that implement user-defined tasks: finding the optimal route, finding the shortest distances, calculating spatial statistics, creating models of geological structures, marine and air currents, etc.

Electronic maps and thematic descriptions are used to graphically represent geographical data describing real objects and their models in GIS. Parameters of location of objects and their relations are spatial

(metric) data, parameters of temporal and thematic properties – attribute (descriptive) information.

The GIS data model is based on the map object classifier. It defines the composition and content of metric, semantic, thematic, dynamic properties of the object and their visual means. The system of symbols is formed using the palette of colors, the texture of lines and fillings, character templates and fonts.

In modern GIS, the technology of layered graphical representation of information is implemented, it corresponds to the representation of coordinate models in topological form (representation of objects and their relations in the form of a graph). Attribute information is displayed on the electronic map layer by numbers, symbols and their sets – inscriptions. Coordinate and attribute data are established in the database via the appropriate identifiers (default or user interface).

Bitmaps and vector models are used to represent geographic features.

A raster model is a representation of land and oceans as a discrete set of elements that make up the desired picture. These elements are called Pixels (Picture Element), and they display an electronic map themed layer on the monitor screen.

Each pixel occupies some small area in the form of a rectangle, has the coordinates of the center (X, Y) in the plane of the map layer associated with the coordinates of the points of the geographical object, and the description of its properties (brightness, color and tone density), corresponding to similar properties of the object.

Bitmap digital images can be obtained directly by digitally photographing the Earth's surface from satellites, or when processing aerial photos by digital scanning methods using digitizers.

Such images are good for visual perception and are convenient for multidimensional processing. However, they take up a lot of space in the memory of computing devices and are poorly scaled – with multiple and multiple zooms, compression and decryption, image clarity is greatly impaired. Therefore, in those cases where the need to scale images without loss of clarity is pre-determined, vector graphics technology is used.

A vector model is a structurally defined graphic representation of a spatial object. The position of the points of the object is given by the coordinates of the end of the vector (x, y, z) and a description of the properties of this point. The mapping of an object is given by a set of

vectors. Since the end of the vector (point) has no area, there is no distortion when the image is zoomed in or out multiple times (scaled). Vector graphics operate with point, line (arcs and contours) and surface (polygon) models of spatial objects.

The following forms of vector data model are valid:

- whole-polygonal structure (topological structure of "spaghetti" type);
- linear nodal (graph structure);
- relational (structure of relations);
- irregular triangulation network.

The formation of the topology is to determine the position of points and nodes in the selected coordinate system on a plane or in space (for relief images) and the digital coding of relationships between point, line and area geographic objects.

Currently, object-oriented geographic database models (such as ESRI's ArcGIS), object forming classes, relationship classes, geometric networks, and layered topologies are being used.

3. GIS Implementation and Support Tools

GIS can be divided into four broad functional categories:

- simple map and charting tools;
- desktop computer and embedded GIS packages;
- full-featured systems;
- Enterprise-wide GIS (corporate systems).

4. Data Diagramming and Mapping Tools

The tools in this category are cheap and easy to use, but with some functionality, they can be fully mapped to more complex systems. Typical examples are spreadsheet tools, such as Microsoft Map in Excel and Lotus Maps. These applications are accessible to any user of MS Excel spreadsheets and Lotus Notes and make it easy to use thematic mapping features – displaying map information from their database on the map. Any manager in ten minutes will learn how to make the cards needed to prepare a business decision.

Another simple but quite functional tool is Business Map. It is designed for users who need more than just thematic mapping. Business Map works with the data of the most popular spreadsheets and databases and supports

such business and management analysis capabilities as, for example, spatial queries, display map composition, identifying and linking coordinates, zip codes and real address information of objects. This category also includes Viewer Facilities. For example, you can cite Geomedia Viewer from Intergraph or a free ArcExplorer that allows you to view and request ArcInfo, ArcView and SDE data, including over the Internet.

An important factor limiting the widespread use of more complex GIS in business tasks is the relative complexity of studying software. To address this obstacle, advanced interfaces have been developed that give the average user powerful and comprehensible geographical analysis tools.

5. Desktop computers and embedded GIS packages

In the first half of the 1990s, the growth of GIS sales was largely driven by the demand for desktop and embedded GIS. And if the first Desktop Mapping systems had limited geographic data capabilities, then modern GISs, "delivered" to a personal computer or embedded in other software, offer a complete set of tools for data analysis and management. These products include: ArcView, Maplnfo, GeoMedia, GeoGraph/GeoDraw, which have advanced DBMS functionality and provide tools for analyzing, integrating and displaying geographic data[2].

For example, an ArcView software package can be used to bind spatial data (via GPS or GLONASS satellite positioning), import data from other sources (mapping and government or corporate databases), and perform complex statistical and modeling studies, to build variants of scenarios of situation development, to carry out on-line processing of field data obtained during geodetic surveys of terrain with laser theodolites.

Let's take a brief look at two of the most typical GISs in this class – ArcView and MapInfo.

ArcView has the tools to select, view and edit a variety of geographic data, create layouts and map templates with legends, graphs and charts, digitize maps using a scanner, associate map objects with attribute information in HotLink mode (with image archives obtained multimedia tools), address coding, printing of cartographic materials. ArcView works directly with many data formats, provides access to standard DBMS (Ingres, Sybase, Oracle, Informix), reads DXF and DWG file formats, and includes

[2] Фролов А.В., Фролов Г.В. Глобальные сети компьютеров: Практическое введение в Internet, E-mail, FTP, WWW и HTML, программирование для WindiwsSockets. Москва: Диалог. Москва: МИФИ, 1996. 283 с.

the following features: invoking remote RPC (Unix) procedures, connection to other applications via DDE (Windows), connecting applications to VisualBasic. There are also a number of standard ArcView applications for engineering research, GPS SAPR3 interoperability, Internet submission.

MapInfoProfessional (http: //www.esti – map.ru) is now one of the real GIS leaders in digital mapping. In addition to the traditional features for a DBMS of this type, MapInfo allows you to collect, store, display, edit and process mapping data based on the spatial and temporal relationships of objects.

Data in different formats can be used in one session at a time.

Data sources can be:

- tables of own MapInfo databases;
- data in CAD vector formats (for embedded GIS applications) and various geoinformation systems: AutoCAD (DXF, DWG), Intergraph/MicroStationDesign, ESRIShape, ARC/INFOExport;
- bitmaps in GIF, JPEG, TIFF, PCX, BMP, PSD, ECW, BIL and GRID (GRA, GRD) formats;
- data obtained by GPS, GLONASS, electronic geodetic instruments (laser theodolites and rangefinders);
- Excel files, Access BASE, Lotus 1-2-3, and text files that, in addition to attribute (descriptive) information, can store the geographic coordinates of point objects.

MapInfo GIS can serve as a "mapping client" when working with common DBMSs such as Oracle and DB2, as it supports an effective mechanism for interacting with them through ODBC.

Moreover, access to data from Oracle DBMS is also possible through the internal interface (OCI) of this database.

MapInfo has a "geographical" extension of the built-in SQL query language, which allows you to organize samples based on the spatial relationships of objects – the distribution, nesting, overlapping, the intersection of object areas. Database queries can be saved as templates for later use.

MapInfo also has the ability to search and map objects by coordinates, address or system of different installed indexes. Windows Application Interaction allows you to integrate MapInfo's Maps window into Delphi, VisualBasic, C.

Sharing MapInfo and the MapBasic development environment enables each user to create specific applications to solve specific application tasks.

6. Full-featured systems

Full-featured software products originate from major government projects of the 60s and 70s that were implemented on major Mainframe computers. They were used mainly by emerging analysts and experts in geoinformatics and were a tool to support unique and specialized research. Such GIS could be used only by qualified specialists who are competent both in software, in the principles of geography, and in problems of a specific application area.

Today, the state of things has changed – modern GIS tools are implementing geoinformatics methods using powerful software and hardware: open-access geographic Web servers, complex multi-factor spatial analysis tools, devices for generating the most accurate electronic, and preparing high-quality paper maps.

Full-featured GIS contain a complete set of geospatial processing tools, including data collection, integration, storage, automatic processing, editing, creation and maintenance of topology, spatial analysis, database connection, visualization and hard copies of any mapping information. The system runs on both WindowsNT and RISC – Unix workstations. In addition to the basic set ArcInfo contains a number of modules that extend the ability to handle location data in different applications.

7. Corporate Systems

Corporate GIS is typically distributed IS with client-server jobs. Enterprise GIS can be implemented using Spatial Database Engine (SDE) spatial data servers that work with ArcView and ArcInfo desktop applications. Such GISs allow you to operate huge amounts of geographic and attribute data and deliver this data to any user on a local or global network. In addition, because spatial data servers are typically implemented in standard relational databases, they are migrated to most database environments. Thus, tools like SDE can be used to:

- build high-speed GIS applications;
- integrate sophisticated geographical data processing features into application programs;
- deliver applications on a range of software and hardware platforms;
- increase the availability of geographical and attribute data and the ability to process and interpret it for business decisions;

- integrate geographic data management into existing enterprise database management systems.

Such applications are most important for companies managing large infrastructures or utilities (such as energy networks), working in transportation and transportation, or developing natural resources – leading oil and gas companies everywhere use GIS to manage exploration, production, and resource allocation.

Corporate-type GIS is closely linked to a number of other types of information systems – Computer Aided Design (CAD), Enterprise Resource Planning (ERP), Logisticand Supply Chain Management (LSCM). Its main difference is the ability to collect, process, manipulate spatial data and perform qualified analysis.

The geographic information system GRASS – Geographic Resources AnalysisSupport System, freely distributed under the GNU Public License, has gained widespread popularity. In the current version, GRASS is a modular multifunctional geoinformation system of universal application.

The primary interface of GRASS to the Unix system is imprinted on the system interface, and the solution can be described as a combination of command and window interfaces. Moreover, the general concept of the interface is guessed in versions under different platforms.

In addition to the standard GUI, different GUI shells can be used, such as the widely known QGIS shell for the GRASS kernel. There is also a Java version of GRASS-JAVAGRASS, which provides a unique cross-platform. All this has ensured the success and wide spread of this geoinformation system.

8. Related technologies: GIS, GPS and GLONASS

GIS database management systems are designed to store and manage all types of data, including geographical (spatial) data. These data are most often obtained by methods of spatial remote sensing – measurements of the coordinates of objects on the Earth's surface using laser rangefinders at Earth observation points and reflectors on board artificial satellites of the Earth (ASE).

Global positioning system receivers and other Doppler radiometers are also used. These devices collect data in the form of sets of coordinates or images (mostly digital) and provide extensive processing, analysis and visualization of the data obtained. Development of the NAVSTAR GPS

(NAVigation Satellite Timing And Ranging Global Positioning System) concept began in 1973 at the initiative of the US Department of Defense. The latest at that time navigation systems at the time, the Loran-C and Omega terrestrial systems, and the Transit satellite have ceased to meet the requirements of accuracy, independence from weather, round-the-clock operation and coverage.

In February 1978, the first experimental GPS satellite was launched. By mid-1993, there were already 24 satellites in orbit, which was enough to ensure continuous navigation anywhere on Earth. The final commissioning of the system was announced only in July 1995.

The GPS system consists of three parts: space, ground and user equipment.

The space part is 24 satellites moving in six orbits. The inclination of the orbits to the Earth's equator is 55 degrees, the angle between the orbital planes is 60 degrees. The orbit height is 20180 km, the circulation period is 12 hours. 50W Satellite Transmitter Power If one of them fails, the others are able to fill gaps in the system, moving in orbit.

An important element of the satellite is an atomic clock, rubidium and cesium, four each, which set the on-board timeline. These scales are constantly in sync with the terrestrial precision time standards.

Each satellite is identified by a Pseudo Random Number (PRN) displayed on the GPS receiver. The terrestrial part consists of 4 surveillance stations located on the tropical islands. They track visible satellites and transmit data to the Command and Control Station at the Colorado Springs Air Force Base for processing on complex orbital software models called ephemeris. The data are transmitted back to the satellites through the ground stations and then transmitted by the satellite to the GPS receivers.

The custom portion includes a satellite receiver, a decoder and a program module for calculating the coordinates of the object on which the receiver is located. The accuracy of coordinate determination depends on many factors – the accuracy of the transmitting and receiving devices, the onboard and terrestrial time scales, the state of the ionosphere and troposphere, solar activity, humidity and pressure in the atmosphere, the geometry of the satellites in the field of view of the receiving antenna. By measuring the distances (pseudorange) of r1 and r2 by long-range or radiometric methods for several satellites, and

comparing them with satellite surveying methods, it is possible to obtain the coordinates of ground-based tracking points and corrections to satellite orbital elements.

Satellite geometry is measured by the PDP (Position Dilution Of Precision) factor. The ideal location of the satellites corresponds to PDP = 1, the large values indicate poor satellite geometry. The PDP value is used as a factor for other errors when comparing observations.

Each pseudorange measured by the receiver has its own error, dependent on atmospheric interference, errors in ephemeris, reflected signal, etc. So, if the estimated values of these errors in the sum are about 50 meters and PDOP = 1.5, then the expected error in determining the location will be 75 meters. If the receiver "caught" four satellites, and they are all close to the zenith of the observation site, then such satellite geometry is "bad" and the result error will be 90-150 meters. With the same 4 satellites, accuracy is much higher if they are spaced evenly along the horizon at an altitude of 20 to 50 degrees. In this case, the accuracy reaches 30 meters, which is about 1 second of the arc – which is already good accuracy.

Modern stationary GPSs provide accurate positioning of up to several fractions of a second when processing spatial data in GIS and precision of distance determination – up to several millimeters. It is clear that such precision is required for scientific and defense applications.

Aeronautical and marine GPS, installed on aircraft and ships, provide accuracy of up to 1 meter, for non-professional use is now quite a few meters accuracy.

Such GPS devices are mounted in mobile phones, in car navigation systems, etc. The final error of the {GPS – GIS – electronic map} will depend on the accuracy of each element of the system. It will be worth mentioning that coordinate map systems – such as, for example, Map Datum – are associated with different terrestrial ellipsoid models used in map construction in different countries. The difference between them can be up to 500 m. When working with GPS and an electronic map, the user must take this into account and make the necessary adjustments.

A Global Navigation Satellite System (GLONASS) is being deployed today, similar to US GPS and operating on the same principles. The difference lies in the signal coding and decryption systems and the spatial data processing algorithms.

9. Cloud technology capabilities

The classic approach to business process automation, established in the period 2000–2010, requires that an organization must have a pool of server equipment to provide services for information support and reliable protection of its core processes. Obviously, such infrastructure requires expensive servers and networking equipment, including routers and firewalls for security, as well as client stations for service users and related software. It is also clear that many organizations, especially in the small and medium-sized businesses, cannot afford this approach to information infrastructure.

The trend of the last five years, characterized by the widespread proliferation of cloud services and cloud storage and data processing, opens up new opportunities for automation and maintenance of business processes.

Cloud computing is a model for providing on-demand network access to a pool of configurable computing and information resources, such as data networks, servers, storage, applications and services. This approach provides a lot of convenience for users, shortens the waiting time and access to the resource, makes the user independent in the choice of resources. However, there are a number of new problems. Not all the necessary services will be able to be transferred to the clouds in the coming years.

There are a number of restrictions that you can not get around. Requirement for the width of the data channel, for data protection and encryption, the inability to work in a virtual environment and a hypervisor environment – the list can be continued. That is why a new approach to data organization and work is currently being actively developed, on the basis of which hybrid systems are designed to inform the organization's processes.

In particular, it is proposed to gradually, in the course of modernization, rebuild the existing information infrastructure into infrastructure built on the principle of a private cloud. This allows you to get results in the form of rapid migration between public and private cloud. For example, collaborative, distributed work technologies are in great demand today.

One of the tools for organizing such work is a corporate or educational portal. The MS SharePoint portal allows you to organize distributed work.

If the infrastructure is built on the principle of a private cloud, it will only require copying virtual machines to a public cloud. In the case of a classic approach to information infrastructure development, a migration project would involve the deployment of new infrastructure and the transfer of old data to a new environment, which is a very time consuming project. This solution can be effectively integrated with your existing organization network. It can be implemented in a hypervisor environment, allowing you to effectively manage the cluster of virtual machines, if necessary, migrate them to the cloud, such as the Windows Azure platform.

Thus, today it is possible to build a hybrid solution – a portal on a corporate server and working applications and data arrays in a private cloud, with the ability to scale into a public cloud.

A hybrid approach to information infrastructure development is an approach whereby some of the resources for which it is appropriate are brought to the public cloud and some of the most critical, business-relevant services remain within the company's information infrastructure. Such an information infrastructure should be built on the principles of a private cloud, using virtualization technologies, to allow for the migration of services, if necessary, in both directions. When using this approach, services should be designed based on the same principles, in order to organize unified approaches to information security.

To ensure the safe operation of a hybrid infrastructure, the following basic rules must be followed:

- control of strict observance of information security policy in the distributed parts of the organization;
- admission to cloud services or hybrid solution by professionals only;
- agreeing on local policies and safeguards at the level of users, network providers and service owners;
- additional local data storage, where possible;
- taking into account the importance of a particular information resource of the enterprise for the business as a whole;
- accounting for new threats when migrating any content to external services.

The private cloud approach to the organization of infrastructure within the company will allow to provide high availability and resiliency of such services, using virtualization technologies. On the one hand, the solution

remains secure, on the other hand, it becomes effective and scalable. The designed infrastructure becomes distributed, which in its competent organization, reduces the risks for enterprises in case of emergencies.

REFERENCES

1. Марк Спортак, Френк Паппас и др. Компьютерные сети и сетевые технологии. PlatinumEdition: Пер. сангл. Санкт-Питербург.: ООО «ДиаСофтЮП», 2005. 720 с.

2. Фролов А.В., Фролов Г.В. Глобальные сети компьютеров: Практическое введение в Internet, E-mail, FTP, WWW и HTML, программирование для WindiwsSockets. Москва: Диалог. Москва: МИФИ, 1996. 283 с.

Information about the author:
Kyselov V. B.
Doctor of Technical Sciences, Professor,
Director of the Institute of Municipal Administration
and Urban Economics
of the V. I. Vernadsky Taurida National University

DOI https://doi.org/10.36059/978-966-397-104-9/96-117

CYBER SECURITY AND COMPUTER ATTACKS

Domnich V. I.

1. Virtual private networks and public information networks

The aspects of security of modern information networks and the specifics of the use of virtual private network technology are considered, considered on the example of the Internet sharing network, the information security features of which largely determine the modern directions of building information networks of large companies and organizations[1].

It is interesting to note that 95% of US Department of Defense traffic is transmitted through public networks (including the Internet) in peacetime. In wartime this proportion should be "only" 70%.

We can assume that the Pentagon is not the poorest organization. The US military relies on public service networks because it develops its infrastructure in the face of rapid technological change – a very expensive and futile exercise, justified even in critical national organizations only in exceptional cases.

There are a number of common attacks based on protocol features and network structure, describing the reasons why they are possible, and how to resolve vulnerabilities. Recommendations are given to increase the degree of protection of modern information networks.

Typical attacks are discussed, but some general definitions must be made first and security classification should be considered. In addition, it should be noted that, according to statistics, data destruction in computer systems is most often caused not by hackers, program errors or virus actions (17%) or technical failures (16%), but by errors and unauthorized user actions (67%).

2. Basic concepts of computer security

A computer system security threat is a potentially possible event that may adversely affect the system itself, as well as the information stored therein[2].

[1] Крол Эд. Все об Internet: Руководство и каталог. Пер. с англ. С.М. Тимачева. Киев: BNV, 1995. 591 с.

[2] Вертузаев М. С., Юрченко О.М. Защита информации в компьютерных системах от несанкционированного доступа. Київ: Европ. ун-т, 2001. 320 с.

The vulnerability of a computer system is some of its unsuccessful characteristics that make it possible to create a threat.

Finally, an attack on a computer system is an action taken by an attacker to identify and exploit a particular vulnerability.

Researchers typically identify three major types of security threats:

- disclosure,
- integrity,
- denial of service.

The threat of disclosure is that the information becomes known to those who should not know it. Sometimes, the term "disclosure" uses the terms "theft" or "leakage."

The threat of integrity involves any deliberate alteration of data stored in a computer system or transmitted from one system to another. Disclosure threats are generally considered to be predominantly exposed by government agencies, and threats to integrity are business or commercial.

The threat of denial of service occurs every time that some actions block access to some computing system resource.

In fact, the blocking can be permanent, so that the requested resource is never received, or it can only cause a delay of the requested resource, long enough for it to become unnecessary. In such cases, the resource is said to be exhausted.

In local area network (LAN), the most common threats are disclosure and integrity, and in the global are the threat of denial of service.

3. Computer network security features

The main feature of any network system is that its components are distributed in space and the connection between them is physically carried out through network connections (coaxial cable, twisted pair, optical fiber, etc.). п.) And programmatically through a message mechanism. In this case, all control messages and data transmitted between the objects of the distributed computing system are transmitted over the network connections in the form of packets[3].

Network systems are characterized by the fact that, in addition to the usual (local) attacks carried out within the same computer system, they are

[3] Ярочкин В.И. Основы защиты информации. Москва: Летописец, 2000. 150 с.

subject to a specific type of attacks, due to the distribution of resources and information in space.

These are so-called remote or network attacks. They are characterized, first, by the fact that the attacker can be located thousands of kilometers from the attacked object, and, second, by the fact that the information transmitted over network connections may not be attacked by a specific computer[4].

With the development of local and global networks, it is remote attacks that are leading in both the number of attempts and the success of their application and, accordingly, ensuring the security of the OS in terms of counteracting remote attacks is of paramount importance.

4. Classification of computer attacks

The forms of organization of attacks are very diverse, but in general they all fall into one of the following categories[5]:

- Remote Computer Intrusion: Applications that gain unauthorized access to another computer over the Internet (or local area network).
- Local Computer Intrusion: Applications that gain unauthorized access to the computer they are running.
- Remote computer lock: Programs that block the entire remote computer or an individual program on it through the Internet (or network).
- Local computer lock: Programs that block the computer on which they work.
- Network Scanners: Applications that collect network information to determine which computers and applications running on them are potentially vulnerable to attack.
- Vulnerability Scanners: Applications that scan large groups of computers on the Internet in search of computers vulnerable to one or * other specific type of attack.
- Password crackers: applications that detect easily guessed passwords in encrypted password files.
- Network Analyzers (sniffers): Applications that listen to network traffic. Often, they have the ability to automatically isolate usernames, passwords, and credit card numbers from traffic.

[4] Зепкды П.Д. Теория и практика обеспечения информационной безопасности. Под ред. Москва: Яхтсмен, 1996. 302 с.

[5] HackZone- территория взлома (httn://www.hackzone.ru).

- Modification of transmitted data or substitution of information. Replacing a trusted distributed CS object (working on its behalf) or a faulty distributed system object (DCS).
- Social engineering is unauthorized access to information, other than hacking software. The goal is to trick people into getting passwords to the system or other information that will help break the security of the system.

5. Statistics of the most common attacks

In 1999, NIST (National Institute of Standards and Technology) analyzed 237 computer attacks, the information of which was published on the Internet. This analysis provided the following statistics:

29% of the attacks were from Windows.

Conclusion: It is not necessary to consider only the Unix system dangerous. The availability of hacking applications on the network allows them to be used not only by specialists.

In the future, this percentage is likely to grow.

In 20% of attacks, attackers were able to remotely infiltrate network elements (routers, switches, hosts, printers, and firewalls).

Conclusion: Attacks in which an attacker gains unauthorized access to remote hosts are not that rare.

In 3% of attacks, websites attacked their visitors.

Conclusion: Finding information on the WWW (World Wide Web) is no longer a completely safe activity.

In 4% of attacks, the Internet was scanned for vulnerable hosts.

Conclusion: There are many auto-scanning tools that can compromise hosts. System administrators must scan their systems regularly (otherwise someone else will do it).

5% of attacks were successful attacks against routers and firewalls.

The components of the Internet infrastructure themselves are vulnerable to attack (though, most of these attacks were remote computer-locked and scanned attacks, and only a small fraction were remote-penetration).

According to a 1999 survey by the Computer Security Institute and the FBI on computer crimes, 57% of organizations surveyed said they consider the connection point from local network to the Internet as point from where attacks are often organized. 30% of those surveyed reported

that they had penetrated their network, and 26% said that the information had been stolen in the course of the attacks. The Federal Center for Computer Crime in the US – FedCIRC reported that in 1999, about 130,000 state networks with 1,100,000 computers were attacked.

6. Network Traffic Analysis of the Internet

One way to obtain passwords and user IDs on the Internet is to analyze network traffic. Network analysis is carried out by means of a special program-package analyzer (sniffer), intercepts all packets transmitted by a segment of the network, and distinguishes among them those in which the user ID and his password are transmitted.

In many protocols, data is transmitted in an open, unencrypted form. Network traffic analysis allows to intercept data transmitted via FTP and TELNET protocols (passwords and user IDs), HTTP (transfer of hypertext between web-server and browser, including user-entered forms on web-pages), SMTP, POP3, IMAP, NNTP (email and conferences) and IRC (online chat). Thus, passwords can be intercepted to access mail systems with a web interface, credit card numbers when working with e-commerce systems and various personal information, the disclosure of which is undesirable.

Currently, various exchange protocols have been developed to protect the network connection and encrypt the traffic (for example, SSL and TLS, SKIP, S-HTTP, etc.). Unfortunately, they have not yet changed the old protocols and have not become the standard for every user.

To some extent, restrictions on the export of strong cryptography tools have prevented their proliferation. Because of this, the implementation of these protocols either did not build into the software, or significantly weakened (limited the maximum key length), which led to the practical futility of them, as the ciphers could be opened within an acceptable time.

7. Fake ARP-server on the Internet

To address IP packets on the Internet, in addition to the host IP address, you need either the Ethemet address of its network adapter (in the case of addressing within one subnet), or the Ethemet address of the router (in the case of inter-network addressing). Initially, the host may not have information about the Ethemet addresses of other hosts that reside with it in the same segment, including the router's Ethernet address.

Therefore, a standard problem solved with the remote search algorithm is facing the host.

The Internet uses the Address Resolution Protocol (ARP) to solve this problem. The ARP protocol allows one-to-one correspondence of IP and Ethemet addresses for hosts within one segment. This protocol works as follows: the first time you access a network resource, the host sends a ARP broadcast request, which specifies the IP address of the desired resource (router or host) and asks for its Ethemet address.

This request is received by all stations in this segment of the network, including the station being searched for. Upon receiving this request, the host enters the station request record into its ADR table and then sends an ADR response to the host with its Ethemet address.

Received in the ARP response The Ethemet address is stored in the ARP table stored in the operating system memory on the host.

Because of the use of remote search algorithms, it is possible to execute a typical remote attack in such a network.

The general scheme of this attack:

- waiting for an ARP request;
- upon receipt of an APR request, a network transmission to the host of an erroneous ARP response that specifies the address of the network adapter of the attack station (erroneous ARP server) or the Ethernet address at which the ARP server will receive packets;
- receiving, analyzing, influencing and transmitting packets of exchange between interacting hosts (affecting the intercepted information);
- The simplest solution to eliminating this attack is to create a static ARP table as a file containing address information and install this file on each host within the segment.

8. Fake DNS-server on the Internet

As you know, 32-bit IP addresses are used to access hosts on the Internet, uniquely identifying each network computer. But for users, the use of IP addresses when accessing hosts is not very convenient and not the most obvious. Therefore, for their convenience, it was decided to assign all computers on the Network names, which in turn required the transformation of these names into IP addresses, since at the network level packet addressing goes not by names, but by IP addresses.

Initially, when there were few computers on the Internet, there was a special file (the so-called hosts file) to solve the problem of converting names into addresses, in which the names were assigned IP addresses. The file was regularly updated and sent to the Web.

As the Internet evolved, the number of networked hosts increased, and such a scheme became less efficient. Therefore, she was replaced by a new name conversion system that allows the user to obtain an IP address corresponding to a specific name from the nearest DNS server. This workaround is named Domain Name System, (DNS). A DNS protocol was developed to implement this system.

The algorithm for DNS service:

The host sends the IP address of the nearest DNS server to the DNS request, which specifies the name of the server whose IP address you want to find.

When receiving such a request, the DNS server looks for the specified name in its name database. If it and the corresponding IP address are found, the DNS server sends a DNS response to the host, which specifies that address.

If the name is not found in its name database, the DNS server sends a DNS request to one of the top-level DNS servers responsible for the domains. This procedure is repeated until the name is found or found.

As you can see from the above algorithm, in the network using the DNS protocol, it is possible to introduce an erroneous object – a false DNS server.

Because by default, the DNS service is UDP-based, which does not provide messaging tools, unlike TCP, which makes it less secure.

The following scheme of operation of the erroneous DNS server is possible:

- Waiting for a DNS request.
- Extracting from the received message the necessary information and sending to the host a false DNS response on behalf (from IP address) of the real DNS server and indicating the IP address of the false DNS server in that response.
- When a packet is received from a host, the IP header of the packet of its IP address is changed to the IP address of the fake DNS server and the packet is transmitted to the server. An fake DNS server is running the server on its own behalf.

➢ When a packet is received from a server, it changes the IP header of the packet to its IP address to the fake DNS server address and transmits the packet to the host.

The false DNS server for the host is the real server.

There are two possible options for implementing this attack.

In the first case, a prerequisite is the interception of a DNS request, which requires finding the attacker either in the path of the main traffic, or in the same segment with the DNS server.

In the second case, a directional storm of false prepared DNS responses to the attacked host is created.

On the Internet, when using an existing version of DNS, there is no acceptable solution to protect against a fake DNS server. You can drop the remote search engine and go back to the method with the hosts file, as it was before the DNS service appeared, but so far, this file can only include information about the most frequently visited addresses.

You can also use TCP instead of UDP to make this attack more difficult, although documentation does not always tell you how to do this, and TCP still does not provide complete security.

9. Connecting a False Route Host Using ICMP to Create an Fake Internet Router

Consider another attack related to the introduction of a false object in the DCS. Routing on the Internet is performed on a network layer (IP layer). To provide it in the memory of the network operating system of each host there are routing tables containing information about possible routes.

Each segment of the network is connected to the Internet at least through one router.

All messages addressed to other segments of the network are forwarded to the router, which, in turn, forwards them further to the IP address specified in the packet, while choosing the optimal route.

As mentioned earlier, there is an ICMP management protocol on the Internet, one of the purposes of which is to dynamically modify the routing table of end network systems. Remote routing management is implemented as a transmission to the host of the Redirect ICMP Message.

To perform this attack, you must prepare an fake ICMP Redirect Datagrams for the Host, where you specify the host address to which the route will be changed, and the IP address of the fake router. This message is then transmitted to the attacked host on behalf of the router.

This attack allows you to gain control over the traffic between that host and the server of interest to the attacker if the host and the attacker are in the same segment, or disrupt the host if they are located in different segments.

It is possible to protect against this influence by filtering passing ICMP-messages by the Firewall systems. Another way is to change the network kernel of the OS to prevent the response to the Redirect ICMP message.

10. Changing one of the subjects of a TCP connection on the Internet (hijacking)

TCP (Transmission Control Protocol) is one of the basic protocols of the transport layer of the Internet. It allows you to correct errors that may occur during packet transmission by establishing a logical connection – a virtual channel. This channel is transmitted and received packets with the registration of their sequence, is managed information flow, organized retransmission of distorted packets, and at the end of the session the channel is disconnected. The TCP protocol is the only basic protocol of the TCP/IP family, which has an additional message and connection identification system.

To identify a TCP packet, there are two 32-bit identifiers in the TCP header that also play the role of a packet counter.

Their names are Sequence Number and Acknowledgment Number.

To generate an fake TCP packet, the attacker needs to know the current identifiers for the connection. This means that it is sufficient for it, having selected the corresponding current values of the TCP packet identifiers for the given TCP connection, to send the packet from any host on the Network on behalf of one of the participants of the given connection, and this packet will be perceived as correct.

When finding a cracker and an attack object in the same segment, the task of obtaining the ID values is solved by network traffic analysis. If they are in different segments, you have to use mathematical prediction of the initial value of the identifier by extrapolating its previous values.

To protect against such attacks, it is necessary to use OS, in which the initial value of the identifier is really randomly generated. You must also use secure protocols such as SSL, S-HTTP, Kerberos, etc.

11. Flood of false TCP connection requests

For each TCP connection request received, the operating system must generate the initial value of the ISN and send it in response to the host. Since the Internet (IPv4 standard) does not provide control over the IP address of the sender of the message, it is impossible to track the true route traveled by the IP packet, and therefore, the end subscribers of the network can not limit the number of possible requests received per unit of time from one host. Therefore, a typical Denial of Service attack is possible, which will involve sending as many false TCP requests to the attacked host to create a connection on behalf of any host on the network. At the same time attack the network OS, depending on the computing power of the computer or – in the worst case – almost freezes, or – in the best case – ceases to respond to legal requests for connection (denial of service).

This is because, for the whole mass of fake requests received, the system must, first, store the information received in each request and, second, produce and send a response to each request

Thus, all system resources are "eaten up" by fake queries: the query queue overflows, and the system deals only with their processing.

A new type of attack has recently been reported on the Web. Instead of typical Denial of Service attacks, hackers overflow their corporate router packet buffer, not from single machines, but from as many as thousands of zombie computers.

Such attacks are capable of blocking channels up to and including T3 (44.736 Mbps) and several such cases have already been noted. The risk of attack becomes more important as more businesses use private VPN networks and other Internet technologies. After all, the failure of the channel with a public service provider will not just lead to the shutdown of individual users, but to the halt of huge corporations.

In this case, there are difficulties in determining the source of the attack – erroneous packets come from different unique IPs. "Zombie attack" is called the most difficult of the known. The lone victim is attacked by an entire army, and each zombie hits only once.

There are no acceptable methods of protection against such attacks in the IPv4 network, since it is impossible to control the message route.

To increase the reliability of the system, you can use as powerful as possible computers capable of withstanding the directional storm of erroneous connection requests.

12. Attacks that use network service implementation errors

In addition to these attacks, there are various attacks against specific platforms. example:

Land Attack – An IP packet is formed in which the sender's address matches the recipient's address. All Windows versions of Windows NT 4.0 Service Pack 4, are vulnerable to this vulnerability. When such requests are received, access to the system becomes impossible.

Teardrop and bonk attacks are based on bugs of OS developers in the module responsible for compiling fragmented IP packages. In this case, a block of negative length is copied or "holes" remain in the package after the fragments are assembled – empty, not filled with space data, which can also cause the OS kernel to crash. Both of these vulnerabilities are present in Windows95 / NT before Service Pack 4, including early versions of Linux (2.0.0).

WinNuke – Windows systems attack by sending TCP/IP packets with Out Of Band (OOB) flag to an open (usually 139th) TCP port. Today, this attack is outdated. Early versions of Windows95 / NT were freezing.

There are various other attacks specific to certain operating systems only.

13. WWW Attack

In the last few years, with the rapid development of WorldWideWeb, the number of attacks through the Web has increased significantly. In general, all types of attacks through the Web can be divided into two large groups:

- Attack on the client;
- Attack on the server.

In their development, browsers went very far from the original versions intended only for viewing hypertext. Browser functionality is constantly increasing, now it is already a complete component of the OS. In parallel, there are numerous security issues with the technologies used,

such as plug-ins, ActiveX elements, Java applications, JavaScript scripting tools, VBScript, PerlScript, Dynamic HTML.

Thanks to the support of these technologies, not only browsers but also mail clients and the presence of bugs in them, in the last year or two a large number of email viruses as well as viruses that infect html files (implemented on VBScript using ActiveX). Trojans are very common.

The event of the year was the release of the BackOrifice 2000 Cult of the Dead Cow hacker group, which, unlike the previous version, runs on WindowsNT and is also distributed in source texts, enabling anyone to create a clone of this program for their specific needs, probably cannot be detected by antivirus programs.

Server software security is mainly determined by the absence of the following types of errors:

- server errors:

errors that lead to a loss of privacy; errors that lead to denial-of-service attacks and errors that cause unauthorized code to execute on the server;

- errors in utilities;
- administration errors.

14. Reasons for the success of remote attacks

"What is invented by one person
can be understood by another," – Holmes.
A. Conan Doyle The Adventure of the Dancing Men

Use of unstable identification algorithms. Unfortunately, the interaction of objects on a virtual channel in a distributed CS is not a panacea for all problems associated with the identification of objects of the DCS. VC is a necessary but not sufficient condition for safe interaction. It is extremely important in this case to choose the identification algorithm when creating a virtual channel.

The basic requirement for these algorithms is the following: the interception of key information exchanged by DCS objects when creating VCs should not allow the attacker to obtain summary channel and object IDs.

However, in the basic identification algorithms used in the creation of VC in most existing network OS, this requirement is virtually ignored.

Lack of control over virtual communication channels. Distributed CS objects that interact across virtual channels may be subject to a typical denial of service attack. The peculiarity of this influence is that, acting by absolutely legal means of the system, one can remotely achieve a violation of its performance.

What is the reason for the success of this attack? In the absence of the necessary control over the connection.

The task of control is divided into two sub-tasks:

- control over connection creation;
- control over connection usage.

If the ways to solve the second problem are clear – usually the connection is broken by a timeout defined by the system – so done in all known network OS (but there is a serious problem of choosing a specific timeout value), then control over the creation of VC is quite difficult: In a system where static key information about all its objects is missing, it is impossible to separate false connection requests from real ones.

It is also clear that if one network interaction entity is able to anonymously occupy an unlimited number of channels due to a remote object, then such a system may be completely paralyzed by that entity.

Thus, if any object in a distributed system is able to anonymously send messages on behalf of another object (for example, routers do not check the IP address of the sender), it is virtually impossible to control virtual creation of connections.

Therefore, the main reason for the typical threat of "denial of service" is the lack of an acceptable solution to the task of controlling the message route.

Inability to control the message route. If the DCS does not provide control over the route of the message, then the address of the sender of the message is not confirmed.

Thus, the system will be able to work on behalf of any object by specifying a message in the header of another sender's address (IP Spoofing).

In such a DCS it is difficult to determine where the message actually came from, and therefore to calculate the coordinates of the attacker (the initiator of a unidirectional remote attack cannot be found on the Internet).

Lack of complete information about network objects. In a distributed system with a branched structure consisting of a large number of objects, there may be a situation where the necessary information, that is, the address of the given object, will not be available for access to a particular host.

Obviously, in a system of this type, there is a potential danger of entering an fake object and issuing one object at a time by transmitting an incorrect response to a search query.

No dedicated channel of communication between Internet objects. A global network cannot be built on the principle of direct communication between objects, because for each object it is impossible to provide a dedicated communication channel with any other object. Therefore, the Internet connects through a chain of routers, and therefore, messages passing through a large number of intermediate subnets can be intercepted.

Also, a large number of local Ethernet networks that use the "common bus" topology are connected to the Internet; In networks with this topology, it is easy to programmatically intercept messages.

Insufficient identification and authentication. In the basic protocols of exchange, identification and authentication of objects are virtually absent.

For example, in application protocols – FTP, TELNET, POP3, the user names and passwords are transmitted over the network as unencrypted open messages.

Use of unstable object identification algorithms when creating a virtual TCP connection. As already emphasized, TCP is the only basic transport layer protocol that has connection protection.

However, using the simplest object identification algorithm when creating a virtual TCP channel, especially when the simplest time-dependent TCP generation laws apply to network OSs, nullifies all attempts to provide channel and object identification when interacting with TCP.

No cryptographic protection of messages. The existing TCP / IP core protocols that provide network and transport interactions do not provide the ability to encrypt messages, although it is obvious that adding them to TCP did not pose any problems. The developers have decided to shift cryptographic protection tasks to higher-level

protocols, such as the application layer. The basic application protocols (FTP, TELNET, HTTP, etc.)

They also did not provide any encryption of messages. Just recently, a publicly available SSL application built into browsers has emerged, allowing both secure encryption and authentication of messages.

In conclusion, I would like to point out that all of the reasons described above, for which a successful implementation of the security threats to the DCS is possible, make the Internet unsafe. Therefore, all network users can be attacked at any time.

15. Virtual Private Networks

One of the most important tasks is protecting the flow of corporate data transmitted over open networks. Open channels can be securely protected by only one method – cryptographic.

The so-called dedicated lines do not have special advantages over the public security lines in terms of information security. The selected ones will be located at least in part in an uncontrolled area where they may be damaged or unauthorized.

The only real dignity is the guaranteed bandwidth of the dedicated lines, and not increased security. However, modern fiber-optic channels are able to meet the needs of many subscribers, and therefore the dignity is not always dressed up in a real form.

Of course it is natural to put on the firewall the task of encrypting and decrypting corporate traffic on the way to and from the external network. In order for such encryption/decryption to be possible, an initial allocation of keys must take place.

Modern cryptographic technologies offer a number of methods for this purpose.

After the firewalls have encrypted the closure of corporate data streams, the territorial location of the network segments is detected only at different rates of exchange with different segments. The rest of the network looks like a whole, and subscribers do not need to bring any additional security.

Probably, nowhere the word "virtual" has become as widespread as in the field of information technology: virtual memory, virtual machine, virtual reality, virtual channel, virtual office. This is due to the ability to

simulate the logic of the operation of the object so that for the user its (logical) behavior and properties will not differ from the real prototype.

Escape to the "virtual world" can be caused by, say, a fundamental inability to operate with a real object, economic considerations, or a temporary factor.

Virtual Private Networks (VPNs) are not only a hot topic for industry analysts, but are also receiving close attention from both Network Service Provider (NSP) and Intemet (ISP) providers and corporate users.

Infonetics Research expects the VPN market to grow more than 100% annually by 2002, reaching 12 billion. $ She also reports that 92% of major ISPs and 60% of total ISPs planned to provide VPN services by the end of 1999.

Before proceeding to the analysis of the causes that have caused such a rapid increase in the popularity of VPNs, it should be reminded that simple (corporate) data networks are built, as a rule, using leased (dedicated) public switched telephone networks (Public Switched Telephone Network – PSTN).

Over the years, such private networks have been designed to meet specific corporate requirements, resulting in branded protocols that support proprietary applications (though Frame Relay and ATM have recently become popular).

Dedicated channels allow for reliable protection of sensitive information, but the downside of the coin is the high cost of operation and difficulty in expanding the network, not to mention the possibility of connecting to it by a mobile user at an unpredictable point.

At the same time, modern business is characterized by considerable dispersion and labor mobility.

More and more users need access to corporate information through dial-up channels, and the number of employees working at home is also increasing. Western analysts predict that by the end of 1999, 80% of corporate users will have at least one laptop computer (of course, the projection of this prediction on Ukraine can only cause a smile, but sooner or later the Ukrainian economy, raped by progress, will have to adopt game rules dictated by industrialized countries).

Further, private networks are unable to provide the same business opportunities offered by the Internet and IP-based applications, such as product promotion, customer support or ongoing contact with suppliers.

Such online interaction requires the integration of private networks, which typically use different protocols and applications, different network management systems, and different communications providers.

Thus, the high cost, static and difficulties that arise when necessary to unite private networks based on different technologies, contradict with the dynamically developing business, its desire for decentralization and is a recent tendency to merge companies.

At the same time, there are, at the same time, devoid of these shortcomings of the public data network and the Internet, literally enveloping its "web" with the whole globe. However, they are also deprived of the most important dignity of private networks – reliable protection of corporate information.

Virtual Private Networking technology combines the flexibility, scalability, low cost and availability of virtually anytime anywhere Internet and public-facing networks with the security of private networks. VPNs are essentially private networks that use global public networks (Internet, Frame Relay, ATM) to transmit traffic. The virtuality, however, is that for corporate users, they appear to be dedicated private networks.

Let's look at the basic requirements for virtual private networks.

15.1 Compatibility

Compatibility issues do not arise when Frame Relay and ATM services are directly used by VPNs, as they are well suited for multi-protocol environments and are suitable for both IP and full IP applications.

All that is required in this case is the availability of an appropriate network infrastructure covering the required geographical area. Frame Relay Access Device (FRAD) or routers with Frame Relay and ATM interfaces are most commonly used as access devices. Numerous permanent or switched virtual channels can work (virtually) with any mix of protocols and topologies. It's complicated if a VPN is based on the Internet. In this case, the programs need to be IP-compatible. If this requirement is fulfilled, you can use the Internet as it is to build a VPN, providing the necessary level of security beforehand.

But since most private networks are multi-protocol or use unofficial, internal IPs, they cannot connect directly to the Internet without proper adaptation. There are many compatibility solutions available.

The most popular are:

- converting existing protocols (IPX, NetBEUI, AppleTalk, or others) into an IP protocol with an official address;
- converting internal IPs to official IPs;
- installation of special IP-gateways on servers;
- use of virtual IP routing;
- use of universal tunneling technique.

The first way, at least conceptually, is clear, so let's briefly look at others.

Converting internal IPs to official IPs is required if the private network is IP-based. Class B addresses that are in the range 192.168.0.0 – 192.168.255.255 are typically used for internal addressing, which allows 65536 nodes to be identified.

Address transformation for the entire corporate network is unnecessary, as official IP addresses can coexist with the internal switches and routers of the enterprise network. In other words, the server with the official IP address is still accessible to the private network client through the local infrastructure.

Most often use the technique of sharing a small block of official addresses by many users. It is similar to sharing a modem pool because it also relies on the assumption that not all users need Internet access at the same time.

There are two industry standards: Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT), which differ slightly. DHCP "leases" the node address for the time specified by the set administrator, while NAT translates the internal IP address to the official dynamically, during a session with the Internet.

Another way to make a private network compatible with the Internet is to install an IP gateway. The gateway does not transmit IP protocols to IP protocols and vice versa. Most network operating systems that use native protocols have IP gateway software.

The essence of virtual IP routing lies in the extension of private routing tables and address space to the infrastructure (routers and switches) of the ISP.

A virtual IP router is a logical part of a physical IP owned and operated by service provider. Each virtual router serves a specific group of users.

However, perhaps the best way to ensure compatibility is through tunneling methods. These methods, along with various encapsulation techniques, have long been used to transmit multiprotocol packet flow over a common line.

Currently, this proven technology is optimized for Internet-based VPNs.

The main components of the tunnel are:

- the initiator of the tunnel;
- routed network;
- tunnel switch (optional);
- one or more tunnel terminators.

Tunneling must be performed at both ends of the through channel. The tunnel should begin with a tunnel initiator and end with a tunnel terminator. The initialization and completion of tunnel operations can be performed by various network devices and software. For example, a tunnel can be initiated by a remote computer that has a modem and VPN software needed, a corporate branch front-end router, or a service provider's network access hub.

To transmit packets other than IP network protocols over the Internet, they are encapsulated into IP packets by the source.

The most commonly used method of creating VPN tunnels is to encapsulate the NOT IP packet into the PPP (Point-to-Point Protocol) package, followed by encapsulation into the IP packet. Recall that the PPP protocol is used to connect point-to-point, for example, to communicate with the client server.

The process of IP encapsulation involves adding a standard IP header to the original packet, which is then considered as useful information. The corresponding process at the other end of the tunnel removes the IP header, leaving the original package unchanged.

The PPP protocol provides service at level 2 of the OSI reference model, so this approach is called level 2 tunneling (L2 Tunneling Protocol – L2TP).

Today, the Point-to-Point Tunneling Protocol, developed by 3Com and Microsoft, which comes with Windows 95 and Windows NT operating systems, has become quite widespread.

Because tunneling technology is quite simple, it is also the most cost-effective.

15.2 Security

Providing the right level of security is often a key consideration when considering a corporation's ability to use a Intemet-based VPN. Many IT managers have become accustomed to the inherent privacy of private information security networks and consider the Internet as too "public" to use as a private network.

However, if the necessary steps are taken, Intemet-based virtual private networks can become more secure than PSTN-based VPNs.

If you use English terminology, there are three "P", the implementation of which together provides complete protection of information:

- Protection – protection of resources by means of firewalls;
- Proof – authentication (integrity) of the package and authentication of the sender (confirmation of the right of access);
- Privacy – protect sensitive information through encryption.

All three P's are equally relevant to any corporate network, including VPN. In purely private networks, it is enough to use simple passwords to protect the resources and confidentiality of information.

Once a private network connects to a public network, none of the three P's can provide the necessary protection. Therefore, for any VPN, firewalls must be installed at all points of its interaction with the public network, and packets must be encrypted and authenticated.

Firewalls are an essential component in any VPN. They skip only authorized traffic for trusted users and block all other traffic. In other words, all attempts to reach unknown or untrusted users intersect.

This form of protection should be provided for each site and user, since the lack of it anywhere means the absence of everywhere.

Special protocols are used to ensure the security of VPNs. These protocols allow hosts to "agree" on the encryption and digital signature technique used, which preserves the confidentiality and integrity of the data and performs user authentication.

Microsoft Point-to-Point Encryption (MPRE) encrypts PPP packets on a client machine before sending them to a tunnel. The 40-bit key version comes with Windows 95 and Windows NT (there is also a 128-bit key version). The encryption session is initialized during communication with the PPP tunnel terminator.

Secure IP (IPSec) protocols are a series of previous standards developed by the Internet Engineering Task Force (IETF). The group

offered two protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP).

The AH protocol adds a digital signature to the header that authenticates the user and ensures the integrity of the data by tracking any changes in the transmission process. This protocol only protects data, leaving the IP address packet unchanged.

ESP, on the other hand, can either encrypt the entire packet (Tunnel Mode) or only the data (Transport Mode). These protocols are used both individually and in combination.

Security management uses the industry standard RADIUS (Remote Authentication Dial-In User Service), which is a database of user profiles containing passwords (authentication) and permissions (authorization).

Security measures are not limited to the following examples. Many router and firewall vendors offer their solutions. These include 3COM, Checkpoint and Cisco.

15.3 Availability

Availability includes three equally important components: service time, bandwidth, and delay time. Service time is the subject of a contract with a service provider, and the other two components are related to the elements of Quality Of Service.

Modern transportation technologies allow you to build VPNs that meet the requirements of virtually all existing applications.

15.4 Controllability

Network administrators always want to be able to manage end-to-end, corporate networking, including the part that relates to a telecommunications company, and it turns out that VPNs provide more power than conventional private networks.

Typical private networks are administered from border to border, that is, the service provider manages the network to the front routers of the corporate network, while the subscriber manages the corporate network to the WAN access devices.

VPN technology avoids this peculiar separation of "spheres of influence" by providing both the provider and the subscriber with a unified system for managing the network as a whole, both its corporate part and the network infrastructure of the public network.

The enterprise network administrator has the ability to monitor and reconfigure the network, manage front-end access devices, and determine the network status in real time.

REFERENCES

1. Крол Эд. Все об Internet: Руководство и каталог. Пер. с англ. С.М. Тимачева. Киев: BNV, 1995. 591 с.

2. Вертузаев М.С., Юрченко О.М. Защита информации в компьютерных системах от несанкционированного доступа. Київ: Европ. ун-т, 2001. 320 с.

3. Ярочкин В.И. Основы защиты информации. Москва: Летописец, 2000. 150 с.

4. Зепкды П.Д. Теория и практика обеспечения информационной безопасности. Под ред. Москва: Яхтсмен, 1996. 302 с.

5. HackZone- территория взлома (httn://www.hackzone.ru).

Information about the author:
Domnich V. I.
Candidate of Technical Sciences, Professor,
Head at the Department of Automated Process Control
of the V. I. Vernadsky Taurida National University

DOI https://doi.org/10.36059/978-966-397-104-9/118-138

INFORMATION PROTECTION

Domnich V. I.

1. Information security issues

Internet and information security are incompatible by nature. It was born as a purely corporate network, but now, through a single stack of TCP / IP protocols and a single address space, it connects not only corporate and departmental networks (educational, government, commercial, military, etc.), which is by definition, restricted networks, but also ordinary users who are able to access the Internet directly from their home computers through modems and a public telephone network[1].

It is known that the easier access to the Web, the worse its information security, so it is reasonable to say that the original ease of access to the Internet – worse then theft, because the user may not even know that they were copied – files and programs, not to mention the possibility of spoiling and correcting them.

What determines the rapid growth of the Internet, which is characterized by an annual doubling in the number of users? The answer is simple – "freebie", that is, cheap software (TCP / IP), which is now included in Windows 95, ease and cheap access to the Internet (either by IP address or provider) and to all the world's information resources.

Paying for the use of the Internet is a general reduction of information security, so to prevent unauthorized access to their computers, all corporate and departmental networks, as well as enterprises using the Internet technology, put filters (firewall) between the internal network and the Internet, which in fact means leaving the single address space.

Even greater security will be given away from TCP/IP and access to the Internet through gateways.

This transition can be done simultaneously with the process of building a worldwide public information network, based on the use of network computers, which, using a 10Base-T network card and cable modem, provide high-speed access (10 Mbps) to a local Web server via a cable network TV.

[1] Библиотека Сетевой Безопасности URL: http://securitv.tsu.ru.

To address these and other issues when transitioning to the new Internet architecture, you must provide the following:

First, to eliminate the physical connection between the future Internet (which will become the World Wide Web Information Organization) and corporate and departmental networks by retaining only an information link through the World Wide Web.

Second, replace the routers with switches by switching off processing at the nodes of the IP protocol and replacing it with Ethernet frame broadcast mode, in which the switching process is reduced to a simple MAC address comparison operation.

Third, to move to a new single address space based on physical access points to the transmission medium (MAC layer), tied to the geographical location of the network, and within 48-bits to create addresses of more than 64 trillion nodes.

Data security is one of the major problems on the Internet. More and more scary stories are emerging about how hackers, using increasingly sophisticated techniques, get into other people's databases. Of course, all this does not contribute to the popularity of the Internet in business.

The mere thought that some hooligans, or worse, competitors, will be able to access commercial data archives is forcing corporate executives to refuse to use open information systems.

Experts say such fears are unfounded because companies with access to both open and private networks have almost equal chances of becoming victims of cyber terror.

Every organization that deals with whatever values are facing their encroachment sooner or later. The prudent start planning protection in advance, the unpredictable – after the first major "puncture". One way or another, the question arises as to what, how and from whom to protect.

Usually the first reaction to a threat is the desire to hide the values in an inaccessible place and to protect them. This is relatively straightforward when it comes to values that you don't need for a long time: taken away and forgotten. It is much more difficult if you need to work with them constantly.

Each request to the store for your values will require a special procedure, will take time and will create additional inconvenience. This is the security dilemma: you have to choose between the security of your property and its accessibility to you, and therefore the ability to use it.

All this is true in relation to information. For example, a database containing sensitive information is only then fully protected against encroachment when it is on disks removed from the computer and stored in a secure place.

Once you have installed these disks on your computer and started using them, there are several channels at which the attacker, in principle, has the opportunity to access your secrets without your knowledge. In other words, your information is either inaccessible to anyone, including you, or not 100 percent secure.

It may seem that there is no solution to this situation, but information security is the same as maritime security: both are possible only with some tolerable degree of risk.

In the area of information, the security dilemma is worded as follows: one must choose between the security of the system and its openness. It is more correct, however, to speak not of choice but of balance, since a system that does not possess the property of openness cannot be used.

In the banking sector, the problem of information security is complicated by two factors: first, almost all the values that the bank deals with (except cash, etc.) exist only in the form of one or another information. Secondly, a bank cannot exist without connections with the outside world: without customers, correspondents, etc. At the same time, the information that expresses the values with which the bank works (or information about these values and their movements, which sometimes cost more than the values themselves) is necessarily transferred from the links.

Documents are coming in from outside which the bank transfers money from one account to another. Outside, the bank sends orders to move funds to correspondent accounts, so that the bank's openness is set first.

It should be noted that these considerations hold true not only for automated systems, but also for systems built on traditional paper-based circulation and utilizing links other than courier mail.

Automation has added a headache to security services, and new developments in the banking industry, based entirely on information technology, are compounding the problem.

2. Basic methods of protection against remote attacks on the Internet

The simplest and most inexpensive are the administrative security methods: the use of persistent cryptography, static ARP tables, hosts files

instead of dedicated DNS servers, the use or non-use of certain operating systems, and other methods.

The following group of remote attack protection methods are firmware:

- network hardware encryption hardware;
- Firewall methodology;
- secure network crypto protocols;
- attack detection software (IDS – Intrusion Detection Systems or ICE – Intrusion Countermeasures Electronics);
- security analysis software tools (SATAN – Security Analysis Network Tool for Administrator, SAINT, SAFEsuite, RealSecure, etc.);
- secure network OS.

In general, the Firewall technique implements the following basic functions:

- multi-level filtering of network traffic; Proxy schema with additional authentication and user authentication on the Firewall host. The meaning of a proxy scheme is to create a connection to a destination through an intermediate proxy server on a Firewall host;
- creating private networks with "virtual" IPs. Used to hide the true topology of the internal IP network.

Here you can distinguish a subset of security methods – software methods. These include primarily crypt protocols, which can improve the security of connection protection.

3. Modern cryptographic methods

3.1 Introduction to Cryptography

The rapid development of cryptographic systems were during the first and second world wars. From the postwar period to the present day, the advent of computing has accelerated the development and improvement of cryptographic methods[2].

The problem of using cryptography methods in information systems is now particularly urgent because, on the one hand, the use of computer networks, in particular the global Internet network, through which large amounts of information of state, military, commercial and private nature

[2] An Introduction to Computer Security: The NIST Handbook. Draft. – National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1994. 310 c.

are transmitted, does not allow access to it bystanders. On the other hand, the emergence of new powerful computers, network and neural computing technologies has made it possible to discredit cryptographic systems, which have recently been considered virtually undisclosed.

The problem of information protection through its transformation is addressed by cryptology (kryptos – secret, logos – science).

Cryptology is divided into two areas – cryptography and cryptanalysis. The purpose of these directions is the exact opposite.

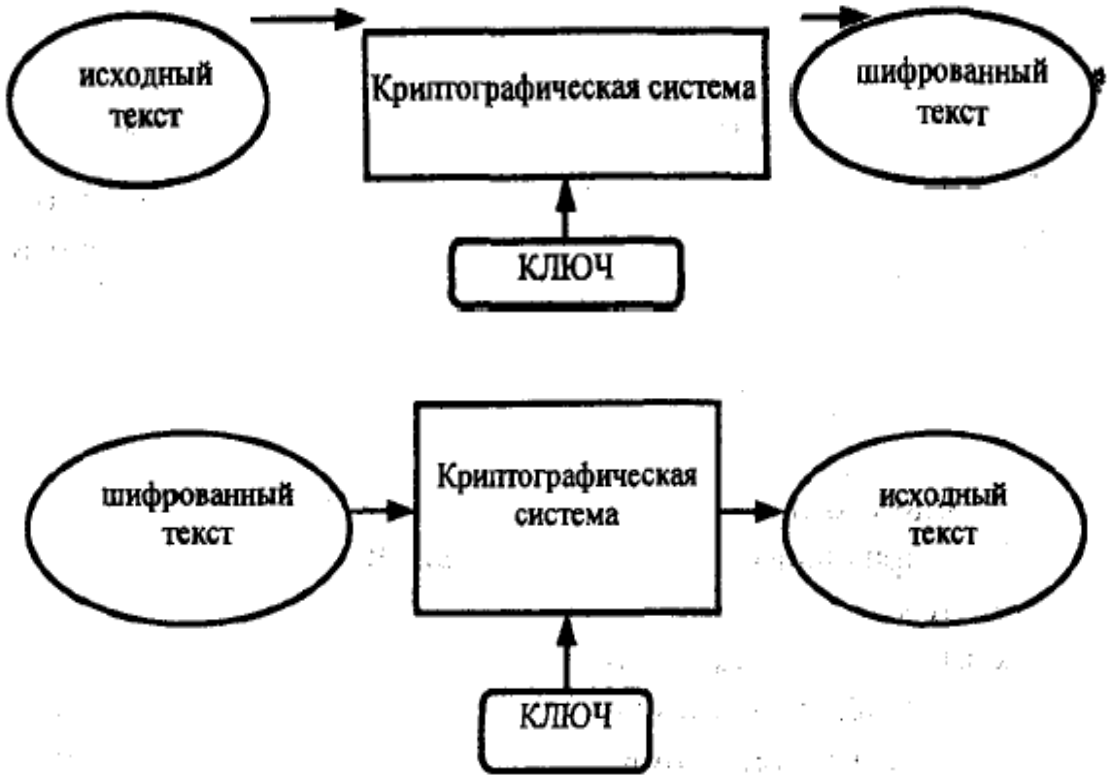
Cryptography deals with the search and research of mathematical methods of information transformation.

The area of interest of cryptanalysis is exploring the possibility of decrypting information without knowing the keys. "

Encryption is a transformative process: the source text, also called plaintext, is replaced by encrypted text.

Decryption is the reverse of the encryption process. Based on the key, the digitized text will be converted to output. Based on the key, the digitized text will be converted to output.

The key is the information needed to seamlessly encrypt and decrypt texts.



Cryptosystems are divided into symmetric and public key systems. In symmetric cryptos, the same key is used for both encryption and decryption.

Public key systems use two keys, public and private, that are mathematically related to each other. The information is encrypted with a public key accessible to all comers and decrypted with a private key known only to the recipient of the message.

An electronic (digital) signature is called text-encrypted conversion, which, when received by another user, verifies the authorship and authenticity of the message.

Crypto-stability is called the characteristic of a cipher, which is its resistance to decryption without knowing the key (ie cryptanalysis). There are several indicators of crypto-stability, including: the number of all possible keys; the average time required for cryptanalysis.

In the past, cryptography was only used for military purposes. But now, with the emergence of the information society, it is becoming a central tool for privacy.

As the information society is formed to the great powers, technological means of total surveillance of millions of people become available. Therefore, cryptography is becoming one of the main tools for securing privacy, trust, authorization, electronic payments, corporate security and countless other important things.

Encryption details. Encryption is the reverse conversion of data to hide them from third parties. Encryption methods have been devised in many ways – from simple-to-replace ciphers (the most famous example is Conan Doyle's "Dancing Men") to the Vernam cipher (binary addition of source text with a single random sequence).

Almost all encryption methods use the encryption key, a secret code sequence that is used in the information conversion process. Somewhere even read the following definition of encryption: "Encryption is the process of replacing your big secret (document) with a small one (key)."

If Vernam encryption is used, the encryption key is the length of the encrypted message, and must still be used once. Although Vernam's cipher, when properly used, provides "absolute" secrecy, it is not convenient for most applications. Modern cryptosystems use a key to encrypt 64 to 1024–2048 bits in length.

The tradition of measuring the key length in bits will probably stay with us forever. The question is – where did these figures come from, and why is TripleDES considered to be no less reliable than the 1024-bit RSA? And in general, how does the reliability of encryption (or, as they say, the stability of the cipher) depend on the length of the key used?

In order to answer these questions, you need to understand what encryption algorithms are currently used in practice. Generally, "classical ciphers" are called symmetric block ciphers. That is, those who use the same key to encrypt and decrypt information and encrypt information with blocks. The block length is usually 8 or 16 bytes.

There are algorithms that allow for variable block length. The first block cipher, widely used in practice, became DES (Data Encryption Standard), developed by IBM specialists in the early 70's of the last century and for a long time served as the standard for encryption of data in the United States. Then came many block algorithms – IDEA, Blowfish, Soviet GOST 28147-89 (and now is the Russian standard).

The original DES, for example, used a 112-bit key and a 64-bit encryption block. But after its analysis by NSA experts, the key length was reduced to 64 bits. In the key, there were only 56 bits of unique, and 8 bits of control, employees to control the integrity of the key. It is with a key length of 56 bits DES and has been approved as the National Standard.

At the same level of development of computers, the task of sorting 256 keys in an acceptable time was either technically not feasible or unreasonably expensive. Currently, a DES with a key length of 56 bits does not seem to be a stable algorithm.

Most modern symmetric algorithms use a key length of 64–256 bits (8–32 bytes). The following are the main currently used algorithms, their block lengths and key lengths.

Алгоритм	Длина ключа (в битах)	Длина блока (в битах)
DES	64	64
Blowfish	Переменная до 448 бит	64
IDEA	128	64
ГОСТ 28147-89	256	64
RC5	Переменная	Переменная

It should be noted that in addition to block ciphers, streaming ciphers exist and are being actively used. They, like block ciphers, use a symmetric key, but they encrypt the input stream byte or, sometimes, byte.

The idea behind the current cipher is that a symmetric key produces a key sequence, or a gamma sequence, which is modulated with an input stream. Streaming encryption is typically more productive than block cipher and is used to encrypt language, network traffic, and other data of a previously unknown length. With a fairly frequent change of key to produce gamma, the stream ciphers provide sufficient stability.

In particular, GSM-standard mobile communication provides the ability to encrypt the transmitted voice stream at a site from the telephone to the base station with a cipher that is streamed by it. One instructive story is associated with this algorithm. Initially, the description of the algorithm was closed. But due to a legal error of the company that owns the algorithm, its description has hit the Internet and the algorithm has been analyzed. Its resistance was even lower than that of DES.

Recognizing the importance of openness of algorithms to ensure their stability, developers of the third generation of GSM network have promised to make the proposed algorithms for voice encryption be acquired by the general cryptographic public. The example shows the importance of having an open description of the algorithm, even for its developers.

To date, algorithms with a key length of 64 bits or more provide acceptable stability.

The use of asymmetric cryptography radically simplifies the process of key distribution. The public key was therefore called "public" that it is no secret.

You can create a public "public key directory" where you can place the public keys of all participants in the exchange. In this case, each key owner is free to withdraw his key from the directory or replace it – this procedure will not affect the other participants of the exchange. This raises the problem of the authenticity of the key in the directory, but it is solved. But for convenience, you have to pay.

In the case of asymmetric cryptography, the key is the time and length of the keys. The characteristic length of the keys is when using asymmetric cryptography – 512–1024 bits. Now that high-performance computing systems are available, the use of 2048-bit keys is gaining popularity.

Is it possible to shorten the encryption time by keeping the asymmetric cryptography handy and adding block cipher speed? It turns out you can. They usually come as follows: produce a random (or pseudorandom) sequence and use it as a one-time (so-called session) key to encrypt a document with a fast symmetric algorithm. Then, using an asymmetric algorithm, they encrypt the session key and transmit it in encrypted form with the document.

When decrypting a document, first decrypt the session key, and then the document itself.

Because the session key is of small length, it takes a little time to encrypt it. Currently used symmetric crypto algorithms have a performance of about megabytes per second (for software implementations) and tens of megabytes when using specialized cryptoprocessors.

Asymmetric algorithms show performance from one to tens of kilobytes per second, depending on the length of the key. With a session key of 8-32 bytes, such a hybrid crypto scheme is quite effective.

3.2 A brief description of the basic data encryption algorithms

What is Blowfish? Blowflsh is a 64-bit block cipher developed by Schneier in 1993. This is a Feistel cipher and each pass consists of a permutation key dependent and a replacement key dependent. All operations are based on XORs and additions on 32-bit words.

The key has a variable length (max 448 bits) and is used to generate multiple subkey arrays. The cipher was created specifically for 32-bit machines and significantly faster DES.

In 1994, Dr. Dobb magazine sponsored an open competition with a $ 1,000 prize. This competition ended in April 1995 and several weak keys were found among the results. However, Blowfish may be considered secure, and Schneier invited crypto-analysts to continue investigating his code.

What is DES? DES (Data Encryption Standard) was announced in 1977 by the US National Bureau of Standards and was formally recognized as a result of the work of Subcommittee X3.92 of the US National Institute of Standards in 1981 (ANSI X3.92-1981, American National Standards Data Encryption Algorithm, © American National Standards Institute, 1981).

DES's status as a US national standard has aroused wide interest from both equipment developers and cryptographer theorists around the world. DES is based on national standards in some other countries of the world, such as Australia – Australian Standard AS2805.5-1985.

DES has penetrated and is widely used in Russia as an integral part of various software and hardware, of which the most widely known are the S.W.I.F.T. system, VISA and EUROPAY secret modules, ATMs and trading terminals, and, finally, smart cards.

Particularly intense debate over data encryption algorithms is caused by smart cards. However, there are good reasons to believe that the reliability of Russian cryptosystems of conversion origin will be superior to foreign counterparts.

DES's mathematical studies are devoted to thousands of huge investments. The general conclusion that can be drawn from open publications is that today DES sufficiently satisfies the requirements of reliability and there are no known methods of its direct reading (decryption) when fulfilling the relevant requirements for keys.

A little excursion into theory. The encryption algorithm is the implementation of some ambiguous mathematical function of converting one data (open) to other data (closed). This conversion is performed on the basis of some exclusively secret data – encryption keys, which are only owned by members of the secret correspondence. If the encryption algorithm itself is not a secret, and moreover, widely published, it is clear that the reliability of the secret is equivalent to the reliability of storage and use of keys.

All this is correct with one very important caveat – the algorithm itself must be a "very random" function and not generate a direct or statistical dependence of the closed data on the source-open data. This, in fact, is the mathematical understanding of crypto reliability.

Stability is an exceptionally broad concept, the number of which is considered to be the number of mathematical operations that can be read with certainty to read this encrypted message. It is clear that knowing the time of one elementary operation, you can calculate how much time, money, computers, etc. will be necessary for the attacker to acquire secret knowledge.

Let's look at a specific type of DES – encryption on keys 56 bits long (in fact – 8 bytes, but every lower bit – checks and is not used in

encryption). Since we seem to have tuned in to crack this code, then we will arm ourselves with a calculator and figure out what we will do.

Output: You should try to decrypt your existing encrypted text into 2^{56} possible key variants, that is, perform DES decryption approximately 10^{15} times.

Since the DES operation is long enough, we will immediately have a dedicated processor that performs 105 DES operations in 1 sec. priced at $ 20 per chip. Breaking the ciphers is serious, so let's build a computing system with thousands of such chips.

The result: a simple calculation shows that it will take us 10 million seconds to operate such a system, that is, about 3,000 hours. The code is broken for a total of 115 days.

You can doubt the possibility of creating the described cryptosystem, however, jokes aside, for the skeptics, here's a help: someone Matsui made a successful attack on a one-time DES, the code was broken 50 days later with 12 workstations HP 9735. Special methods of theoretical stability reduction were applied.

Modern cryptography assumes that the cipher, which can be broken by such available means, is not theoretically stable. The masses here are the main reasons, the most important of which is the current trend of increasing the power of computer systems.

A tragedy could be worldwide if it were not purely practical considerations: is information worth more than decrypting it; when the information is still decrypted, will it cost anything at all; just to take possession of the encrypted information, etc. However, the thoroughness and well-known maximism of the Russian cryptocurrency market contributed to the unambiguous conclusion: DES with a key length of 56 bits is virtually stable.

The same conclusion, but back in 1988, was made by experts of the French company NET1 Products Serge Bellamant and Andre Mansvelt when designing patented technology of cashless payments on the basis of smart cards under the name U.E.P.S. They also offered a way out – twice the consistent use of DES on a key pair.

This approach does not greatly increase the encryption time (which is important for a low-power smart card processor), but allows for very good theoretical stability – 2^{112}.

A simple calculation shows that if in our engineered super system each chip will perform 10 million DES operations in 1 second, then the whole process will take 25 thousand times for 10 billion years. In such cases, cryptographers who are satisfied with the result prefer to express themselves in space categories, for example, during periods of life of the solar system. It should be emphasized that sequential encryption on the same keys practically does not increase stability, since the number of key-search options does not change.

Double DES looks very attractive and maybe it would be enough. However, how to deal with systems still using one-time encryption, how to ensure the compatibility of key distribution schemes and hardware solutions? A rather original answer was found. Recently, the standard of encryption – the triple DES on a key pair – has been de facto established.

The idea of using a triple DES with a key pair is very simple: if the keys are the same, then the encryption result is equivalent to a single encryption. This ensures full compatibility with existing key distribution and use systems on both single and dual DES. (Double DES – single use sequential application).

According to the Center for Democratic Technology (CDT) February 13, 1995, a new triple-DES standard is being developed by the Accredited Standards Committee (ASC) Subcommittee X9, which implements data protection standardization in the US financial and banking field. In addition, AT&T and VLSI Technologies, major developers of custom hardware and hardware, have announced plans to build triple-DES applications.

It can be noted that the leading world manufacturer of smart cards GEMPLUS International has already announced the transition to a new standard for triple DES encryption for a new line of their products – the MPCOS series cards.

What practical conclusions can be drawn?

If the keys are stored securely and the key length (key pair) is 112 bits, then the DES encryption algorithm provides sufficient stability.

Triple DES encryption for a pair of stability keys does not exceed double encryption for the same pair and provides full compatibility with both single and dual DES. Triple DES has become the de facto standard for protecting information in the banking and financial fields.

What is DES with independent subkeys?

DES allocates from the 56-bit key entered by the user 16 48-bit keys for use in each of the 16 permutations. It is interesting to compare the effect when using a 768-bit key (divided into 16 48-bit connectors) instead of using 16 dependent keys created by the key mode in the DES algorithm.

When using independent keys, the number of attempts required to exhaustively search for keys will increase significantly. Changing the cipher will only cause a slight increase in the stability of the cipher against differential and linear cryptanalytic attacks than in conventional DES. It was open to bits (Bitham).

What is IDEA?

IDEA (International Data Encryption Algorithm) is the second version of the block cipher developed by K. Lai D. Massey in the late 80's. This is a cipher consisting of 64-bit sequences of blocks with a 128-bit key and eight rounds. Although this encryption code is not Feistel encryption, decryption is performed on the same principle as encryption.

The cipher structure was designed for easy implementation both software and hardware, and IDEA security is based on the use of three incompatible types of arithmetic operations over 16-bit words. The IDEA software speed is comparable to the DES gray.

One of the principles of IDEA creation is to complicate differential cryptanalysis. Also, not one linear cryptanalytic attack ended successfully, as no algebraic weaknesses were identified.

The most comprehensive analysis was conducted by Daemen. It opened a large class of 2 ^ 51 weak keys, which, when used in the encryption process, the key can be detected and updated. Since there are 2 ^ 128 possible key variants in IDEA, this opening does not affect the practical security of the cipher.

What is RC5?

RC5 is a fairly fast block cipher developed by Rivest for RSA Data Security. This parameter algorithm, that is, with variable block size, key length, and variable number of passes. The block size can be 32, 64 or 128 bits. The number of passes in the range from 0 to 2048 bits. Parametric of this kind gives flexibility and efficiency of encryption.

RC5 consists of key expansion, encryption and decryption.

When entering the key, the number of passes, block size, etc. are also entered. Encryption consists of 3 primitive operations: compilation, bit XOR and rotation. The exceptional simplicity of the RC5 makes it easy to

use, and the RC5 text, as well as the RSA, can be added to the end of the email in encrypted form.

RC5 security is based on data-dependent interleaving and mixing of the results of various operations. An RC5 with a block size of 64 bits and 12 or more passes provides good stability against differential and linear cryptanalysis.

What is RSA?

RSA (authored by Rivest, Shamir and Alderman) is a public-key system designed for both encryption and authentication; was developed in 1977. It is based on the difficulty of decomposing very large integers into prime factors. RSA is a very slow algorithm.

For comparison, at the software level DES is at least 100 times faster than RSA, on hardware 1,000-10,000 times, depending on the execution.

What is GOST 28147-89?

GOST 28147-89 is a standard adopted in 1989 in the Soviet Union and established an algorithm for encrypting data that constitutes state secrets. The history of this algorithm is a mystery. According to the witnesses involved in its implementation and use of people, the algorithm was developed in the 70-ies in the 8th General Directorate of the KGB of the USSR, at that time it had the stamp " Top Secret». Then the mark was reduced to "Secret", and when in the 89th year the algorithm was conducted through the State Standard and became the official state standard, the mark was removed from it. In the early 1990s, it became fully open.

GOST provides 3 modes of encryption (simple replacement, gamification, gamble with feedback) and one mode of imitation insertion. The first of the encryption modes is intended to encrypt key information and cannot be used to encrypt other data; two other encryption modes are provided.

The mode of production of the simulation insert (cryptographic control combination) is intended for imitation protection of encrypted data, ie for their protection against accidental or deliberate unauthorized changes.

The algorithm is built on the same principle as DES – a classic block cipher with a private key – but differs from DES'a longer key length, a large number of rounds and a simpler scheme for constructing the rounds

themselves. Below are its main parameters, for convenience – compared to the parameters DES'a:

1. Размер блока шифрования	64 бита	64 бита
2. Длина ключа	256 бит	56 бит
3. Число раундов	32	16
4. Узлы замен (S-блоки)	Не фиксированы	Фиксированы
5. Длина ключа для одного раунда	32 бита	48 бит
6. Схема выработки раундового ключа	Простая	Сложная
7. Начальная и конечная перестановки битов	Нет	Есть

Due to the much longer length of the GOST key, the DES'a is much more resistant to opening by "brute force" – by a complete search of the set of possible values of the key.

The GOST encryption function is much simpler than the DES'a encryption function, it does not contain bit permutations that are plentiful in DES and which are extremely ineffectively implemented on modern universal processors (though very simple in hardware). Because of that, with twice as many rounds (32 vs. 16), the software implementation of GOST on Intel 86 processors is more than 2 times higher than the DES'a implementation. Naturally, close to the optimum in speed of implementation were compared

Of the other differences GOST from DES'a note the following.

Each round of encryption uses a "round key", in DES'a it is 48-bit and is produced by a relatively complex algorithm that includes bit permutations and table replacements, in GOST it is taken as a fragment of the encryption key.

GOST encryption key length is 256 bits, round key length is 32 bits. Together we get that the GOST encryption key contains 256/32 = 8 round keys. In GOST 32 round, therefore, each round key is used 4 times, the order of use of round keys is set in the GOST and different for different modes.

The GOST Replacement Table – an analogue of DES'a blocks – is an 8x16 table (matrix) containing a number from 0 to 15. In each row, each of the 16 numbers must meet exactly once.

Unlike DES'a the table of changes in GOST is the same for all rounds and is not fixed in the standard, but is a changeable secret key element. The quality of this table depends on the quality of the cipher.

With a "strong" table, the substitution of the stability of the cipher does not fall below some permissible limit even in the case of its disclosure. Conversely, using a "weak" table can reduce the cipher's stability to an unacceptably low limit.

No information on the quality of the table of substitutions in the open press of Russia has been published, but the existence of "weak" tables is not in doubt – an example is the "trivial" table of replacement, each of which is replaced by itself. This makes it unnecessary for the competent authorities of Russia to limit the length of the key – you can simply put an insufficiently "strong" replacement table.

GOST, unlike DES'a, does not have the initial and final bit permutations of the encrypted block, which, according to some experts, do not significantly affect the stability of the cipher, although affect (downward) on the effectiveness of its implementation.

What is Encryption function?

Many algorithms, including DES and GOST, are built on the same principle: the encryption process consists of a set of rounds and steps are performed at each step. The input block is divided into halves (L) and younger (R).

The value of the encryption function from the younger part (R) and the round key (k) X = f (R, k) is calculated.

The function used at this stage is called the ROUND ENGINE FUNCTION. It can be one for all rounds or one for each round. In the latter case, the encryption functions of different rounds of the same cipher differ, as a rule, only in detail.

The output block is formed, its upper part is equal to the younger part of the input block L '= R, and the younger part is the result of performing a bitwise OR operation (denote it (+)) for the older part of the input block and the result of calculating the encryption function R' = L (+) f (R, k).

Symmetric cryptosystems. All the variety of existing cryptographic methods can be reduced to the following transformation classes (see diagram).

Mono- and poly-alphabet substitutions.

The simplest kind of transformation is to replace the source characters with others (of the same alphabet) by a more or less complicated rule.

The simplest kind of transformation is to replace the source characters with others (of the same alphabet) by a more or less complicated rule.

Permutations. Also a simple method of cryptographic transformation. It is usually used in combination with other methods.

Gamming. This method is to overlay the output of some pseudo-random key-generated sequence.

Block ciphers. Represents a sequence (with possible repetition and alternation) of the basic methods of conversion, applied to the block (part) of the ciphertext. Block ciphers are more common in practice than "pure" transformations of a particular class due to their higher cryptocurrency. Russian and American encryption standards are based on this particular class of ciphers.

3.3 RSA algorithm

If cryptographic systems were not sophisticated and reliable – their weak point in practical implementation – the problem of key distribution.

In order for confidential information to be exchanged between two IP entities, a key must be generated by one of them and then transmitted in confidence to the other. That is, in general, the transfer of the key again requires the use of some cryptosystem.

Public key systems were proposed to solve this problem based on the results obtained from classical and modern algebra.

The essence of them is that each IP addressee generates two keys that are linked by a specific rule.

One key is declared public and the other is private.

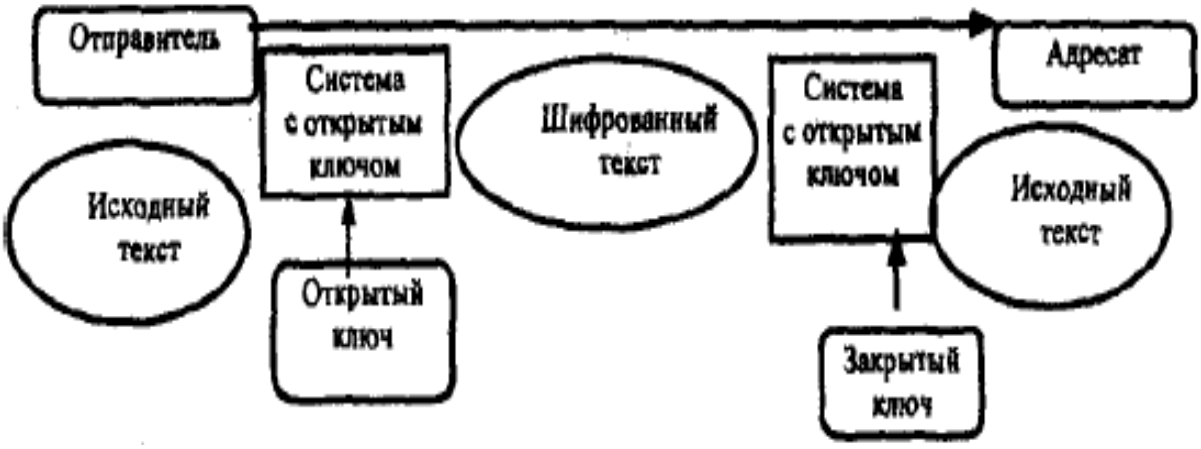
The public key is published and accessible to anyone who wishes to send a message to the addressee. The secret key is kept secret.

The source text is encrypted with the public key of the recipient and transmitted to him. Encrypted text cannot, in principle, be decrypted with the same public key.

The message can only be decrypted using a private key known only to the recipient.

Asymmetric cryptographic systems use so-called irreversible or one-sided functions that have the following property: given a value of x it is relatively simple to calculate the value of *f(x)*, but if *y= f(x)*, there is no easy way to calculate the value of *x*. Public key encryption algorithms are widespread in modern information systems.

Yes, the RSA algorithm has become the worldwide de facto standard for open systems.



Open-key cryptosystem algorithms can be used for three purposes:

1. Independent means of protection of transmitted and stored data.
2. Funds for key distribution.
3. User authentication tools.

Algorithms for public-key cryptosystems are more time consuming than traditional cryptosystems, so using them as standalone shields is irrational. Therefore, in practice, it is rational to distribute keys with a small amount of information as public information using cryptosystems. And then, using conventional algorithms, exchange large information flows.

Despite the large number of different open-key cryptosystems, RSA is the most popular cryptosystem, developed in 1977 and named after its creators: Rivest, Shamir, and Eidelman.

They took advantage of the fact that finding large prime numbers in the computational relation is easy, but decomposing the product of the product of two such numbers is almost impossible.

It has been proved (Rabin's theorem) that the disclosure of the RSA cipher is equivalent to such a decomposition. Therefore, for any length of the key, you can give a lower estimate of the number of operations to open the cipher, and given the performance of modern computers to estimate and the time required.

4. Internet: The evolution of the protection philosophy

The problem of information security on the Internet is posed and, with varying degrees of efficiency, is solved since the advent of networks based on TCP/IP family protocols.

In the evolution of security technologies, there are three main areas.

The first is the development of standards that implement certain network remedies, primarily administrative ones. An example is the IP security option and TCP / IP protocol variants used by the US Department of Defense.

The second direction is the culture of firewalls, long used to regulate access to subnets.

Third, the youngest and most actively developing direction is the so-called virtual secure network technologies (VPN, virtual private network, or Intranet).

The explosive rise in popularity of the Internet and related commercial projects in recent years has been the impetus for the development of a new generation of information security technologies on TCP/IP networks. Moreover, if earlier, up until the early 90's, the main task of protecting the Internet was to conserve resources mainly from hacker attacks, then nowadays the task of protecting commercial information becomes urgent.

Qualitatively, these are completely different types of protection. Attacking commercial information can entail high costs for hacking security and, therefore, significantly higher levels of traffic surveillance, information capture, cryptanalysis, and various types of imitations, diversions, and fraud.

Naive security methods, such as requesting a password and then forwarding it publicly over a communication channel and access lists on servers and routers, become ineffective under these conditions.

What can be contrasted with a skilled and technically armed attacking party? Of course, only a complete, cryptographically secure system.

There are a lot of offers of such means on the Internet market. However, for a number of parameters, none of them can be recognized as an adequate task of protecting information for the Internet.

For example, crypto-resistance and the great idea of forming a "web of trust" is the widespread PGP (Pritty good privacy) system. However, since PGP provides file encryption, it can only be used where file sharing is possible. It is difficult to protect online applications using PGP, for example.

In addition, the PGP security level is too high. Joining PGP protection with other applications requires some efforts, if of course it will prove feasible.

The choice of information security technology for a large open system – the Internet scale, large corporate network, communication network provider – must meet a number of specific requirements:

- the presence of an open specification, the absence of monopoly over technological solutions;
- wide scalability of solutions on technical and price parameters, versatility of technology, portability, multi-platform, compatibility of hardware, software, communication solutions;
- providing, where appropriate, comprehensive information security, ease of key management and secure communications for newly connected users.

Full use of the server requires its connection through a local router, which will become one of the security frontiers. The router can be programmed in such a way that it will block dangerous functions and allow the transmission of incoming requests from outside to dedicated servers only.

Partial protection is provided by port blocking, which is implemented in most modern routers by creating access control lists based on the language of the router commands. Another way to protect yourself is to configure your router so that it can only connect to the Internet with those computers on the network whose information is open to the public. The

rest of the network is isolated from these computers by firewalls or other means. This type of protection is used by many large corporations.

Standalone traffic filtering packages installed on PCs or workstations are attached to routers in their functions. A typical product of this class is FireWall-1 software from Check-Point Software Technologies, installed on Sun workstations and filtering inbound and outbound streams. Unlike routers, Fire Wall-1 is able to dynamically open data paths according to Internet protocols, such as FTP.

In addition, this package is equipped with a user-friendly graphical interface, security alarms and network access loggers that generate reports of unusual activity. Such products generally provide better protection than routers, but are of high cost.

The firewall router and products of the FireWall-1 software just reviewed do not have some features that increase the security against intrusion. For example, when transmitting a data stream, they do not analyze its content and are unable to validate access to network resources.

Such capabilities are firewalls – dedicated computers with active functions of filtering information flows at the point of communication of the local network with the outside world. The main task of systems in this category is to isolate the network from outside encroachments by viewing data packets, blocking suspicious traffic, and using special means of acknowledging access privileges.

Thus, the firewall acts as a watchdog, which does not miss any input or output that does not meet explicit criteria. Today there is a wide variety of firewall-based data security tools on the market.

REFERENCES

1. Библиотека Сетевой Безопасности URL: http://securitv.tsu.ru.

2. An Introduction to Computer Security: The NIST Handbook. Draft. – National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 1994. 310 c.

Information about the author:
Domnich V. I.
Candidate of Technical Sciences, Professor,
Head at the Department of Automated Process Control
of the V. I. Vernadsky Taurida National University

DOI https://doi.org/10.36059/978-966-397-104-9/139-161

CRYPTOSYSTEMS AND INFORMATION SECURITY IN INTRANET

Muliava O. M.

1. Evaluation of the reliability of cryptosystems

A group of well-known cryptographic experts, created under the auspices of the Business Software Alliance (an industry organization that prevents software misuse), has come to the conclusion that the required key length should now be at least 75 bits with a further increase over the next 20 up to 90 bits.

Let's check this statement.

The problem of finding keys in a symmetric cryptosystem by sorting through all the possible keys belongs to a class of problems that allow parallelization. Applying Distributed Computing to Organize the Search of Such Keys[1].

The exponential growth dynamics of computing systems' performance over time (10 times in 5 years) has an even more significant impact on the overall performance of the system.

Thus, progress in this area is possible due to:

1) use of advances in scientific and technological progress and the use of technological innovations to increase the productivity of an individual device;

2) increasing the number of such devices in the system. From a physical point of view, that type of transistor, which is the basis of the modern integrated circuit, can be reduced by about 10 times, to a size of 0.03 microns. At this limit, the process of switching on/off the microscopic switches will be practically impossible. Thus, the maximum speed will be 1016 operations/second, and the limit of growth will come in about 2030.

There are no other ways to increase the computing power.

Thus, from the point of view of information security by cryptographic methods, the analysis of potential capabilities of the distributed computing method is of great interest for both crypto-analysts and developers of

[1] Немет Э., Снайдер Г., Сибасс С., Хейн Г.Р. UNIX: руководство системного администратора. Пер. с англ. Киев: BHV, 1996. 270 с.

cryptographic systems. So let's try to analyze the limit values of two of these trends.

From the list that appeared in the summer of 1999, it follows that supercomputers are distributed as follows:

with a power of about 10^{12} FLOPS 3 approx.;

with a power of about 10^{11} FLOPS 54 approx.;

with a power of about 10^{10} FLOPS 428 approx.;

with a power of about 10^{9} FLOPS 251 approx.;

The first place in the world in the number of supercomputers is occupied by the USA 254 (51%), followed by Japan 87 (17.5%), Germany 45 (9%), Great Britain 24 (4.8%), France 18 (3.6%)), Korea 8 (1.6%), Canada 7 (1.4%), Sweden, Switzerland and Norway 6 each (1.2%). Russia is mentioned only once in this list: the 156th place is the LDC Ultra 10000 computer (peak performance 16600 MFLOPS), manufactured by SUN and installed in the National Reserve Bank of Russia.

Десять самых мощных суперкомпьютеров в мире по состоянию на 1999 г.

Рейтинг	Наименование машины	Страна-обладатель	Фирма-производитель	Количество процессоров	Мощность (GFLOPS)
1	Intel ASCI Red	США	Intel (США)	9125	1333
2	Hitachi/Tsukuba CP-PACS	Япония	Hitachi/Tsukuba (Япония)	2048	368
3	SGI/Cray T3E	Великобритания	Cray (США)	696	265
4	Fujitsu Numerical Wind Tunnel	Япония	Fujitsu (Япония)	167	230
5	Hitachi SR2201	Япония	Hitachi (Япония)	1024	220
6	SGI/Cray T3E	Германия	Cray (США)	512	176
7	SGI/Cray T3E	США	Cray (США)	512	176
8	SGI/Cray T3E	Германия	Cray (США)	512	176
9	SGI/Cray T3E	США	Cray (США)	512	176
10	SGI/Cray T3E	США	Cray (США)	512	176

Interesting detail: there are no foreign computers in the US. Americans only work on domestic machines and also supply them to the whole world.

Power attack on cryptosystems is futile. However, the disadvantages of the algorithms can significantly reduce the number of search options.

Use as meaningful words as a key allows you to use dictionary attack. Therefore, further development of cryptography will occur in the field of cryptanalysis.

2. Why are cryptos not reliable?

In modern software, crypto algorithms are widely used not only for data encryption tasks but also for authentication and integrity checking. To date, there are well-known and proven crypto-algorithms (with symmetric and asymmetric keys), whose cryptocurrency is either proved mathematically or based on the need to solve a mathematically difficult problem (factorization, discrete logarithm, etc.).

The most famous of them are DES, GOST, RSA. Thus, they can not be disclosed other than a complete search or solution of the specified problem.

On the other hand, in the computer world, information about errors or "holes" in a particular program (including using crypto algorithms) or that it has been cracked is constantly being displayed. This creates a distrust of both specific programs and the ability to protect anything by cryptographic methods not only from special services, but also from simple hackers[2].

Therefore, knowledge of the history of attacks and "holes" in cryptosystems, as well as understanding the reasons for their occurrence, is one of the necessary conditions for the development of secure systems. A promising area of research in this area is the analysis of successfully conducted attacks or revealed vulnerabilities in cryptosystems in order to generalize, classify and identify the causes and patterns of their appearance and existence.

By, by analogy with the taxonomy of the causes of OS security breach, let us distinguish the following reasons for the unreliability of cryptographic programs:

- inability to use stable crypto algorithms;
- errors in the implementation of crypto algorithms;
- improper use of crypto algorithms:
- human factor.

Note that the following causes cover only two types of potential threats: disclosure and integrity, leaving aside the threat of denial of

[2] Гайкович В., Першин А. Безопасность электронных банковских систем. Москва: Единая Европа, 1994. 264 с.

service, which is increasingly important as distributed cryptosystems develop.

Inability to use persistent crypto algorithms

This group of reasons is most common because of the following factors.

The speed of stable crypto-algorithms is low

This is a major factor complicating the use of good algorithms, for example, in "total" encryption or "on-the-fly" encryption systems. In particular, Norton DiskReet, although it has a DES implementation, may not re-encrypt the entire disk when it is changed by the user, since this will take a very long time. Similarly, on-the-fly Stacker compression software from Stac Electronics has the option of closing off the offset data. However, it has no physical ability to encrypt its file with this password, it is usually several hundred megabytes in size, so it is limited by a very weak algorithm and stores the hash function against the password along with the protected data.

Export restrictions

This is due to the export of crypto algorithms or the need to buy a patent or rights. In particular, the export of crypto algorithms with key lengths greater than 40 bits is prohibited from the US. Obviously, such crypto-stability cannot be considered reliable with modern computing power and even on a personal computer. Putting the speed of the search at 50,000 passwords/sec, we get a search time of an average of about 4 months.

Well-known examples of programs that are subject to export restrictions are recent browsers of the Internet, including Netscape Navigator from Netscape Communications and Microsoft's Internet Explorer. They provide encryption with a 128-bit key for users in the US and a 40-bit key for everyone else. Also in this group is the latest version of the ARJ 2.60 archiver. known for its weak archive encryption algorithm. known for its weak archive encryption algorithm.

Users in the US can now use the GOST crypto-algorithm. The comism of the situation is that, although this algorithm is Russian, even Russians under US law can still not use it in the ARJ program.

Using your own crypto algorithms

Ignorance or unwillingness to use known algorithms is a paradox, especially in Freeware and Shareware applications, such as archivers.

As already mentioned, the ARJ archiver (up to version 2.60 inclusive) uses (by default) a very weak encryption algorithm – simple gamming. It would seem that in this case its use is permissible, since the archived text should be completely redundant and statistical methods of cryptanalysis are not suitable here. However, upon closer examination, it appeared that some non-random information is present in the archived text (and this is true for any archiver) – for example, the Huffman table and some other official information. Therefore, knowing exactly or predicting with some probability the values of these service variables, it is equally possible to determine the corresponding password characters.

Further, the use of weak algorithms often leads to the success of a plaintext attack. In the case of an ARJ archiver, if an attacker knows at least one file from an encrypted archive, it can easily determine the password of the archive and extract from it all other files (ARJ cryptocurrency with open text – 2^0!). Even if there is no encrypted file, it is still simple gamification allows you to reach a speed of 350,000 passwords/sec on a Pentium machine.

The same is true for popular Microsoft Office applications – you only need to know the 16 bytes of a .doc or .xls file to determine your password, and then just browse through 24 options. Microsoft Office 97 made significant improvements to the encryption algorithms, leaving only the possibility of a complete search, but ... not everywhere – MS Access 97 uses a primitive algorithm, and not the data itself, but the password itself with a fixed constant XOR operation!

Novell Netware's Novell networking system (version 3.x and 4.x) also has its own hashing algorithm. At the input, the hash function receives a 32-byte value obtained in the original user password by either compressing a password longer than 32 characters by XOR operation, or multiplying a password less than 32 characters, and outputting a 16-byte hash value (Hash 16). It (for Novell Netware 3.x) is stored in the database bindery as a property of "PASSWORD".

One of the key features of a hash function is that it must not allow easy collision building (such as the crypt() function used in UNIX, which is DES-based). This property is broken in the hash function used in Novell Netware.

The hash algorithm under consideration has remained in version 4 of Novell Netware.

Microsoft, in turn, also has major shortcomings in its mainstream hash algorithm, which is applicable to all its operating systems, starting with Windows 3.11, when authenticated on local (NetBIOS) and global (CIFS and http) networks, called LM (Lan Manager) – X3in. (However, Microsoft refers to the fact that it has remained since OS / 2 and that it was developed by IBM).

It is calculated as follows: the password is converted to a 14-character string by either cutting off long passwords or supplementing short passwords with null elements.

All lowercase characters are replaced with uppercase characters. Numbers and special characters remain unchanged.

The 14-byte string is split into two seven-byte halves.

Using each half of the string as a DES key, it encrypts a fixed constant, yielding two 8-byte strings at the output.

These lines merge to create a 16-bit hash value.

Obviously, attacks on the LM hash are easily successful for the following reasons:

Converting all characters to uppercase limits the already small number of possible combinations for each (26 +10 + 32 = 68).

Two seven-byte "half" passwords are hashed independently. Thus, the two halves can be sorted independently, and passwords longer than seven characters are no stronger than passwords with a length of seven characters.

There is no salt element, as in crypt() – two users with the same password will always have the same hash value.

Thus, you can pre-compile a dictionary of hashed passwords and search for an unknown password in it.

Wrong implementation of crypto algorithms

Although crypto-resistant or certified algorithms are used in this case, this group of reasons leads to a security breach of cryptosystems due to their incorrect implementation.

Decrease in cryptocurrency during key generation

This is because of the many examples where the crypto system either cuts the user's password or generates data with fewer bits than the password itself. Examples:

In many (older) versions of UNIX, the user password is truncated to 8 bytes before the hash. Interestingly, for example, Linux 2.0, requiring

users to enter passwords containing necessarily letters and numbers, does not verify that the 8-character password start also consists of letters and numbers. Therefore, by asking, for example, a sufficiently strong password 'passwordIsgoodlÇ', one would be very surprised to learn that a hacker has logged in under his name with a simple password 'password'.

Novell Netware allows users to have passwords up to 128 bytes, which gives (including Latin letters without case, numbers and special characters) $68^{128} \sim 2^{779}$ combinations. But first, the hash function (see above). It only receives a 32-byte value at the input, which limits the effective length of the password to the same value. Moreover, secondly, the output hash value is only 128 bits long, which corresponds to 2^{128} combinations. This further reduces the effective length to =21 символа[3], ie 6 times compared to the original length.

The situation with the RAR 1.5 * archiver is quite similar – choosing a password of more than 10 characters does not increase the time it takes to open it.

If the length of the "top" password in this case is determined by the implementation of cryptographic algorithms, then the restriction on the length of the "bottom" is already associated with the concept of unit of information or entropy. In the considered example from Novell Netware, to create a hash value with an entropy of 128 bits, the password length must be at least 22 characters. The fact that many cryptosystems do not limit the minimum length of the password, which in turn leads to the success of attacks not by keys and passwords.

Lack of checking for weak keys

Some crypto-algorithms (such as DES, IDEA), when encrypting with specific keys, may not provide the right level of cryptocurrency. Such keys are called weak. DES is known for 4 weak and 12 semi-weak. (Semi-weak) keys. Although the probability of getting into them is $\sim 2 * 10^{-16}$, for serious cryptographic systems it can not be neglected.

The power of many IDEA weak keys is 2^{51} (however, because of the total number of keys 2^{128}, the likelihood of getting into it is 333 times less than in DES).

Insufficient security against MS

MS (malicious software) are computer viruses, Trojan horses, software bookmarks, etc. applications that can intercept the private key or the unencrypted data themselves, and simply replace the algorithm with

non-encrypted ones. If the programmer has not provided sufficient security against the MS, they are easily capable of negatively affecting the security of the cryptosystem. This is especially true for operating systems that do not have built-in security or access control features, such as MS DOS or Windows 95:

Password Interception

An example is the oldest method of password stealing, known since the days of major computers, when the phantom program emulates the OS invitation, offering to enter a user name and password, memorize it in some file and stop working with the message 'Invalid password'. For MS DOS and Windows there are many bookmarks for reading and saving passwords that are typed on the keyboard (by intercepting the corresponding interrupt), for example, when using Diskreet V. 6.0.

Crypto algorithm replacement

An example of this is the bookmark masked under the Turbo Krypton-type accelerator application. This tab replaces the GOST 28147-89 encryption algorithm implemented by the Kgurton-C board (demo version) with another, simple and easily decrypted algorithm.

Trojan horse in email

A recent example is the June 1998 attempt to infiltrate a Trojan horse via email. The letter contained a pornographic image and an EXEC file FREECD.EXE, which, while the user was having fun with the letter, decrypted the passwords to the provider (Dial-Up) and sent them to ispp@usa.net.

Time limit for key processing

This is a relatively new aspect of the lack of correct implementation of crypto algorithms discussed in the article. There it is shown that many cryptosystems process different input data differently quickly. This is due to both hardware (different cycles per operation, CPU cache, etc.) and software reasons (especially when optimizing the program over time). Time may depend on both the encryption key and (de) encrypted data.

Therefore, the attacker, having detailed information about the implementation of the crypto algorithm, having encrypted data and being able to somehow measure the processing time of this data (for example, analyzing the time of sending packets with data), can try to pick up a secret key. The paper describes in detail the tactics of attacks on systems that implement algorithms RSA, Diffie-Hellman and DSS. moreover, the key

can be obtained by specifying bit by bit, and the number of required measurements of time is directly proportional to the length of the key.

Although it has not been possible to bring these studies to a concrete result (calculate the secret key), this example shows that the programming of critical systems (including cryptosystems) should be particularly careful and may need to use special security methods. programming and specialized development tools (especially compilers).

Errors in software implementation

Clearly, as long as programs are written by people, this factor will always be the case. A good example is Novell Netware 3.12, where, despite a well-thought-out authentication system that, according to Novell, "an unencrypted password is never transmitted over the network", SYSCON v. 3.76 was found to have an error where openly falls into one of the network packets.

This is not the case with either earlier or later versions of this program, which makes it possible to speak about a purely programming error. This error occurs only if the supervisor changes the password to someone (including himself). Apparently, somehow the keyboard buffer falls into the network packet.

The presence of hatches

The reasons for the presence of hatches in cryptosystems are obvious: the developer wants to have control over the information processed in his system and leaves for himself the ability to decrypt it without knowing the user's key. It is also possible that they are used for debugging and for some reason are not removed from the final product. Naturally, this sooner or later becomes known to a large number of individuals and the value of such a cryptosystem becomes almost zero. The most famous examples here are the AWARD BIOS (up to version 4.51PG) with its universal password "A WARD SW" and Borland International's Paradox DBMS, also has "SuperPassword", "jIGGAe" and "pbbrrh".

Along with the availability of hatches in the implementation (obviously, in this case, they use explicitly unstable algorithms or store the key together with the data) are adjacent algorithms that allow a third party to read an encrypted message, as is done in a high-profile CLIPPER project, where the third party acts, always fond of stuffing his nose in the secret of his citizens.

Disadvantages of the Random Data Generator (RDG)

A good, mathematically proven and correctly implemented RDG is as important for the cryptosystem as a good, mathematically stable and correct crypto-algorithm, otherwise its disadvantages can affect the overall crypto-stability of the system. In this case, pseudorandom number sensors, typically characterized by a period, scatter, and the need for its seed initiation, are usually used to model the RDG on the computer. The use of PDG for cryptosystems is not generally considered a good solution, so good cryptosystems use physical PDG (special charge) for this purpose, or at least produce a number to initialize PDG using physical values (for example, user key press time).

The short period and the bad scatter are related to the mathematical disadvantages of the RDG and appear if for some reason your own RDG is selected. In other words, choosing your own PDG is as dangerous as choosing your own crypto algorithm.

In the case of a small period (when the pseudorandom values produced by the sensor are less than the possible key values), the attacker can shorten the search time for the key by searching not pseudorandom keys but generating keys from them.

If the sensor is badly scattered, the attacker can also reduce the average search time if the search starts with the most likely pseudorandom numbers.

The most common mistake that can be found in the case of a good PDG is its incorrect initialization. In this case, the number used for initialization has either less number of bits of information than the sensor itself, or is calculated from non-random numbers and can be predicted with varying degrees of probability.

This was the case with Netscape Navigator version 1.1. It initializes the PDG using the current time in seconds (sec) and microseconds (usee), as well as process IDs (pid and ppid). As researchers J. Goldberg and D. Vagner have found out, at such scheme as a maximum 47 significant bits of information (though this sensor was used for 40- or 128 (!) – bit keys) were obtained. But, if the attacker had the ability to intercept packets transmitted over the network and had access (account) to the computer where the program is running, then it did not cause any problems with a high degree of probability to learn sec, pid and ppid. If condition (2) was not satisfied, the attacker could still try to set the time via network time

daemons, the pid could be obtained through the SMTP daemon (usually included in the Message-ID field), a ppid or not very different from the pid, or generally equal to 1.

The researchers wrote the unssl program. which, looking through the microseconds, found a secret 40-bit key in an average of a minute.

Incorrect application of crypto algorithms

This group of reasons leads to the unreliable crypto-stability and correctly implemented algorithms.

Short key length

Its the most obvious reason. The question is: how can stable crypto algorithms have a small key length? Probably due to two factors: some algorithms can work with variable key lengths, providing different cryptocurrency – and it is the developer's job to choose the required length based on the desired cryptocurrency and efficiency. Sometimes, other circumstances, such as export restrictions, impose this desire.

Some algorithms were developed a long time ago when the length of the key used in them was considered more than sufficient to meet the required level of protection.

With a sharp leap in computing performance, the RSA algorithm was first encountered, for which it is necessary to solve the factorization problem. In March 1994, was completed, which lasted for 8 months factorization of the number of 129 digits. To this end, 600 volunteers and 1600 email-connected machines were involved. Machine time was equivalent to approximately 5000 MIPS leagues.

The progress in solving the factorization problem is largely due not only to the growth of computing power, but also to the emergence of new efficient algorithms recently. (The factoring of the next number out of 130 digits took only 500 MIPS years). To date, it's basically a matter of factoring 512-bit numbers. If you mention that such numbers have recently been used in PGP. it can be argued that this is the fastest growing field of cryptography and number theory.

On January 29, 1997, RSA Labs announced a competition to open a symmetric RC5 algorithm. The 40-bit key was revealed 3.5 hours after the start of the contest! (This didn't even require connecting computers over the Internet – enough of a local network of 250 machines at Berkeley University). After 313 hours, a 48-bit key was opened.

Thus, it became obvious to everyone that the length of the key, which would satisfy the export restrictions, could not provide even the minimum reliability.

In parallel with the unveiling of the RC5, a pillar of American cryptography, a DES algorithm with a 56-bit key, was also challenged. And it fell on June 17, 1997, 140 days after the start of the contest (with about 25% of all possible keys tested and about 450 MIPS spent).

It was a remarkable achievement, which meant the actual death of DES as an encryption standard. Indeed, when in the beginning of 1998 the next DES Key Competition came to fruition in just 39 days, the National Institute of Standards (NIST) announced a competition to approve the new Advanced Encryption Standard (AES). The AES must be a fully open symmetric algorithm with a 128, 192, 256 bit key and a 128 bit encryption unit.

Invalid algorithm class selection

This is also a very common reason why a developer chooses a good, but completely inappropriate, algorithm. Most often it is to encrypt instead of hashing or to choose a symmetric algorithm instead of an algorithm with public keys.

For example, it is almost all programs that restrict access to the computer password when it is turned on or loaded, for example, AMI BIOS, which stores instead of the password hash its encrypted version, which, of course, is easily decrypted.

In all network authentication procedures, it is natural to use asymmetric cryptography, which will not allow you to pick up the key, even with full traffic capture. However, such algorithms (from network OS) so far only implement Novell Netware 4.x, others are satisfied (at best!) Standard query-response scheme, in which you can perform a fairly fast search for intercepted values of 'query' and 'feedback'.

Re-imposition of cipher gamma

Already a classic example is the encryption vulnerability in Windows 3.x and the first versions of Windows 95. In this case, Microsoft programmers, well-known for their security knowledge, used the RC4 algorithm (which is nothing like gamma encryption), without changing the gamut, several times to different data – network resources stored in .pwl files.

It turned out that one of the datasets of the .pwl file was more than specific text – a 20-character username (uppercase) and a set of pointers to resources. Thus, guessing the user (which in most cases also matches the file name), you can calculate at least 20 bytes of gamma. Since the gamma does not change when encrypting other resources (this is the main mistake of using RC4 in this case), the first 20 bytes of all resources that include the length of each can be calculated. By calculating the length, you can find the value of pointers and thus add a few tens of bytes to the guessed gamut. This algorithm is implemented in the known program elide.

Storing the key along with the data

This reason leads to the fact that data encrypted using a crypto-stable and correctly implemented algorithm can be easily decrypted. This is due to the specifics of the solved problem, in which it is impossible to enter the key from the outside and it is stored somewhere inside in almost unencrypted form. In other words, the encryption algorithm on the key, and the key (with the help of some secondary key) will be the most vulnerable here. But since (which again obviously follows from the specifics of the task) this secondary key cannot be stored from the outside, the master data will sooner or later be decrypted without the use of methods, iteration.

A typical example here would be all WWW-, ftp-, e-mail clients. The fact is that for basic (most common) authentication in these protocols, the password must be transmitted to the server in an open form. Therefore, client programs are forced to encrypt (not hashed) the password, and with a fixed key, so as not to bother the user with constant questions. It follows that somewhere inside any browser, mail or ftp client (be it Netscape Communicator, Eudora, Outlook, FAR, etc.), all your passwords are stored in a virtually open form, and that deciphering them is no problem. (Most often, by the way, the password in such programs is not even encrypted, and is encoded with a base-64 algorithm).

The human factor

In any critical system, human operator errors are by far the most expensive and widespread. In the case of cryptosystems, unprofessional actions of the user negate the most stable crypto-algorithm and its most correct implementation and application. First of all, it is related to the choice of passwords. Obviously, short or comprehending passwords are easily remembered by the person, but they are much easier to open. Using long and meaningless passwords is definitely better in terms of crypto-

persistence, but a person usually can't memorize and write them on a piece of paper, which then either gets lost or falls into the hands of the attacker.

In recent years, much attention has been paid to resolving this contradiction, but recommendations for choosing good passwords are beyond the scope of this article.

In addition to the fact that inexperienced users usually choose either short or meaningful passwords, there are two methods of their disclosure: full-blown attack and dictionary attack.

Due to the sharp increase in computing power, full-on-attack attacks are much more likely to succeed than before (see also 'Small Key Length'). If crypt(), which is responsible for password hashing, was implemented for UNIX for almost 1 second on a PDP class machine, the speed of its calculation was increased 15,000 times in twenty years (!). Therefore, if earlier hackers (and developers who limited the length of the password to 8 characters) and could not imagine a complete search, today such an attack will on average lead to success in 80 days. Below is the password speed for different cryptosystems.

Full-speed search on a Pentium / 166 computer

Криптосистема	Скорость, паролей/сек.
ARJ 2.50	350 000
RC5 - 56 бит	150 000
LM-хэш	50 000
Novell Netware 3.x	25 000
MS Office 97	15 000
UNIX - crypt()	15 000
RAR 2.0	1 000
UNIX -MD5	500

However, back to a few years ago, when computing power was not enough to completely reset all passwords. However, hackers have come up with a clever method based on the fact that as a password a person selects an existing word or any information about himself or his acquaintances (name, date of birth, etc.). Well, since there are no more than 100,000 words in any language, it will take quite a bit of time to search

them, and 40 to 80% of your existing passwords can be guessed using a simple scheme called "dictionary attack." up to 80% of these passwords can be guessed using a dictionary of only 1000 words!). Even the Morris virus (1988!).

Used this way, especially since UNIX often has a dictionary file on hand, often used by proofreaders. As for "own" passwords, the /etc/passwd file can give a lot of information about the user: his input name, first name, home folder.

The Morris virus has successfully used the following assumptions:

- the input username is taken as the password;
- password is a double repeat of the username;
- same but read from right to left;
- first or last name of the user;
- same but lowercase.

Today, users already understand that it is impossible to choose such passwords, but as long as a person is working with a computer, computer security experts will not wait to use such simple and happy souls of passwords as 34jXs5U @ bTa! 6.

Therefore, even the experienced user cheats and selects such passwords as hopel, userl997, pAsSwOrD, toor, roottoor, password, gfhjkm, asxz. It can be seen that they are usually based on a meaningful word and some simple rule of its transformation: to add a number, to add a year, to translate a letter in another register, to spell the word opposite, to spell the word in Latin, to type Russian a word on a keyboard with a Latin layout, to password with a number of keys located on the keyboard, etc.

Therefore, one should not be surprised if such a "tricky" password will be revealed by hackers – they are not more stupid than the users themselves, and have already inserted into their programs the rules that can be converted words.

In the most advanced programs (John The Ripper Password Cracking Library) these rules can be programmed and set using a special language by the hacker.

Here is an example of the effectiveness of such a search strategy. Many security books suggest choosing a meaningful password for two meaningful words separated by a character, such as "good.password". We calculate how long, on average, such passwords will be cracked if such a rule is included in a cracker program (let the dictionary of 10,000 words,

punctuation marks can be 10 digits and 32 punctuation marks and special characters, Pentium class machine with a speed of 15000 crypt / sec): = 140,000 seconds or less than 1.5 days!

3. Information security in Intranet

3.1 Developing network security policies

Security policy is defined as a set of documented management decisions aimed at protecting information and its associated resources[3].

In developing and implementing it in life, it is advisable to be guided by the following principles:

- inability to pass protective equipment;
- strengthening the weakest link;
- inability to transition to a dangerous state;
- minimizing privileges;
- division of responsibilities;
- separation of defense;
- variety of protective equipment;
- simplicity and controllability of the information system;
- providing general support for security measures.

Let's explain the meaning of the above principles. If an attacker has a disgruntled user with the ability to bypass security, he will, of course, do so. With respect to firewalls, this principle means that all information flows to and from the protected network must pass through the firewall. There should be no "secret" modem or test line inputs that bypass the firewall.

The reliability of any defense is determined by the weakest link. The attacker does not fight against strength, he prefers an easy victory over weakness. Often, the weakest link is not the computer or the program, but the person, and then the problem of information security becomes non-technical.

The principle of inability to move into a dangerous state means that in all circumstances, including freelance, the protective agent either performs its functions completely or completely blocks access. Figuratively speaking, if the strength of the drawbar mechanism breaks down, the bridge must remain elevated, obstructing the passage of the enemy.

[3] URL: http://www.ksu.vntu.edu.ua/files/akit/bakalavr/14_4.pdf

The principle of minimizing privileges requires that users and administrators be granted only the access rights they need to perform their duties.

The principle of division of responsibilities implies such a division of roles and responsibilities, in which one person can not initiate a process critical to the organization. This is especially important to prevent malicious or unqualified system administrator actions.

The principle of separation of the defense dictates not to rely on one defensive line, no matter how reliable it may seem. Physical security means must be followed by software and hardware, access control and, as the last line, logging and auditing. An echelon of defense is capable of at least deterring an attacker, and the presence of a line such as logging and auditing makes it difficult to make a criminal act imperceptible.

The principle of the diversity of protective equipment recommends the organization of different defensive lines in character, so that the potential attacker would require mastering a variety and, if possible, incompatible skills (such as the ability to overcome high fencing and knowledge of the weaknesses of several operating systems).

A very important principle is the simplicity and manageability of the information system as a whole and security in particular. Only for a simple safeguard can it be formally or informally proven correct. Only in a simple and manageable system can you check the consistency of the configuration of the various components and perform centralized administration.

In this regard, it is important to note the integrating role of the Web service, hiding the diversity of objects and providing a single, visual interface. Accordingly, if objects of some kind (say database tables) are accessible through the Web, you must block direct access to them, otherwise the system will be complicated.

The last principle – general support for security measures – is non-technical. If users and / or system administrators consider information security to be superfluous or even hostile, the security mode is deliberately failed. From the outset, a set of measures aimed at ensuring the loyalty of staff, continuous training, theoretical and, most importantly, practical, should be envisaged.

Risk analysis is the most important step in developing a security policy. In assessing the risks to which the Internet system is exposed, the following circumstances should be considered:

- New threats to old services that result from the ability to passively or actively listen to the network. Passive listening means reading the network traffic, while active listening means changing it (theft, duplicate modification of transmitted data). For example, authentication of a remote client using a reusable password cannot be considered reliable in a network environment, regardless of the length of the password;
- New (network) services and associated threats.

As a rule, Internet systems should adhere to the principle of "all that is not allowed, forbidden", since "unnecessary" network service can provide a channel of penetration into the corporate system. In principle, the same view expresses the statement "all incomprehensibly dangerous."

3.2 Software environment security

The idea of networks with so-called active agents, where not only passive but active data (ie programs) are transmitted between computers, is certainly not new. Initially, the goal was to reduce network traffic by performing the bulk of the processing where the data is located (approximating programs to the data). In practice, this meant moving applications to servers. A classic example of implementing this approach is the stored procedures in the DBMS[4].

For Web servers, programs that support the Common Gateway Interface (CGI) are analogous to stored procedures.

CGI procedures are hosted on servers and are commonly used to dynamically generate HTML documents. Organization security policies and procedures should determine who is allowed to connect to the CGI server. Rigid control is necessary here, as executing the wrong program by the server can lead to any serious consequences. A reasonable measure of a technical nature is to minimize the privileges of the user on whose behalf the Web server is running.

In Intranet technology, if you care about the quality and expressive power of the user interface, there is a need to move applications from Web servers to client computers – to create animations, perform semantic controls when entering data, etc. In general, active agents are an integral part of the Internet technology.

[4] URL: https://issuu.com/alex.voronkin/docs/

In whatever direction programs are moved over the network, these actions are of great danger because a program obtained from an unreliable source may contain unintentionally made malicious intentionally generated malicious code.

This program potentially threatens all major aspects of information security:

- accessibility (the program can absorb all available resources);
- integrity (the program can delete corrupted data);
- privacy (the application can read the data and transmit it over the network).

The problem of unreliable programs was recognized for a long time, but apparently only within the programming system.

Java is the first to offer a holistic concept for its solution.

Java offers three defensive lines:

- reliability of language;
- control upon receipt of programs;
- control when executing programs.

However, there is another, very important way to ensure information security – the unprecedented openness of the Java system. The source code of the Java compiler and interpreter is available for verification, so it is likely that honest experts, not malicious users, will be the first to detect errors and shortcomings.

In conceptual terms, the greatest difficulty is the controlled execution of programs downloaded over the network. First of all, it is necessary to determine what actions are considered acceptable for such programs. Considering that Java is a language for writing client parts of applications, one of the basic requirements for which is mobility, the downloaded program can only serve the user interface and to communicate with the server. The program cannot handle the files at least because there may not be any files on the Java terminal. More meaningful actions must be performed on the server side or performed by programs local to the client system.

An interesting approach is offered by Sun Microsystems specialists to ensure the safe execution of batch files. It's about Safe-Tcl (Tool Comman Language). Sun has proposed a so-called cellular command file interpretation model. There is a master interpreter to whom all language capabilities are available.

If you need to execute a questionable batch file while the application is running, a subordinate command interpreter is created that has limited functionality (for example, files and network capabilities can be removed from it).

As a result, potentially dangerous programs find themselves trapped in cells that protect user systems from hostile action. To perform actions that are considered privileged, the slave interpreter may request the principal.

Obviously, here is an analogy with the separation of operating system address space and user processes and the use of recent system calls. This model has been standard for the OS for about 30 years.

3.3 Authentication in Open Networks

Methods used in open networks to validate and validate entities must be robust to passive and active network listening.

Their essence is as follows.

- The subject demonstrates knowledge of the secret key, with the key either not being transmitted over the network or transmitted in encrypted form.
- The subject demonstrates mastery of the software or hardware for generating one-time passwords by means of a request-response mode. It is easy to see that the intruder and subsequent playback of a one-time password to answer the request does not give the attacker.

3.4 The concept of data transmission in open networks

One of the most important tasks is protecting the flow of corporate data transmitted over open networks. Open channels can be securely protected by only one method – cryptographic.

Of course it is natural to put on the firewall the task of encrypting and decrypting corporate traffic on the way to and from the external network. In order for such encryption/decryption to be possible, an initial allocation of keys must take place. Modern cryptographic technologies offer a number of methods for this purpose.

After the firewalls have encrypted the closure of corporate data streams, the territorial location of the network segments is detected only at different rates of exchange with different segments. The rest of the network looks like a whole, and subscribers do not need to bring any additional security.

Simplicity and homogeneity of architecture

The most important aspect of information security is the manageability of the system. Manageability is both the maintenance of high system availability through early detection and troubleshooting, the ability to change hardware and software configurations according to changed or needs, and notification of attempts to breach information security almost in real time, and reducing the number of administration errors, and many, much more.

Simplicity and homogeneity of architecture

The most important aspect of information security is the manageability of the system. Manageability is both the maintenance of high system availability through early detection and troubleshooting, the ability to change hardware and software configurations according to changed or needs, and notification of attempts to breach information security almost in real time, and reducing the number of administration errors, and many, much more.

Internet technology, at the expense of simplicity and homogeneity of architecture, makes the cost of administering a client workplace virtually nil.

It is also important that the replacement and re-commissioning of the client computer can be accomplished very quickly, since these are "clients without status", they have nothing that requires a long-term recovery or configuration.

At the junction of the client and server parts of the Internet-system is a Web-server. This allows for a single mechanism for registering users and granting them access rights, followed by centralized administration. Interaction with numerous heterogeneous services is hidden not only from users, but also to a great extent from the system administrator.

The task of providing information security on the Internet is simpler than in the case of arbitrary distributed systems built in the client / server architecture. The reason is the homogeneity and simplicity of the Internet architecture.

If application developers are able to take full advantage of this advantage, then at the software and technical level, they will be quite a few inexpensive and easy to learn products. However, a thoughtful security policy and a comprehensive set of procedural measures should be added to this.

Some recommendations

A comprehensive approach to information security is needed.

Information security should be considered as an integral part of the overall security of the bank – and as an important and integral part of it. The development of the concept of information security should necessarily involve the management of the bank's security. This concept should not only encompass information technology-related measures (crypto-protection, user rights management software, their identification and authentication, firewalls to protect network I / O, etc.), but also administrative and technical, including rigid procedures for controlling physical access to the automated banking system, as well as means of synchronization and communication between the banking security module and the security system.

It is necessary for the security management staff to participate in the selection-acquisition-development phase of the automated banking system. This participation should not be limited to verification by the supplier. The security management must monitor the availability of appropriate means of differentiating access to information on the system being purchased.

CONCLUSION

Note that encryption and decryption are required in society not by themselves, but only because they can bring profit or avoid losses, so it is always necessary to know what is the value of one character encrypted and decrypt information and what is the cost?

Are the organizations involved in intercepting or decrypting information profitable, or are they deliberately unprofitable?

The most interesting comparative analysis of data to scientifically justify the share of information security costs. It should also be borne in mind that a significant number of attacks are carried out internally by staff from institutions, which are much more difficult to defend against.

In particular, the problem of key storage is currently the most acute and, if using public keys solves the problem of key distribution and user authentication, then a more efficient way of storing keys than memorizing not found, and the use of memorable passwords allows you to apply dictionary attack.

In addition, the use of reliable cryptographic methods does not guarantee protection against software attacks.

Therefore, when creating computer cryptosystems, it is necessary to provide security at the operating system level, which is more difficult than creating a cryptosystem itself.

SUMMARY

There are 4 main groups of reasons for the unreliability of cryptographic systems: the use of unstable algorithms, the incorrect implementation or application of crypto algorithms, as well as the human factor.

This shows a clear parallel between them and the reasons for the breach of security of computer systems.

For the reasons described, there have been or are security concerns in all classes of software using crypto algorithms, be they operating systems; cryptocurrencies; clients and servers that support them; office applications; user-friendly encryption utilities; popular archives.

In order to intelligently implement your own cryptosystem, it is necessary not only to become acquainted with the errors of the Others and to understand the reasons for their occurrence, but also, perhaps, to apply special protective techniques of programming and specialized development tools.

REFERENCES

1. Немет Э., Снайдер Г., Сибасс С., Хейн Г.Р. UNIX: руководство системного администратора. Пер. с англ. Киев: BHV, 1996. 270 с.
2. Гайкович В., Першин А. Безопасность электронных банковских систем. Москва: Единая Европа, 1994. 264 с.
3. URL: http://www.ksu.vntu.edu.ua/files/akit/bakalavr/14_4.pdf
4. URL: https://issuu.com/alex.voronkin/docs/

Information about the author:
Muliava O. M.
Candidate of Physical and Mathematical Sciences, Associate Professor, Deputy Dean of the National University of Food Technology

NOTES

NOTES

Publishing house “Liha-Pres”
9 Kastelivka str., Lviv, 79012, Ukraine
44 Lubicka str., Toruń, 87-100, Poland

Printed by the publishing house “Liha-Pres”
Passed for printing: August 30, 2019.
A run of 150 copies.