Noncommercial
Joint Stock
Company

ALMATY
UNIVERSITY OF POWER
ENGINEERING AND
TELECOMMUNICATIONS
NAMED AFTER
GUMARBEK DAUKEEV

Department
for Language Studies

PROFESSIONAL ORIENTED FOREIGN LANGUAGE

Methodical Recommendations to work with special texts
for the students of Information System and
technology specialty – 5B070300

Almaty 2020

AUTHOR: Baigaskina Zh.K. – master, senior teacher of the department for Language Studies. Professional oriented foreign language. Methodical Recommendations to work with special texts for the students of Information System and technology specialty – 5B070300 – Almaty: AUPET, 2020. – 43 p.

The present methodological guidelines are intended to develop the skills of reading and translating technical texts in the field of Information Systems.

Methodological guidelines include professionally oriented texts, exercises and assignments for mastering terms in this specialty.

The material can be used both in practical lessons and in the practice of self-study assignments in order to form the foreign language professional competence of students – bachelors of the specialty 5B070300.

Reviewer: Kurpenov B.K.

Published according to the plan of publications of noncommercial JSC «Almaty University of Power Engineering and Telecommunications» named after Gumarbek Daukeev, 2020.

Introduction

The present methodological guidelines are intended to develop the skills of reading and translating technical texts in the field of Information Systems.

Methodological guidelines can be used both in practical lessons and in the practice of self-study assignments in order to form the foreign language professional competence of students – bachelors of the specialty 5B070300.

The material includes professionally oriented texts, exercises and assignments for mastering terms in the specialty Information Systems.

In these texts, you will see how real global businesses use technology and information systems to increase their profitability, improve their customer service, and manage their daily operations. In other words, you will learn how information systems provide the foundation for modern business enterprises.

The goal of the methodological guidelines is to teach the students, how to use IT to master their current or future jobs and to help ensure the success of their organization. We concentrate on placing information systems in the context of business, so that you will more readily grasp the concepts presented in the text.

Methodological guidelines are convenient to use for self-study assignments under the teacher supervision and for extracurricular activities.

Unit 1

Memorize the words
reference – ссылка (на кого-л. / что-л.); упоминание (о ком-л. / чём-л.)
complementary – добавочный, дополнительный, комплементарный
emphasis – акцент; ударение; выделение; подчеркивание; эмфаза
distinction – *различие, распознавание*
capturing – 1) сбор (напр., данных), 2) захват ((напр., канала связи))
semi-formal – полуофициальный, полуформальный
primary focus – передний фокус

Exercise 1. Give a written translation of the text into Native language.

Exercise 2. Give the Russian variant of the following expressions: organizational system designed to collect, store and distribute information, information systems are composed, the aforementioned communication networks, a clear distinction between information systems, alter argues for advantages of viewing an information system, information systems inter-relate with data systems.

Exercise 3. Answer the questions.

1. What is an Information system?
2. What are the functions of the information and communication technology?
3. What can you say about distinction between information systems, computer systems, and business processes?
4. What is work system?
5. What can an information system also be considered?

Text 1. Retell the text.

Information system

An Information system (IS) is a formal, sociotechnical, organizational system designed to collect, process, store and distribute information. In sociotechnical perspective, information systems are composed by four components: task, people, structure (or roles), and technology. Information systems can be defined as an integration of components for collection, storage and processing of data of which the data is used to provide information, contribute to knowledge as well as digital products.

A *computer information system* is a system composed of people and computers that processes or interprets information. The term is also sometimes used to simply refer to a *computer system* with software installed.

Information Systems is an academic study of systems with a specific reference to information and the complementary networks of hardware and software that people and organizations use to collect, filter, process, create and also distribute *data.* An emphasis is placed on an information system having a definitive boundary, users, processors, storage, inputs, outputs and the aforementioned communication networks.

Any specific information system aims to support operations, management and *decision-making*. An information system is the *information and communication technology* (ICT) that an organization uses, and also the way in which people interact with this technology in support of business processes.

Some authors make a clear distinction between information systems, *computer systems,* and *business processes*. Information systems typically include an ICT component but are not purely concerned with ICT, focusing instead on the end-use of *information technology*. Information systems are also different from business processes. Information systems help to control the performance of business processes.

Alter argues for advantages of viewing an information system as a special type of work system. A *work system* is a system in which humans or machines perform processes and activities using resources to produce specific products or services for customers. An information system is a work system whose activities are devoted to capturing, transmitting, storing, retrieving, manipulating and displaying information.

As such, information systems inter-relate with data systems the one hand and activity systems on the other. An information system is a form of communication system in which data represent and are processed as a form of social memory. An information system can also be considered a semi-formal language which supports human decision making and action.

Information systems are the primary focus of study for organizational informatics.

Unit 2

Memorize the words

to meet the needs – удовлетворять потребности

transaction processing system (TPS) – система обработки транзакций

decision support systems – система поддержки принятия решений

knowledge management systems – система управления знанием

database management systems – система управления базой данных; система управления базами данных

malleable – гибко реагирующий на воздействие рекламы; гибкий

chief information officer – директор по информации (руководитель компании, который отвечает за создание и функционирование системы хранения и использования информации внутри компании)

chief executive officer – главный исполнительный директор, менеджеры высшего звена, руководители корпораций и крупных компаний

chief operating officer – (главный) операционный директор, директор по производству

feedback – обратная связь, связь производителя с потребителем, информация от потребителя

machine-readable – машиночитаемый, машинно-считываемый

Exercise 1. Give a written translation of the text into Native language.

Exercise 2. Make up 10 questions about the text and let your neighbor answer them, then change parts.

Text 2. Retell the text.

System view of information system

Mark S. Silver (1995) provided two views on IS that includes software, hardware, data, people and procedures. Zheng (Чжен) provided another *system view of information system* which also adds processes and essential system elements like environment, boundary, purpose, and interactions.

The Association for Computing Machinery defines "Information systems specialists focusing on integrating information technology solutions and business processes to meet the information needs of businesses and other enterprises."

There are various types of information systems, for example: transaction processing systems, decision support systems, knowledge management systems, learning management systems, database management systems, and office information systems. Critical to most information systems are information technologies, which are typically designed to enable humans to perform tasks for which the human brain is not well suited, such as: handling large amounts of information, performing complex calculations, and controlling many simultaneous processes.

Information technologies are a very important and malleable resource available to executives. Many companies have created a position of chief information officer (CIO) that sits on the executive board with the chief executive officer (CEO), chief financial officer (CFO), chief operating officer (COO), and chief technical officer (CTO). The CTO may also serve as CIO, and vice versa. The chief information security officer (CISO) focuses on information security management.

The *six components* that must come together in order to produce an information system are: (Information systems are organizational procedures and do not need a computer or software, this data is erroneous, i.e., an accounting system in the 1400s using a ledger and ink utilizes an information system).

Hardware: The term hardware refers to machinery. This category includes the computer itself, which is often referred to as the central processing unit (CPU), and all of its support equipment. Input and output devices, storage devices and communications devices are support equipment.

Software: The term software refers to computer programs and the manuals (if any) that support them. Computer programs are machine-readable instructions that direct the circuitry within the hardware parts of the system to function in ways that produce useful information from data. Programs are generally stored on some input/output medium, often a disk or tape.

Data: Data are facts that are used by programs to produce useful information. Like programs, data are generally stored in machine-readable form on disk or tape until the computer needs them.

Procedures: Procedures are the policies that govern the operation of a computer system. “Procedures are to people what software is to hardware” is a common analogy that is used to illustrate the role of procedures in a system.

People: Every system needs people if it is to be useful. Often the most overlooked element of the system is the people, probably the component that most influence the success or failure of information systems. This includes “not only the users, but those who operate and service the computers, those who maintain the data, and those who support the network of computers.”

Feedback: it is another component of the IS, that defines that an IS may be provided with feedback (Although this component isn't necessary to function).

Data is the bridge between hardware and people. This means that the data we collect is only data until we involve people. At that point, data is now information.

Unit 3

Memorize the words

transaction processing systems – система обработки транзакций

data warehouses – организация информационных хранилищ

enterprise resource planning – планирование бизнес-ресурсов

expert systems – экспертные системы

search engine – поисковая подсистема; сервер поиска; механизм поиска

office automation – автоматизация управленческих работ

computer-based information systems – автоматизированная информационная система, (компьютеризированный)

pillars – пиляры

dashboard – инструментальная панель, приборная панель, панель приборов, приборный щиток

supply chain management system – управление поставщиками

to duplicate the work – дублировать работу, размножать документы

forecast – предвидеть, предвосхищать, предсказывать

revenues – доход

suggest [sə'ʤest] – предлагать, советовать

Exercise 1. Give a written translation of the text into Native language.

Exercise 2. Make up 10 questions about the text and let your neighbor answer them, then change parts.

Text 3. Retell the text.

Types of information system

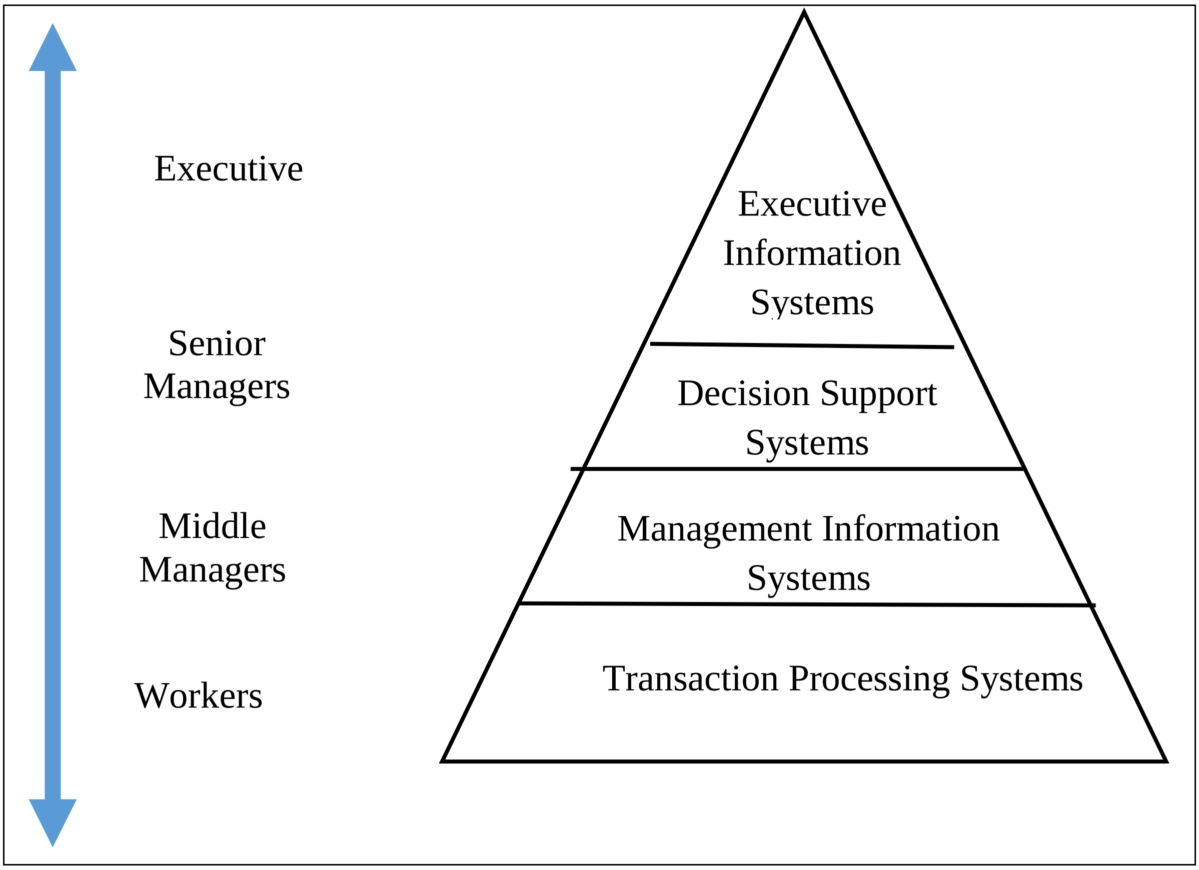
Executive
Senior Managers
Middle Managers
Workers
Executive Information Systems
Decision Support Systems
Management Information Systems
Transaction Processing Systems

Figure 1

The “classic” view of Information systems found in the 1980s was a pyramid of systems that reflected the hierarchy of the organization (Fig. 1), usually transaction processing systems at the bottom of the pyramid, followed by management information systems, decision support systems, and ending with executive information systems at the top. Although the pyramid model remains useful since it was first formulated, a number of new technologies have been developed and new categories of information systems have emerged, some of which no longer fit easily into the original pyramid model.

Some examples of such systems are:

- data warehouses;
- enterprise resource planning;
- enterprise systems;
- expert systems;
- search engines;
- geographic information system;
- global information system;
- office automation.

A **computer (based) information system** is essentially an IS using computer technology to carry out some or all of its planned tasks. The basic components of computer-based information systems are:

- *Hardware* – these are the devices like the monitor, processor, printer, and keyboard, all of which work together to accept, process, show data, and information.
- *Software* – are the programs that allow the hardware to process the data.
- *Databases* – are the gathering of associated files or tables containing related data.
- *Networks* – are a connecting system that allows diverse computers to distribute resources.
- *Procedures* – are the commands for combining the components above to process information and produce the preferred output.

The first four components (hardware, software, database, and network) make up what is known as the information technology platform. Information technology workers could then use these components to create information systems that watch over safety measures, risk and the management of data. These actions are known as information technology services.

Certain information systems support parts of organizations, others support entire organizations, and still others, support groups of organizations. Recall that each department or functional area within an organization has its own collection of application programs or information systems. These functional area information systems (FAIS) are supporting pillars for more general IS namely, business intelligence systems and dashboards. As the name suggests, each FAIS supports a particular function within the organization, e.g.: accounting IS, finance IS, production-operation management (POM) IS, marketing IS, and human resources IS. In finance and accounting, managers use IT systems to forecast revenues and business activity, to determine the best sources and uses of funds, and to perform audits to ensure that the organization is fundamentally sound and that all financial reports and documents are accurate. Other types of organizational information systems are FAIS, Transaction processing systems, enterprise resource planning, office automation system, management information system, decision support system, expert system, executive dashboard, supply chain management system, and electronic commerce system. Dashboards are a special form of IS that support all managers of the organization. They provide rapid access to timely information and direct access to structured information in the form of reports. Expert systems attempt to duplicate the work of human experts by applying reasoning capabilities, knowledge, and expertise within a specific domain.

Unit 4

Memorize the words

implementation – ввод в работу; воплощение; реализация maintenance – содержание и техническое обслуживание, уход; текущий ремонт

enabling – дающий возможность (сделать что-л.); позволяющий (что-л.); способствующий

ongoing research – проводимые в настоящее время исследования

accomplished [ə'kʌmplɪʃt] –достигший совершенства, искусный

outsourcing ['autˌsɔːsɪŋ] – аутсорсинг (*передача независимому подрядчику некоторых бизнес-функций или частей бизнес-процесса предприятия*)

to disseminate information / new ideas / news – распространять информацию / новые идеи / новости

impending disaster – приближающаяся / надвигающаяся беда

emerging information systems – развивающийся информационная система

Exercise 1. Determine which part of speech the words belong to.

application, to develop, systematically, recent, research, geographical, specific, theoretical, foundation, emphasizes, functionality, design.

Exercise 2. Give a written translation of the text into Native language.

Text 4. Retell the text.

Information system development

Information technology departments in larger organizations tend to strongly influence the development, use, and application of information technology in the business. A series of methodologies and processes can be used to develop and use an information system. Many developers use a systems engineering approach such as the system development life cycle (SDLC), to systematically develop an information system in stages. The stages of the system development lifecycle are planning, system analysis, and requirements, system design, development, integration and testing, implementation and operations, and maintenance. Recent research aims at enabling and measuring the ongoing, collective development of such systems within an organization by the entirety of human actors themselves. An information system can be developed in house (within the organization) or outsourced. This can be accomplished by outsourcing certain components or the entire system. A specific case is the geographical distribution of the development team (offshoring, global information system).

A computer-based information system, following a definition of Langefors, is a technologically implemented medium for:

- recording, storing, and disseminating linguistic expressions,
- as well as for drawing conclusions from such expressions.

Geographic information systems, land information systems, and disaster information systems are examples of emerging information systems, but they can be broadly considered as spatial information systems. System development is done in stages which include:

- Problem recognition and specification.
- Information gathering.
- Requirements specification for the new system.
- System design.
- System construction.
- System implementation.
- Review and maintenance.

As an academic discipline

The field of study called *information systems* encompasses a variety of topics including systems analysis and design, computer networking, information security, database management, and decision support systems. Information management deals with the practical and theoretical problems of collecting and analyzing information in a business function area including business productivity tools, applications programming and implementation, electronic commerce, digital media production, data mining, and decision support. *Communications and networking* deals with telecommunication technologies. Information systems bridges business and computer science using the theoretical foundation of information and computation to study various business models and related algorithmic processes on building the IT systems within a computer science discipline. Computer information systems (CIS) is a field studying computers and algorithmic processes, including their principles, their software and hardware designs, their applications, and their impact on society, whereas IS emphasizes functionality over design.

Several IS scholars have debated the nature and foundations of Information Systems which have its roots in other reference disciplines such as Computer Science, Engineering, Mathematics, Management Science, Cybernetic, and others. Information systems also can be defined as a collection of hardware, software, data, people, and procedures that work together to produce quality information.

Unit 5

Memorize the words

scope – масштаб, предел, размах; сфера, область действия
distinct – отдельный; особый, индивидуальный; отличный
differentiating – дифференцирующий, различающий
meaningful – существенный; значащий; значительный
to possess dignity – обладать чувством собственного достоинства
scientific approach – научный подход
prevents somebody from doing something – помешать / не дать кому-либо что-либо сделать

Exercise 1. Think of questions to the following sentences.

1) Information systems are distinct from information technology (IT) in that an information system has an information technology component that interacts with the processes' components.

2) The term information systems are also used to describe an organizational function that applies IS knowledge in the industry, government agencies, and not-for-profit organizations.

3) One problem with that approach is that it prevents the IS field from being interested in non-organizational use of ICT, such as in social networking, computer gaming, mobile personal usage, etc.

4) This approach, based on philosophy, helps to define not just the focus, purpose, and orientation, but also the dignity, destiny and, responsibility of the field among other fields.

Exercise 2. Give a written translation of the text into Native language.

Text 5. Retell the text.

Related terms

In a broad scope, the term *Information Systems* is a scientific field of study that addresses the range of strategic, managerial, and operational activities involved in the gathering, processing, storing, distributing, and use of information and its associated technologies in society and organizations. The term information systems are also used to describe an organizational function that applies IS knowledge in the industry, government agencies, and not-for-profit organizations. Information *Systems* often refers to the interaction between algorithmic processes and technology. This interaction can occur within or across organizational boundaries. An information system is a technology an organization uses and also the way in which the organizations interact with the technology and the way in which the technology works with the organization's business processes. Information systems are distinct from information technology (IT) in that an information system has an information technology component that interacts with the processes' components.

One problem with that approach is that it prevents the IS field from being interested in non-organizational use of ICT, such as in social networking, computer gaming, mobile personal usage, etc. A different way of differentiating the IS field from its neighbor is to ask, "Which aspects of reality are most meaningful in the IS field and other fields? This approach, based on philosophy, helps to define not just the focus, purpose, and orientation, but also the dignity, destiny and, responsibility of the field among other fields.

Unit 6

Memorize the words

decision-making – принятие решения

Project Management – проектный менеджмент, управление проектом

a commercial enterprise – коммерческое предприятие

executive – администратор, ответственный работник [сотрудник], руководство, руководящее звено

Exercise 1. Make up a list of new terms you can find in the text. Translate them into Native language.

Exercise 2. Read the text. Translate it into Native language.

Text 6. Retell the text.

Career pathways

Information Systems workers enter a number of different careers:

- Information System Strategy.
- Management Information systems – A management information system (MIS) is an information system used for decision-making, and for the coordination, control, analysis, and visualization of information in an organization.
- Project Management – Project management is the practice of initiating, planning, executing, controlling, and closing the work of a team to achieve specific goals and meet specific success criteria at the specified time.
- Enterprise Architecture – A well-defined practice for conducting enterprise analysis, design, planning, and implementation, using a comprehensive approach at all times, for the successful development and execution of strategy.
- IS Development.
- IS Organization.
- IS Consulting.
- IS Security.
- IS Auditor.

There is a wide variety of career paths in the information systems discipline. "Workers with specialized technical knowledge and strong communications skills will have the best prospects. Workers with management skills and an understanding of business practices and principles will have excellent opportunities, as companies are increasingly looking to technology to drive their revenue.

Information technology is important to the operation of contemporary businesses; it offers many employment opportunities. The information systems field includes the people in organizations who design and build information systems, the people who use those systems, and the people responsible for managing those systems. The demand for traditional IT staff such as programmers, business analysts, systems analysts, and designer is significant. Many well-paid jobs exist in areas of Information technology. At the top of the list is the chief information officer (CIO).

The CIO is the executive who is in charge of the IS function. In most organizations, the CIO works with the chief executive officer (CEO), the chief financial officer (CFO), and other senior executives. Therefore, he or she actively participates in the organization's strategic planning process.

Unit 7

Memorize the words

behavioral science – наука о поведении
propose [prə'pəuz] – предлагать; вносить предложение
framework – структура; общая схема
domain of study – область изучения
proposition – заявление, предположение, план, проект, задача
represent [ˌreprɪ'zent] – представлять; изображать; отображать; означать

Exercise 1. Read the text and find sentences where the following terms are used. Translate them: scientific paradigms, boundaries of human and organizational capabilities, researching different aspects of Information Technology, statements expressing relationships, *theorize* and *justify* theories about IT artefacts, applicable in practice.

Exercise 2. Read the text. Translate it into Native language.

Text 7. Retell the text.

Research

Information systems research is generally interdisciplinary concerned with the study of the effects of information systems on the behavior of individuals, groups, and organizations. Alan R. Hevner (2004) categorized research in IS into two scientific paradigms including *behavioral science* which is to develop and verify theories that explain or predict human or organizational behavior and *design science* which extends the boundaries of human and organizational capabilities by creating new and innovative artifacts.

Salvatore March and Gerald Smith proposed a framework for researching different aspects of Information Technology including outputs of the research (research outputs) and activities to carry out this research (research activities). They identified research outputs as follows:

1. Constructs which are concepts that form the vocabulary of a domain. They constitute a conceptualization used to describe problems within the domain and to specify their solutions.
2. A model which is a set of propositions or statements expressing relationships among constructs.
3. A *method* which is a set of steps (an algorithm or guideline) used to perform a task. Methods are based on a set of underlying constructs and a representation (model) of the solution space.
4. An instantiation is the realization of an artefact in its environment.

Also research activities including:

1. Build an artefact to perform a specific task.

2. *Evaluate* the artefact to determine if any progress has been achieved.

3. Given an artefact whose performance has been evaluated, it is important to determine why and how the artefact worked or did not work within its environment. Therefore, *theorize* and *justify* theories about IT artefacts.

Although Information Systems as a discipline has been evolving for over 30 years now, the core focus or identity of IS research is still subject to debate among scholars. There are two main views around this debate: a narrow view focusing on the IT artifact as the core subject matter of IS research, and a broad view that focuses on the interplay between social and technical aspects of IT that is embedded into a dynamic evolving context. A third view calls on IS scholars to pay balanced attention to both the IT artifact and its context.

Since the study of information systems is an applied field, industry practitioners expect information systems research to generate findings that are immediately applicable in practice. This is not always the case however, as information systems researchers often explore behavioral issues in much more depth than practitioner would expect them to do. This may render information systems research results difficult to understand, and has led to criticism.

In the last ten years, the business trend is represented by the considerable increase of Information Systems Function (ISF) role, especially with regard to the enterprise strategies and operations supporting. It became a key-factor to increase productivity and to support new value creation. To study an information system itself, rather than its effects, information systems models are used, such as EATPUT.

Unit 8

Memorize the words

enormous [ɪ'nɔːməs] – громадный; гигантский, обширный, огромный

acquire – получать, приобретать, извлекать; достигать; овладевать

regardless [rɪ'gɑːdləs] –безотносительно к чему-либо, невзирая ни на что

maturity [mə'ʧuərətɪ] – завершённость (плана, схемы), последняя стадия развития (какого-л. образования)

incorporate – соединённый, объединённый;

between equals – равноправные обязанности, права

synergy ['sɪnəʤɪ] – успешные совместные усилия; совместная деятельность

Exercise 1. Read the text and find sentences where the following terms are used. Translate them: have enormous strategic value; management information systems; end user computing; managing information resources; the size and nature of the organization, the amount and type of IT resources; the traditional functions and various new, consultative functions of the MIS department; managing systems development, and infrastructure planning.

Exercise 2. Read the text. Translate it into Native language.

Text 8. Retell the text.

Managing Information Resources

Managing information systems in modern organizations is a difficult, complex task. Several factors contribute to this complexity. First, information systems have enormous strategic value to organizations. Firms rely on them so heavily that, in some cases, when these systems are not working (even for a short time), the firm cannot function. (This situation is called "being hostage to information systems.") Second, information systems are very expensive to acquire, operate, and maintain. A third factor contributing to the difficulty in managing information systems is the evolution of the management information systems (MIS) function within the organization. When businesses first began to use computers in the early 1950s, the MIS department "owned" the only computing resource in the organization, the mainframe. At that time, end users did not interact directly with the mainframe. In contrast, in the modern organization, computers are located in all departments, and almost all employees use computers in their work. This situation, known as end user computing, has led to a partnership between the MIS department and the end users. The MIS department now acts as more of a consultant to end users, viewing them as customers. In fact, the main function of the MIS department is to use IT to solve end users' business problems.

As a result of these developments, the responsibility for managing information resources is now divided between the MIS department and the end users. This arrangement raises several important questions: Which resources are managed by whom? What is the role of the MIS department, its structure, and its place within the organization? What is the appropriate relationship between the MIS department and the end users? Regardless of who is doing what, it is essential that the MIS department and the end users work in close cooperation. There is no standard way to divide responsibility for developing and maintaining information resources between the MIS department and the end users. Instead, that division depends on several factors: the size and nature of the organization, the amount and type of IT resources, the organization's attitudes toward computing, the attitudes of top management toward computing, the maturity level of the technology, the amount and nature of outsourced IT work, and even the countries in which the company operates.

Generally speaking, the MIS department is responsible for corporate-level and shared resources, and the end users are responsible for departmental resources. Table 1.2 identifies both the traditional functions and various new, consultative functions of the MIS department. So, where do the end users come in? Take a close look at Table 1. Under the traditional MIS functions, you will see two functions for which you provide vital input: managing systems development, and infrastructure planning. Under the consultative MIS functions, in contrast, you exercise the primary responsibility for each function, while the MIS department acts as your advisor.

Table 1. The Changing Role of the Information Systems Department

Traditional Functions of the MIS Department
• Managing systems development and systems project management ◦ As an end user, you will have critical input into the systems development process. Managing computer operations, including the computer center • Staffing, training, and developing IS skills • Providing technical services • Infrastructure planning, development, and control ◦ As an end user, you will provide critical input about the IS infrastructure needs of your department.
New (Consultative) Functions of the MIS Department
• Initiating and designing specific strategic information systems ◦ As an end user, your information needs will often mandate the development of new strategic information systems. ◦ You will decide which strategic systems you need (because you know your business needs better than the MIS department does), and you will provide input into developing these systems. • Incorporating the Internet and electronic commerce into the business ◦ As an end user, you will be primarily responsible for effectively using the Internet and electronic commerce in your business. You will work with the MIS department to accomplish this task. • Managing system integration including the Internet, intranets, and extranets ◦ As an end user, your business needs will determine how you want to use the Internet, your corporate intranets, and extranets to accomplish your goals. You will be primarily responsible for advising the MIS department on the most effective use of the Internet, your corporate intranets, and extranets. • Educating the non-MIS managers about IT ◦ Your department will be primarily responsible for advising the MIS department on how best to educate and train your employees about IT. • Educating the MIS staff about the business ◦ Communication between the MIS department and the business units is a two-way street. You will be responsible for educating the MIS staff on your business, its needs, and its goals. • Partnering with business-unit executives ◦ Essentially, you will be in a partnership with the MIS department. You will be responsible for seeing that this partnership is one “between equals” and ensuring its success. • Managing outsourcing ◦ Outsourcing is driven by business needs. Therefore, the outsourcing decision resides largely with the business units (i.e., with you). The MIS department, working closely with you, will advise you on technical issues such as communications bandwidth, security, etc. • Proactively using business and technical knowledge to seed innovative ideas about IT ◦ Your business needs often will drive innovative ideas about how to effectively use information systems to accomplish your goals. The best way to bring these innovative uses of IS to life is to partner closely with your MIS department. Such close partnerships have amazing synergies! • Creating business alliances with business partners ◦ The needs of your business unit will drive these alliances, typically along your supply chain. Again, your MIS department will act as your advisor on various issues, including hardware and software compatibility, implementing extranets, communications, and security.

Unit 9

Memorize the words

pillars – пиляры

dashboard – приборная доска; панель приборов; приборная панель; приборный щиток

revenues – доход

funds – фонды предприятия; денежные средства

recruiting – набор персонала, подбор кадров, рекрутинг

standalone – автономная установка, автономная производственная установка || автономный

tightly-integrated modules – плотно интегрированные модули; модули с надёжными связями

transaction processing – обработка транзакций

swipe [swaɪp] – проводить пластиковую карту (через считывающее устройство)

refer [rɪ'fɜː] – относиться, иметь отношение к чему-либо

digitization – оцифровка; дискретизация, преобразование в цифровую форму

determine – определять, устанавливать, решать

hire ['haɪə] – нанимать, предоставлять работу, приглашать на работу

approve of [ə'pruːv] – одобрять что-л., давать официальное согласие; утверждать

Exercise 1. Find in the text following abbreviations and give their full version: FAISs, POM, CAD, CAM, ERP, TPS, MIS, IOSs, B2B, B2C.

Exercise 2. Read the text. Translate it into Native language.

Text 9. Retell the text.

Breadth of Support of Information Systems

Certain information systems support parts of organizations, others support entire organizations, and still others support groups of organizations. This section addresses all of these systems.

Recall that each department or functional area within an organization has its own collection of application programs, or information systems. These *functional area information systems (FAISs)* are supporting pillars for the information systems located at the top of Table 24, namely, business intelligence systems and dashboards. As the name suggests, each FAIS supports a particular functional area within the organization. Examples are accounting IS, finance IS, production/operations management (POM) IS, marketing IS, and human resources IS.

Consider these examples of IT systems in the various functional areas of an organization. In finance and accounting, managers use IT systems to forecast revenues and business activity, to determine the best sources and uses of funds, and to perform audits to ensure that the organization is fundamentally sound and that all financial reports and documents are accurate.

In sales and marketing, managers use information technology to perform the following functions:

Product analysis: developing new goods and services.

Site analysis: determining the best location for production and distribution facilities.

Promotion analysis: identifying the best advertising channels.

Price analysis: setting product prices to obtain the highest total revenues.

Table 2 - Types of Organizational Information Systems

Type of System	Function	Example
Functional area IS	Supports the activities within specific functional area.	System for processing payroll
Transaction processing system	Processes transaction data from business events.	Walmart checkout point-of-sale terminal
Enterprise resource planning	Integrates all functional areas of the organization.	Oracle, SAP system
Office automation system	Supports daily work activities of individuals and groups.	Microsoft® Office
Management information system	Produces reports summarized from transaction data, usually in one functional area.	Report on total sales for each customer
Decision support system	Provides access to data and analysis tools.	“What-if” analysis of changes in budget
Expert system	Mimics human expert in a particular area and makes decisions.	Credit card approval analysis
Executive dashboard	Presents structured, summarized information about aspects of business important to executives.	Status of sales by product
Supply chain management system	Manages flows of products, services, and information among organizations.	Walmart Retail Link system connecting suppliers to Walmart
Electronic commerce system	Enables transactions among organizations and between organizations and customers.	www.dell.com

Marketing managers also use IT to manage their relationships with their customers. In manufacturing, managers use IT to process customer orders, develop production schedules, control inventory levels, and monitor product quality. They also use IT to design and manufacture products. These processes are called computer-assisted design (CAD) and computer-assisted manufacturing (CAM).

Managers in human resources use IT to manage the recruiting process, analyze and screen job applicants, and hire new employees. They also employ IT to help employees manage their careers, to administer performance tests to employees, and to monitor employee productivity. Finally, they rely on IT to manage compensation and benefits packages.

Two information systems support the entire organization: enterprise resource planning systems and transaction processing systems. Enterprise resource planning (ERP) systems are designed to correct a lack of communication among the functional area ISs. For this reason, Table 2 shows ERP systems spanning the FAISs. ERP systems were an important innovation because the various functional area ISs were often developed as standalone systems and did not communicate effectively (if at all) with one another. ERP systems resolve this problem by tightly integrating the functional area ISs via a common database. In doing so, they enhance communications among the functional areas of an organization. For this reason, experts credit ERP systems with greatly increasing organizational productivity.

A transaction processing system (TPS) supports the monitoring, collection, storage, and processing of data from the organization’s basic business transactions, each of which generates data. When you are checking out at Walmart, for example, a transaction occurs each time the cashier swipes an item across the bar code reader. Significantly, within an organization, different functions or departments can define a transaction differently. In accounting, for example, a transaction is anything that changes a firm’s chart of accounts. The information system definition of a transaction is broader: a transaction is anything that changes the firm’s database. The chart of accounts is only part of the firm’s database. Consider a scenario in which a student transfers from one section of an Introduction to MIS course to another section. This move would be a transaction to the university’s information system, but not to the university’s accounting department (the tuition would not change).

The TPS collects data continuously, typically in real time – that is, as soon as the data are generated – and it provides the input data for the corporate databases. TPSs are considered critical to the success of any enterprise because they support core operations. Significantly, nearly all ERP systems are also TPSs, but not all TPSs are ERP systems. In fact, modern ERP systems incorporate many functions that previously were handled by the organization’s functional area information systems.

ERP systems and TPSs function primarily within a single organization. Information systems that connect two or more organizations are referred to as interorganizational information systems (IOSs). IOSs support many interorganizational operations, of which supply chain management is the best known. An organization’s supply chain is the flow of materials, information, money, and services from suppliers of raw materials through factories and warehouses to the end customers.

Note that the supply chain in Table 2 shows physical flows, information flows, and financial flows. Digitizable products are those that can be represented in electronic form, such as music and software. Information flows, financial flows, and digitizable products go through the Internet, whereas physical products are shipped. For example, when you order a computer from www.dell.com, your information goes to Dell via the Internet. When your transaction is completed (i.e., your credit card is approved and your order is processed), Dell ships your computer to you.

Electronic commerce (e-commerce) systems are another type of interorganizational information system. These systems enable organizations to conduct transactions, called business-to-business (B2B) electronic commerce, and customers to conduct transactions with businesses, called business-to-consumer (B2C) electronic commerce.

Unit 10

Memorize the words

execute – осуществлять, выполнять, исполнять (напр., работу, приказ, обязанности); реализовать

capturing – сбор (напр., данных), фиксация

procurement – приобретение, получение; закупка; снабжение

procurement procedure – процедура осуществления закупок и выдачи подрядов

purchase order – заказ на закупку; заказ на поставку

vendors of software – поставщики программного обеспечения

vendors of technology – поставщики технологии

assume [ə's(j)uːm] – принимать, брать на себя (ответственность, управление)

judgement ['ʤʌʤmənt]/to pass/give/render judgement on somebody – выносить приговор кому-л.

Exercise 1. Make up a list of new terms you can find in the text. Translate them into Native language.

Exercise 2. Look through the text. What information did you get about Information Systems and Business Processes?

Text 10. Retell the text.

Information Systems and Business Processes

An information system (IS) is a critical enabler of an organization’s business processes. Information systems facilitate communication and coordination among different functional areas, and allow easy exchange of, and access to, data across processes. Specifically, ISs play a vital role in three areas:

1. Executing the process.
2. Capturing and storing process data.
3. Monitoring process performance.

In this section, you will learn about each of these roles. In some cases, the role is fully automated – that is, it is performed entirely by the IS. In other cases, the IS must rely on the manager’s judgment, expertise, and intuition.

Executing the Process. An IS helps organizations execute processes efficiently and effectively. IS are typically embedded into the processes, and they play a critical role in executing the processes. In other words, an IS and processes are usually intertwined. If the IS does not work, the process cannot be executed. IS help execute processes by informing people when it is time to complete a task, by providing the necessary data to complete the task, and, in some cases, by providing the means to complete the task.

In the procurement process, for example, the IS generates the purchase requisitions and then informs the purchasing department that action on these requisitions is needed. The accountant will be able to view all shipments received to match an invoice that has been received from a supplier and verify that the invoice is accurate. Without the IS, these steps, and therefore the process, cannot be completed. For example, if the IS is not available, how will the warehouse know which orders are ready to pack and ship?

In the fulfillment process, the IS will inform people in the warehouse that orders are ready for shipment. It also provides them with a listing of what materials must be included in the order and where to find those materials in the warehouse.

Capturing and Storing Process Data. Processes create data such as dates, times, product numbers, quantities, prices, and addresses, as well as who did what, when, and where. IS capture and store these data, commonly referred to as process data or transaction data. Some of these data are generated and automatically captured by the IS. These are data related to who completes an activity, when, and where. Other data are generated outside the IS and must be entered into it. This data entry can occur in various ways, ranging from manual entry to automated methods involving data in forms such as bar codes and RFID tags that can be read by machines.

In the fulfillment process, for example, when a customer order is received by mail or over the phone, the person taking the order must enter data such as the customer’s name, what the customer ordered, and how much he or she ordered. Significantly, when a customer order is received via the firm’s Web site, then all customer details are captured by the IS. Data such as the name of the person entering the data (who), at which location the person is completing the task (where), and the date and time (when) are automatically included by the IS when it creates the order. The data are updated as the process steps are executed. When the order is shipped, the warehouse will provide data about which products were shipped and in what quantities, and the IS will automatically include data related to who, when, and where.

An important advantage of using an IS compared to a manual system or multiple functional area information systems is that the data need to be entered into the system only once. Further, once they are entered, other people in the process can easily access them, and there is no need to reenter them in subsequent steps.

The data captured by the IS can provide immediate feedback. For example, the IS can use the data to create a receipt or to make recommendations for additional or alternate products.

Monitoring Process Performance. A third contribution of IS is to help monitor the state of the various business processes. That is, the IS indicates how well a process is executing. The IS performs this role by evaluating information about a process. This information can be created either at the instance level (i.e., a specific task or activity) or the process level (i.e., the process as a whole).

For example, a company might be interested in the status of a particular customer order. Where is the order within the fulfillment process? Was the complete order shipped? If so, when? If not, then when can we expect it to be shipped? Or, for the procurement process, when was the purchase order sent to the supplier? What will be the cost of acquiring the material? At the process level, the IS can evaluate how well the procurement process is being executed by calculating the lead time, or the time between sending the purchase order to a vendor and receiving the goods, for each order and each vendor over time.

Not only can the IS help monitor a process, it can also detect problems with the process. The IS performs this role by comparing the information with a standard—that is, what the company expects or desires—to determine if the process is performing within expectations. Management establishes standards based on organizational goals.

If the information provided by the IS indicates that the process is not meeting the standards, then the company assumes that some type of problem exists. Some problems can be routinely and automatically detected by the IS, whereas others require a person to review the information and make judgments. For example, the IS can calculate the expected date that a specific order will be shipped and determine whether this date will meet the established standard. Or, the IS can calculate the average time taken to fill all orders over the last month and compare this information to the standard to determine if the process is working as expected.

Monitoring business processes, then, helps detect problems with these processes. Very often these problems are really symptoms of a more fundamental problem. In such cases, the IS can help diagnose the cause of the symptoms by providing managers with additional, detailed information. For example, if the average time to process a customer order appears to have increased over the previous month, this problem could be a symptom of a more basic problem.

A manager can then drill down into the information to diagnose the underlying problem. To accomplish this task, the manager can request a breakdown of the information by type of product, customer, location, employees, day of the week, time of day, and so on. After reviewing this detailed information, the manager might determine that the warehouse has experienced an exceptionally high employee turnover rate over the last month and that the delays are occurring because new employees are not sufficiently familiar with the process. The manager might conclude that this problem will work itself out over time, in which case there is nothing more to be done. Alternatively, the manager could conclude that the new employees are not being adequately trained and supervised. In this case, the company must take actions to correct the problem.

Unit 11

Memorize the words

devastating ['devəsteɪtɪŋ] – разрушительный, опустошительный

reveal – выявлять, обнаруживать

exposure [ɪk'spəuʒə] – подвергание какому-л. внешнему воздействию

hack [hæk] – незаконно получать доступ, проникать (в защищённую систему)

intangible cost – нематериальные затраты, неосязаемые затраты (издержки, которые могут быть на законном основании вычтены из налогооблагаемой суммы

breach – нарушение (закона, моральных или материальных обязательств и т. п.)

vulnerability [ˌvʌln(ə)rə'bɪlətɪ] – уязвимость; (vulnerabilities) слабые места в системе защиты

cybercrime ['saɪbəˌkraɪm] – преступления в интернете, сетевая преступность, киберпреступность, киберкриминал

mainframe [meɪnfreɪm] – главный компьютер вычислительного центра, базовое вычислительное устройство

Exercise 1. Think of questions to the following sentences.

a) Information security is especially important to small businesses.

b) Studies have revealed that each security breach costs organization millions of dollars.

c) Security can be defined as the degree of protection against criminal activity, danger, damage, and/or loss.

d) A threat to an information resource is any danger to which a system may be exposed.

Exercise 2. Give a written translation of the text into Native language.

Text 11. Retell the text.

Introduction to Information Security

Information security is especially important to small businesses. Large organizations that experience an information security problem have greater resources to bring to bear on the problem and to enable them to survive. In contrast, small businesses have fewer resources and therefore can be destroyed by a data breach.

Information technologies, when properly used, can have enormous benefits for individuals, organizations, and entire societies. IT has made businesses more productive, efficient, and responsive to consumers. Unfortunately, information technologies can also be misused, often with devastating consequences. Consider the following scenarios:

Individuals can have their identities stolen.

Organizations can have customer information stolen, leading to financial losses, erosion of customer confidence, and legal action.

Countries face the threat of cyberterrorism and cyberwarfare, terms for Internet-based attacks. Cyberwarfare is a critical problem for the U.S. government. In fact, President Obama signed a cyberwarfare directive in October, 2012. In that directive, the White House, for the first time, laid out specific ground rules for how and when the U.S. military can carry out offensive and defensive cyber operations against foreign threats. The directive emphasizes the Obama administration’s focus on cybersecurity as a top priority.

Clearly, the misuse of information technologies has come to the forefront of any discussion of IT. Studies have revealed that each security breach costs organization millions of dollars. For example, after Sony’s PlayStation account database was hacked in 2011, the company had to pay $171 million to rebuild its network and protect users from identity theft. The direct costs of a data breach include hiring forensic experts, notifying customers, setting up telephone hotlines to field queries from concerned or affected customers, offering free credit monitoring, and providing discounts for future products and services. The more intangible costs of a breach include the loss of business from increased customer turnover—called customer churn—and decreases in customer trust.

Unfortunately, employee negligence caused many of the data breaches, meaning that organizational employees are a weak link in information security. It is therefore very important for you to learn about information security so that you will be better prepared when you enter the workforce.

Security can be defined as the degree of protection against criminal activity, danger, damage, and/or loss. Following this broad definition, information security refers to all of the processes and policies designed to protect an organization’s information and information systems (IS) from unauthorized access, use, disclosure, disruption, modification, or destruction. You have seen that information and information systems can be compromised by deliberate criminal actions and by anything that can impair the proper functioning of an organization’s information systems.

Before continuing, let’s consider these key concepts. Organizations collect huge amounts of information and employ numerous information systems that are subject to myriad threats. A threat to an information resource is any danger to which a system may be exposed. The exposure of an information resource is the harm, loss, or damage that can result if a threat compromises that resource. An information resource’s vulnerability is the possibility that the system will be harmed by a threat.

Today, five key factors are contributing to the increasing vulnerability of organizational information resources, making it much more difficult to secure them:

Today’s interconnected, interdependent, wirelessly networked business environment;

Smaller, faster, cheaper computers and storage devices;

Decreasing skills necessary to be a computer hacker;

International organized crime taking over cybercrime;

Lack of management support.

The first factor is the evolution of the IT resource from mainframe-only to today’s highly complex, interconnected, interdependent, wirelessly networked business environment. The Internet now enables millions of computers and computer networks to communicate freely and seamlessly with one another. Organizations and individuals are exposed to a world of untrusted networks and potential attackers. A trusted network, in general, is any network within your organization. An untrusted network, in general, is any network external to your organization. In addition, wireless technologies enable employees to compute, communicate, and access the Internet anywhere and anytime. Significantly, wireless is an inherently nonsecure broadcast communications medium.

The second factor reflects the fact that modern computers and storage devices (e.g., thumb drives or flash drives) continue to become smaller, faster, cheaper, and more portable, with greater storage capacity. These characteristics make it much easier to steal or lose a computer or storage device that contains huge amounts of sensitive information. Also, far more people are able to afford powerful computers and connect inexpensively to the Internet, thus raising the potential of an attack on information assets.

The third factor is that the computing skills necessary to be a hacker are decreasing. The reason is that the Internet contains information and computer programs called scripts that users with few skills can download and use to attack any information system connected to the Internet. (Security experts can also use these scripts for legitimate purposes, such as testing the security of various systems).

The fourth factor is that international organized crime is taking over cybercrime. Cyber-crime refers to illegal activities conducted over computer networks, particularly the Internet. I Defense (http://labs.idefense.com), a company that specializes in providing security information to governments and Fortune 500 companies, maintains that groups of well-organized criminal organizations have taken control of a global billion-dollar crime network. The network, powered by skillful hackers, targets known software security weaknesses. These crimes are typically nonviolent, but quite lucrative. For example, the losses from armed robberies average hundreds of dollars, and those from white-collar crimes average tens of thousands of dollars. In contrast, losses from computer crimes average hundreds of thousands of dollars. Also, computer crimes can be committed from anywhere in the world, at any time, effectively providing an international safe haven for cybercriminals. Computer-based crimes cause billions of dollars in damages to businesses each year, including the costs to repair information systems and the costs of lost business.

The fifth, and final, factor is lack of management support. For the entire organization to take security policies and procedures seriously, senior managers must set the tone. Ultimately, however, lower-level managers may be even more important. These managers are in close con- tact with employees every day and thus are in a better position to determine whether employees are following security procedures.

Unit 12

Memorize the words

deliberate [dɪ'lɪb(ə)rɪt] – тщательно спланированный, преднамеренный, умышленный

threaten ['θret(ə)n] – грозить, угрожать (чем-л.)

perpetrator ['pɜːpɪtreɪtə] – злоумышленник; правонарушитель, преступник

civil disobedience[ˌdɪsə'biːdɪən(t)s] – гражданское неповиновение

keychain drive – флэш-диск, флэш-память небольшое устройство флэш-памяти, имеющее форму продолговатого брелока и подключаемое через USB-порт. Syn: thumb drive USB flash memory

amendment [ə'men(d)mənt] – модернизация; модификация; поправка; коррекция;

Exercise 1. Make up a list of new terms you can find in the text. Translate them into Russian.

Exercise 2. Read the text. Translate it into Native language.

Exercise 3. Make up a detailed plan of each part of the text.

Text 12. Retell each part of the text separately.

Deliberate Threats to Information Systems

There are many types of deliberate threats to information systems. We provide a list of ten common types for your convenience.

1. Espionage or trespass.
2. Information extortion.
3. Sabotage or vandalism.
4. Theft of equipment or information.
5. Identity theft.
6. Compromises to intellectual property.
7. Software attacks.
8. Alien software.
9. Supervisory control and data acquisition (SCADA) attacks.
10. Cyberterrorism and cyberwarfare.

Espionage or Trespass. Espionage or trespass occurs when an unauthorized individual attempts to gain illegal access to organizational information. It is important to distinguish between competitive intelligence and industrial espionage. Competitive intelligence consists of legal information-gathering techniques, such as studying a company's Web site and press releases, attending trade shows, and so on. In contrast, industrial espionage crosses the legal boundary.

Information Extortion. Information extortion occurs when an attacker either threatens to steal, or actually steals, information from a company. The perpetrator demands payment for not stealing the information, for returning stolen information, or for agreeing not to disclose the information.

Sabotage or Vandalism. Sabotage and vandalism are deliberate acts that involve defacing an organization's Web site, possibly damaging the organization's image and causing its customers to lose faith. One form of online vandalism is a hacktivist or cyber activist operation. These are cases of high-tech civil disobedience to protest the operations, policies, or actions of an organization or government agency.

Theft of Equipment or Information. Computing devices and storage devices are becoming smaller yet more powerful with vastly increased storage (e.g., laptops, BlackBerry® units, personal digital assistants, smart phones, digital cameras, thumb drives, and iPods). As a result, these devices are becoming easier to steal and easier for attackers to use to steal information.

In fact, many laptops have been stolen due to such carelessness. The cost of a stolen laptop includes the loss of data, the loss of intellectual property, laptop replacement, legal and regulatory costs, investigation fees, and loss productivity.

One form of theft, known as dumpster diving, involves the practice of rummaging through commercial or residential trash to find information that has been discarded. Paper files, letters, memos, photographs, IDs, passwords, credit cards, and other forms of information can be found in dumpsters. Unfortunately, many people never consider that the sensitive items they throw in the trash may be recovered. Such information, when recovered, can be used for fraudulent purposes.

Dumpster diving is not necessarily theft, because the legality of this act varies. Because dumpsters are usually located on private premises, dumpster diving is illegal in some parts of the United States. Even in these cases, however, these laws are enforced with varying degrees of rigor.

Identity Theft. Identity theft is the deliberate assumption of another person's identity, usually to gain access to his or her financial information or to frame him or her for a crime.

Techniques for illegally obtaining personal information include:

stealing mail or dumpster diving;

stealing personal information in computer databases;

infiltrating organizations that store large amounts of personal information (e.g., data aggregators such as Acxiom) (www.acxiom.com);

impersonating a trusted organization in an electronic communication (phishing).

Recovering from identity theft is costly, time consuming, and difficult. Victims also report problems in obtaining credit and obtaining or holding a job, as well as adverse effects on insurance or credit rates. In addition, victims state that it is often difficult to remove negative information from their records, such as their credit reports.

Your personal information can be compromised in other ways. For example, your identity can be uncovered just by examining your searches in a search engine. The ability to analyze all searches by a single user can enable a criminal to identify who the user is and what he or she is doing. To demonstrate this fact, The New York Times tracked down a particular individual based solely on her AOL searches.

Compromises to Intellectual Property. Protecting intellectual property is a vital issue for people who make their livelihood in knowledge fields. Intellectual property is the property created by individuals or corporations that is protected under trade secret, patent, and copyright laws.

A trade secret is an intellectual work, such as a business plan, that is a company secret and is not based on public information. An example is the Coca-Cola formula. A patent is an official document that grants the holder exclusive rights on an invention or a process for a specified period of time. Copyright is a statutory grant that provides the creators or owners of intellectual property with ownership of the property, also for a designated period. Current U.S. laws award patents for 20 years and copyright protection for the life of the creator plus 70 years. Owners are entitled to collect fees from anyone who wants to copy their creations. It is important to note that these are definitions under U.S. law. There is some international standardization of copyrights and patents, but it is far from total. Therefore, there can be discrepancies between U.S. law and other countries' laws.

The most common intellectual property related to IT deals with software. In 1980, the U.S. Congress amended the Copyright Act to include software. The amendment provides protection for the source code and object code of computer software, but it does not clearly identify what is eligible for protection. For example, copyright law does not protect fundamental concepts, functions, and general features such as pull-down menus, colors, and icons. However, copying a software program without making payment to the owner—including giving a disc to a friend to install on his or her computer—is a copyright violation. Not surprisingly, this practice, called piracy, is a major problem for software vendors. The BSA (www.bsa.org) Global Software Piracy Study found that the commercial value of software theft totals billions of dollars per year. The chapter opening case points out the size of this problem.

Software Attacks. Software attacks have evolved from the early years of the computer era, when attackers used malicious software to infect as many computers worldwide as possible, to the profit-driven, Web-based attacks of today. Modern cybercriminals use sophisticated, blended malware attacks, typically via the Web, to make money. Table 3 displays a variety of software attacks. These attacks are grouped into three categories: remote attacks requiring user action; remote attacks requiring no user action; and software attacks by programmers during the development of a system. IT's About Business 3 provides an example of a software attack.

Table 3 - A variety of software attacks

Types of Software Attacks	**Description**
	(1) Remote Attacks Requiring User Action
Virus	Segment of computer code that performs malicious actions by attaching to another computer program.
Worm	Segment of computer code that performs malicious actions and will replicate, or spread, by itself (without requiring another computer program).
Phishing Attack	Phishing attacks use deception to acquire sensitive personal information by masquerading as official-looking e-mails or instant messages.
Spear Phishing Attack	Phishing attacks target large groups of people. In spear phishing attacks, the perpetrators find out as much information about an individual as possible to improve their chances that phishing techniques will be able to obtain sensitive, personal information.
	(2) Remote Attacks Needing No User Action
Denial-of-Service Attack	Attacker sends so many information requests to a target computer system that the target cannot handle them successfully and typically crashes (ceases to function).
Distributed Denial-of-Service	An attacker first takes over many computers, typically by using malicious software. These computers are called zombies or bots. The attacker uses these bots—which form a botnet—to deliver a

Attack	coordinated stream of information requests to a target computer, causing it to crash.
(3) Attacks by a Programmer Developing a System	
Trojan Horse	Software programs that hide in other computer programs and reveal their designed behavior only when they are activated.
Back Door	Typically a password, known only to the attacker, that allows him or her to access a computer system at will, without having to go through any security procedures (also called a trap door).
Logic Bomb	Segment of computer code that is embedded within an organization's existing computer programs and is designed to activate and perform a destructive action at a certain time or date.

Alien Software. Many personal computers have alien software, or pestware, running on them that the owners do not know about. Alien software is clandestine software that is installed on your computer through duplicitous methods. It typically is not as malicious as viruses, worms, or Trojan horses, but it does use up valuable system resources. In addition, it can report on your Web surfing habits and other personal behavior.

The vast majority of pestware is adware – software that causes pop-up advertisements to appear on your screen. Adware is common because it works. According to advertising agencies, for every 100 people who close a pop-up ad, 3 click on it. This "hit rate" is extremely high for Internet advertising.

Spyware is software that collects personal information about users without their consent. Two common types of spyware are keystroke loggers and screen scrapers. Keystroke loggers, also called key loggers, record both your individual keystrokes and your Internet Web browsing history. The purposes range from criminal – for example, theft of passwords and sensitive personal information such as credit card numbers – to annoying – for example, recording your Internet search history for targeted advertising.

Companies have attempted to counter key loggers by switching to other forms of identifying users. For example, at some point all of us have been forced to look at wavy, distorted letters and type them correctly into a box. That string of letters is called a CAPTCHA, and it is a test. The point of CAPTCHA is that computers cannot (yet) accurately read those distorted letters. Therefore, the fact that you can transcribe them means that you are probably not a software program run by an unauthorized person, such as a spammer. As a result, attackers have turned to screen scrapers, or screen grabbers. This software records a continuous "movie" of a screen's contents rather than simply recording keystrokes.

Spam ware is pestware that uses your computer as a launch pad for spammers. Spam is unsolicited e-mail, usually advertising for products and services. When your computer is infected with spam ware, e-mails from spammers are sent to everyone in your e-mail address book, but they appear to come from you.

Not only is spam a nuisance, but it wastes time and money. Spam costs U.S. companies billions of dollars per year. These costs come from productivity losses, clogged e-mail systems, additional storage, user support, and antispam software. Spam can also carry viruses and worms, making it even more dangerous.

Cookies are small amounts of information that Web sites store on your computer, temporarily or more or less permanently. In many cases, cookies are useful and innocuous. For example, some cookies are passwords and user IDs that you do not want to retype every time you access the Web site that issued the cookie. Cookies are also necessary for online shopping because merchants use them for your shopping carts.

Tracking cookies, however, can be used to track your path through a Web site, the time you spend there, what links you click on, and other details that the company wants to record, usually for marketing purposes. Tracking cookies can also combine this information with your name, purchases, credit card information, and other personal data to develop an intrusive profile of your spending habits.

Most cookies can be read only by the party that created them. However, some companies that manage online banner advertising are, in essence, cookie-sharing rings. These companies can track information such as which pages you load and which ads you click on. They then share this information with their client Web sites, which may number in the thousands. For a cookie demonstration, see http://privacy.net/track/.

Supervisory Control and Data Acquisition (SCADA) Attacks. SCADA refers to a large-scale, distributed measurement and control system. SCADA systems are used to monitor or to control chemical, physical, and transport processes such as those used in oil refineries, water and sewage treatment plants, electrical generators, and nuclear power plants. Essentially, SCADA systems provide a link between the physical world and the electronic world.

SCADA systems consist of multiple sensors, a master computer, and communications infra- structure. The sensors connect to physical equipment. They read status data such as the open / closed status of a switch or a valve, as well as measurements such as pressure, flow, voltage, and current. They control the equipment by sending signals to it, such as opening or closing a switch or a valve or setting the speed of a pump.

The sensors are connected in a network, and each sensor typically has an Internet address (Internet Protocol, or IP, address, discussed in Chapter 6). If attackers gain access to the net- work, they can cause serious damage, such as disrupting the power grid over a large area or upsetting the operations of a large chemical or nuclear plant. Such actions could have catastrophic results, as described in IT's About Business.

Cyberterrorism and Cyberwarfare. Cyberterrorism and cyberwarfare refer to malicious acts in which attackers use a target's computer systems, particularly via the Internet, to cause physical, real-world harm or severe disruption, usually to carry out a political agenda (see IT’s About Business 4.3). These actions range from gathering data to attacking critical infrastructure (e.g., via SCADA systems).

Unit 13

Memorize the words

recovery of damages – возмещение ущерба

deserve [dɪ'zəːv] – заслуживать, быть достойным (чего-либо)

embedded chip = embedded computer chip – заделанная (напр. в инструментальную оправку) микросхема

firewall ['faɪəwɔːl] – межсетевой экран, брандмауэр (аппаратные или программные средства межсетевой защиты)

demilitarized zone – демилитаризированная территория, демилитаризованная зона

malicious software – вредоносное ПО, вредоносные программные средства

infected system – инфицированная система, заражённая [вирусом] система

whitelisting – технология "белых списков" одно из организационных средств борьбы со спамом – составление и ведение списков "проверенных", надёжных серверов, от которых можно принимать почту

peer-to-peer [ˌpɪətə'pɪə] – P2P пиринговый, децентрализованный

P2P network – сеть P2P, пиринговая сеть

Exercise 1. Make up a list of new terms you can find in the text. Translate them into Russian.

Exercise 2. Read the text. Translate it into Native language.

Exercise 3. Make up a detailed plan of each part of the text.

Text 13. Retell each part of the text separately.

Information Security Control

To protect their information assets, organizations implement controls, or defense mechanisms (also called countermeasures). These controls are designed to protect all of the components of an information system, including data, software, hardware, and networks. Because there are so many diverse threats, organizations utilize layers of controls, or defense-in-depth.

Controls are intended to prevent accidental hazards, deter intentional acts, detect problems as early as possible, enhance damage recovery, and correct problems. Before you study controls in more detail, it is important to emphasize that the single most valuable control is user education and training. Effective and ongoing education makes every member of the organization aware of the vital importance of information security.

In the next section, you will learn about three major types of controls: physical controls, access controls, and communications controls. Figure 4.2 illustrates these controls. In addition to applying controls, organizations plan for business continuity in case of a disaster, and they periodically audit their information resources to detect possible threats. You will study these topics in the next section as well.

Physical Controls

Physical controls prevent unauthorized individuals from gaining access to a company's facilities. Common physical controls include walls, doors, fencing, gates, locks, badges, guards, and alarm systems. More sophisticated physical controls include pressure sensors, temperature sensors, and motion detectors. One shortcoming of physical controls is that they can be inconvenient to employees.

Guards deserve special mention because they have very difficult jobs, for at least two reasons. First, their jobs are boring and repetitive and generally do not pay well. Second, if guards perform their jobs thoroughly, the other employees harass them, particularly if they slow up the process of entering the facility.

Organizations also implement physical security measures that limit computer users to acceptable login times and locations. These controls also limit the number of unsuccessful login attempts, and they require all employees to log off their computers when they leave for the day. In addition, they set the employees' computers to automatically log off the user after a certain period of disuse.

Access Controls

Access controls restrict unauthorized individuals from using information resources. These controls involve two major functions: authentication and authorization. Authentication confirms the identity of the person requiring access. After the person is authenticated (identified), the next step is authorization. Authorization determines which actions, rights, or privileges the person has, based on his or her verified identity. Let's examine these functions more closely.

Authentication. To authenticate (identify) authorized personnel, an organization can use one or more of the following methods: something the user is, something the user has, something the user does, and/or something the user knows.

Something the user is, also known as biometrics, is an authentication method that examines a person's innate physical characteristics. Common biometric applications are fingerprint scans, palm scans, retina scans, iris recognition, and facial recognition. Of these applications, fingerprints, retina scans, and iris recognition provide the most definitive identification. The following example shows how powerful biometrics can be for identification purposes.

Something the user has is an authentication mechanism that includes regular identification (ID) cards, smart ID cards, and tokens. Regular ID cards, or dumb cards, typically have the person's picture and often his or her signature. Smart ID cards have an embedded chip that stores pertinent information about the user. (Smart ID cards used for identification differ from smart cards used in electronic commerce. Both types of card have embedded chips, but they are used for different purposes.) Tokens have embedded chips and a digital display that presents a login number that the employees use to access the organization’s network. The number changes with each login.

Something the user does is an authentication mechanism that includes voice and signature recognition. In voice recognition, the user speaks a phrase (e.g., his or her name and department) that has been previously recorded under controlled conditions. The voice recognition system matches the two voice signals. In signature recognition, the user signs his or her name, and the system matches this signature with one previously recorded under controlled, monitored conditions. Signature recognition systems also match the speed and the pressure of the signature.

Something the user knows is an authentication mechanism that includes passwords and passphrases. Passwords present a huge information security problem in all organizations. Most of us have to remember numerous passwords for different online services, and we typically must choose complicated strings of characters to make them harder to guess. Security experts examined the frequency and usage of passwords belonging to 500,000 computer users. They found that each person had an average of 6.5 passwords that he or she used for 25 different online accounts. Unfortunately, as you see in the chapter’s closing case, passwords (even strong passwords) are terribly vulnerable to attack.

All users should use strong passwords, which are difficult for hackers to discover. The basic guidelines for creating strong passwords are:

1. They should be difficult to guess.
2. They should be long rather than short.
3. They should have uppercase letters, lowercase letters, numbers, and special characters.

They should not be recognizable words.

They should not be the name of anything or anyone familiar, such as family names or names of pets.

They should not be a recognizable string of numbers, such as a Social Security number or a birthday.

Unfortunately, strong passwords are more difficult to remember than weak ones. Consequently, employees frequently write them down, which defeats their purpose. The ideal solution to this dilemma is to create a strong password that is also easy to remember. To achieve this objective, many people use passphrases.

A passphrase is a series of characters that is longer than a password but is still easy to memorize. Examples of passphrases are “may the force be with you always” and “go ahead make my day.” A passphrase can serve as a password itself, or it can help you create a strong password. You can turn a passphrase into a strong password in this manner. Starting with the last passphrase above, take the first letter of each word. You will have “gammed.” Then, capitalize every other letter to create “GaMmD”. Finally, add special characters and numbers to create “9GaMmD//*”. You now have a strong password that you can remember.

To identify authorized users more efficiently and effectively, organizations frequently implement more than one type of authentication, a strategy known as multifactor authentication. This system is particularly important when users log in from remote locations.

Single-factor authentication, which is notoriously weak, commonly consists simply of a password. Two-factor authentication consists of a password plus one type of biometric identification (e.g., a fingerprint). Three-factor authentication is any combination of three authentication methods. In most cases, the more factors the system utilizes, the more reliable it is. However, stronger authentication is also more expensive, and, as with strong passwords, it can be irritating to users.

Authorization. After users have been properly authenticated, the rights and privileges they have on the organization’s systems are established in a process called authorization. A privilege is a collection of related computer system operations that a user is authorized to perform. Companies typically base authorization policies on the principle of least privilege, which posits that users be granted the privilege for an activity only if there is a justifiable need for them to perform that activity.

Communications Controls

Communications controls (also called network controls) secure the movement of data across networks. Communications controls consist of firewalls, anti-malware systems, whitelisting and blacklisting, encryption, virtual private networks (VPNs), secure socket layer (SSL), and employee monitoring systems.

Firewalls. A firewall is a system that prevents a specific type of information from moving between untrusted networks, such as the Internet, and private networks, such as your company’s network. Put simply, firewalls prevent unauthorized Internet users from accessing private networks. All messages entering or leaving your company’s network pass through a firewall. The firewall examines each message and blocks those that do not meet specified security rules.

Firewalls range from simple, for home use, to very complex for organizational use. In this case, the firewall is implemented as software on the home computer. Corporate firewalls typically consist of software running on a computer dedicated to the task. A demilitarized zone (DMZ) is located between the two firewalls. Messages from the Inter- net must first pass through the external firewall. If they conform to the defined security rules, they are then sent to company servers located in the DMZ. These servers typically handle Web page requests and e-mail. Any messages designated for the company’s internal network (e.g., its intranet) must pass through the internal firewall, again with its own defined security rules, to gain access to the company’s private network.

The danger from viruses and worms is so severe that many organizations are placing firewalls at strategic points inside their private networks. In this way, if a virus or worm does get through both the external and internal firewalls, then the internal damage may be contained.

Anti-malware Systems

Anti-malware systems, also called antivirus, or AV, software, are software packages that attempt to identify and eliminate viruses and worms, and other malicious software. AV software is implemented at the organizational level by the information systems department. There are currently hundreds of AV software packages available. Among the best known are Norton Antivirus (www.symantec.com), McAfee Virus Scan (www.mcafee.com), and Trend Micro PC-cillin (www.trendmicro.com). IT’s About Business 4.4 provides an example of how a software program known as FireEye helps protect organizations from malware

Anti-malware systems are generally reactive. Whereas firewalls filter network traffic according to categories of activities likely to cause problems, anti-malware systems filter traffic according to a database of specific problems. These systems create definitions, or signatures, of various types of malware and then update these signatures in their products. The anti-malware software then examines suspicious computer code to determine whether it matches a known signature. If the software identifies a match, it removes the code. For this reason, organizations regularly update their malware definitions.

Because malware is such a serious problem, the leading vendors are rapidly developing anti-malware systems that function proactively as well as reactively. These systems evaluate behavior rather than relying entirely on signature matching. In theory, therefore, it is possible to catch malware before it can infect systems.

Whitelisting and Blacklisting. A report by the Yankee Group (www.yankeegroup.com), a technology research and consulting firm, stated that 99 percent of organizations had installed anti-malware systems, but 62 percent still suffered malware attacks. As we have seen, anti- malware systems are usually reactive, and malware continues to infect companies.

One solution to this problem is whitelisting. Whitelisting is a process in which a company identifies the software that it will allow to run on its computers. Whitelisting permits accept- able software to run, and it either prevents any other software from running or it lets new software run in a quarantined environment until the company can verify its validity.

Whereas whitelisting allows nothing to run unless it is on the whitelist, blacklisting allows everything to run unless it is on the blacklist. A blacklist, then, includes certain types of soft- ware that are not allowed to run in the company environment. For example, a company might blacklist peer-to-peer file sharing on its systems. In addition to software, people, devices, and Web sites can also be whitelisted and blacklisted.

Encryption

Organizations that do not have a secure channel for sending information use encryption to stop unauthorized eavesdroppers. Encryption is the process of converting an original message into a form that cannot be read by anyone except the intended receiver.

All encryption systems use a key, which is the code that scrambles and then decodes the messages. The majority of encryption systems use public-key encryption. Public-key encryption— also known as asymmetric encryption—uses two different keys: a public key and a private key (see Figure 4.4). The public key (locking key) and the private key (the unlocking key) are created simultaneously using the same mathematical formula or algorithm. Because the two keys are mathematically related, the data encrypted with one key can be decrypted by using the other key. The public key is publicly available in a directory that all parties can access. The private key is kept secret, never shared with anyone, and never sent across the Internet. In this system, if Han- nah wants to send a message to Harrison, she first obtains Harrison's public key (locking key), which she uses to encrypt her message (put the message in the "two lock box"). When Harrison receives Hannah's message, he uses his private key to decrypt it (open the box).

Although this arrangement is adequate for personal information, organizations that con- duct business over the Internet require a more complex system. In these cases, a third party, called a certificate authority, acts as a trusted intermediary between the companies. The certificate authority issues digital certificates and verifies the integrity of the certificates. A digital certificate is an electronic document attached to a file that certifies that the file is from the organization it claims to be from and has not been modified from its original format. As you can see in Figure 4.5, Sony requests a digital certificate from VeriSign, a certificate authority, and uses this certificate when it conducts business with Dell. Note that the digital certificate contains an identification number, the issuer, validity dates, and the requester's public key. For examples of certificate authorities, see www.entrust.com, www.verisign.com, www.cybertrust.com, www.secude. com, and www.thawte.com.

Virtual Private Networking. A virtual private network is a private network that uses a public network (usually the Internet) to connect users. VPNs essentially integrate the global connectivity of the Internet with the security of a private network and thereby extend the reach of the organization's networks. VPNs are called virtual because they have no separate physical existence. They use the public Internet as their infrastructure. They are created by using log-ins, encryption, and other techniques to enhance the user's privacy, the right to be left alone and to be free of unreasonable personal intrusion.

VPNs have several advantages. First, they allow remote users to access the company net- work. Second, they provide flexibility. That is, mobile users can access the organization's network from properly configured remote devices. Third, organizations can impose their security policies through VPNs. For example, an organization may dictate that only corporate e-mail applications are available to users when they connect from unmanaged devices.

To provide secure transmissions, VPNs use a process called tunneling. Tunneling encrypts each data packet to be sent and places each encrypted packet inside another packet. In this manner, the packet can travel across the Internet with confidentiality, authentication, and integrity. Figure 4.6 illustrates a VPN and tunneling.

Secure Socket Layer. Secure socket layer, now called transport layer security (TLS), is an encryption standard used for secure transactions such as credit card purchases and online banking. TLS encrypts and decrypts data between a Web server and a browser end to end.

TLS is indicated by a URL that begins with “https” rather than “http,” and it often displays a small padlock icon in the browser’s status bar. Using a padlock icon to indicate a secure connection and placing this icon in a browser’s status bar are artifacts of specific browsers. Other browsers use different icons (e.g., a key that is either broken or whole). The important thing to remember is that browsers usually provide visual confirmation of a secure connection.

Employee Monitoring Systems. Many companies are taking a proactive approach to protecting their networks against what they view as one of their major security threats, namely, employee mistakes. These companies are implementing employee monitoring systems, which monitor their employees’ computers, e-mail activities, and Internet surfing activities. These products are useful to identify employees who spend too much time surfing on the Internet for personal reasons, who visit questionable Web sites, or who download music illegally. Vendors that provide monitoring software include Spector Soft (www.spectorsoft.com) and Websense (www.websense.com).

Business Continuity Planning

An important security strategy for organizations is to be prepared for any eventuality. A critical element in any security system is a business continuity plan, also known as a disaster recovery plan.

Business continuity is the chain of events linking planning to protection and to recovery. The purpose of the business continuity plan is to provide guidance to people who keep the business operating after a disaster occurs. Employees use this plan to prepare for, react to, and recover from events that affect the security of information assets. The objective is to restore the business to normal operations as quickly as possible following an attack. The plan is intended to ensure that critical business functions continue.

In the event of a major disaster, organizations can employ several strategies for business continuity. These strategies include hot sites, warm sites, and cold sites. A hot site is a fully configured computer facility, with all services, communications links, and physical plant operations. A hot site duplicates computing resources, peripherals, telephone systems, applications, and workstations. A warm site provides many of the same services and options as the hot site. However, it typically does not include the actual applications the company needs. A warm site includes computing equipment such as servers, but it often does not include user workstations. A cold site provides only rudimentary services and facilities, such as a building or a room with heating, air conditioning, and humidity control. This type of site provides no computer hardware or user workstations. The point of a cold site is that it takes care of long lead-time issues. Building, or even renting, space takes a long time. Installing high-speed communication lines, often from two or more carriers, takes a long time. Installing high-capacity power lines takes a long time. By comparison, buying and installing servers should not take a particularly long time.

Hot sites reduce risk to the greatest extent, but they are the most expensive option. Conversely, cold sites reduce risk the least, but they are the least expensive option.

Information Systems Auditing

Companies implement security controls to ensure that information systems work properly. These controls can be installed in the original system, or they can be added after a system is in operation. Installing controls is necessary but not sufficient to provide adequate security. In addition, people responsible for security need to answer questions such as: Are all controls installed as intended? Are they effective? Has any breach of security occurred? If so, what actions are required to prevent future breaches?

These questions must be answered by independent and unbiased observers. Such observers perform the task of information systems auditing. In an IS environment, an audit is an examination of information systems, their inputs, outputs, and processing.

Types of Auditors and Audits. There are two types of auditors and audits: internal and external. IS auditing is usually a part of accounting internal auditing, and it is frequently per- formed by corporate internal auditors. An external auditor reviews the findings of the internal audit as well as the inputs, processing, and outputs of information systems. The external audit of information systems is frequently a part of the overall external auditing performed by a certified public accounting (CPA) firm.

IS auditing considers all of the potential hazards and controls in information systems. It focuses on issues such as operations, data integrity, software applications, security and privacy, budgets and expenditures, cost control, and productivity. Guidelines are available to assist auditors in their jobs, such as those from the Information Systems Audit and Control Association (www.isaca.org).

How is Auditing Executed? IS auditing procedures fall into three categories: auditing around the computer, auditing through the computer, and auditing with the computer.

Auditing around the computer means verifying processing by checking for known outputs using specific inputs. This approach is best used in systems with limited outputs. In auditing through the computer, auditors check inputs, outputs, and processing. They review program logic, and they test the data contained within the system. Auditing with the computer means using a combination of client data, auditor software, and client and auditor hardware. This approach enables the auditor to perform tasks such as simulating payroll program logic using live data.

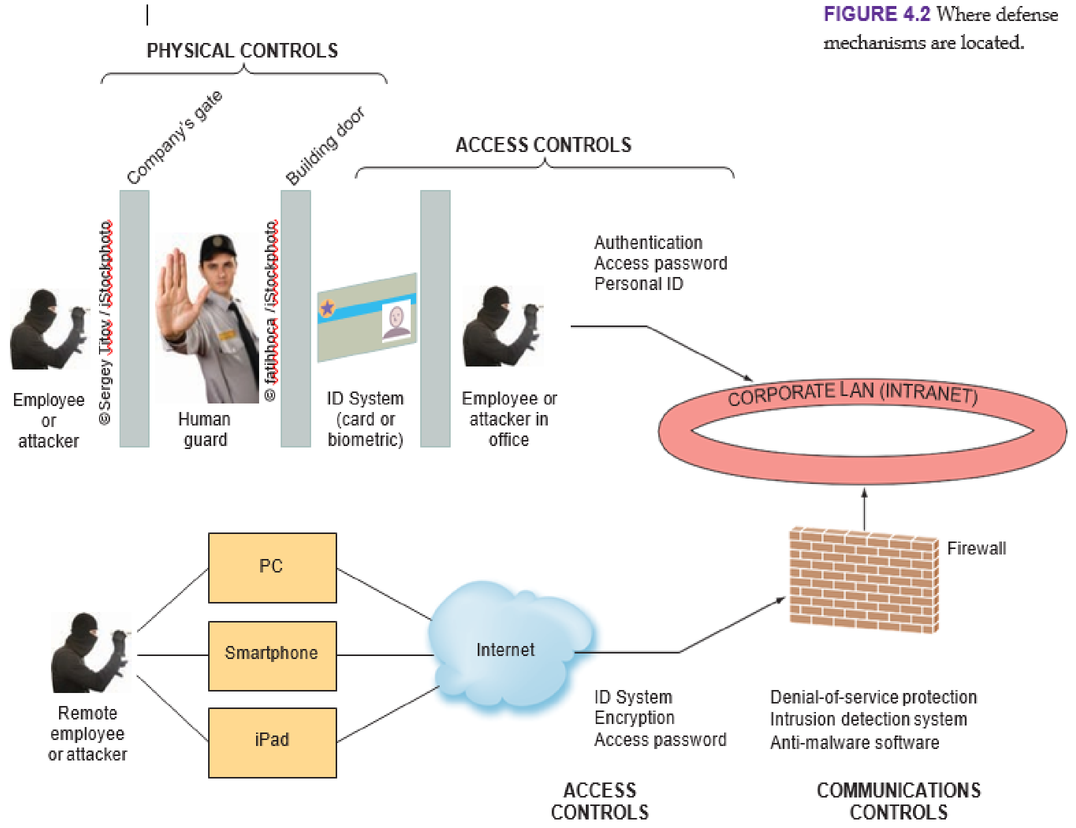

FIGURE 4.2 Where defense mechanisms are located.

Figure 2

List of literature

1 Information systems foundations: theory, representation and reality by Dennis N. Hart and Shirley D. Gregor, Published by ANU E Press, The Australian National University, Canberra ACT 2010, Australia.

2 Amami M, Beghini G, La Manna M. Use of project management information system for planning information systems development projects. Int J Project Manage. 2013; 11(1): 21–8.

3 Голикова Ж.А. Learn to Translate by Translating from English into Russian. – М.: Высшая школа, 2007 .

4 R.Kelly Rainer Jr., Brad Prince, Casey Cegielski – Introduction to Information Systems. Fifth Edition at www.wiley.com/go/returnlabel. Outside of the United States, please contact your local representative, 2017.

5 Kautz, K., & Bjerknes, G. (2015). Tales of IT consultants: Understanding psychological contract maintenance and employment termination. Australasian Journal of Information Systems, 19, 71-95.

6 Kautz, K., Bjerknes, G., Fisher, J. & Jensen, T. (2018). A process model of co-creation as an approach to information systems development. In Proceedings of the 27th International Conference on Information Systems Development.

7 Kautz, K., Bjerknes, G., Fisher, J. & Jensen, T. (2019). The process of co-creation in information systems development: A case study of a digital game development project. In B. Andersson, B. Johansson, C. Barry, M. Lang, H. Linger, C. Schneider (Eds.), Advances in information systems development: Designing digitalization (pp. 187-206). Cham, Switzerland: Springer.

8 Kautz, K., Bjerknes, G., Fisher, J., & Jensen, T. (2020). Applying complex adaptive systems theory to understand distributed participatory design in crow.

9 Urbach, N., & Ahlemann, F. (2019). IT management in the digital age. Cham, Switzerland: Springer.

10 Rolland, K., Mathiassen, L., & Rai, A. (2018). Managing digital platforms in user organizations: The interaction between digital options and digital debt. Information Systems Research, 29(20), 419- 443.

11 www.wiley.com/college/rainer (дата обращения: 20.10.2020).

12 https://en.wikipedia.org/wiki/Information_management (дата обращения: 20.10.2020).

13 Technology. Accessed May 1, 2017: http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=152106 (дата обращения: 20.10.2020).

14 http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf (дата обращения: 20.10.2020).

Contents

Summary plan 2020, pos.42

Жулдыз Кенжетаевна Байгаскина

PROFESSIONAL ORIENTED FOREIGN LANGUAGE

Methodical Recommendations to work with special texts
for the students of Information System and
technology specialty – 5B070300

Editor: Курманбекова М.Д.

Specialist for standardization : Данько Е.Т.

Signed for publication «___»___2020 Format 60x84 1/16
Edition 50 copies Typographical paper №1
Volume 2,8 quires Order ___. Price _1400 *tg*.

Non-Profit JSC «AUPET»
126, Baytursynov st., Almaty

Copying-duplicating bureau of
Non-Profit Joint Stock Company
«Almaty University of Power Engineering and Telecommunications»
named after Gumarbek Daukeev
050013, 126/1, Baytursynov str., Almaty