Lukinova O.V.

BUSINESS PROCESS DESIGN METHOD INSURING INFORMATION SYSTEM SECURITY BASED ON INTERCATEGORICAL REPRESENTATION OF PROTECTION PLANES IN OSE\RM MODELS

The paper describes the procedure for building business processes insuring the security of information system resources, which is the environment of an enterprise's automated business processes operation and represented in the form of a reference model of an open environment.

Keywords: *integrated system of protection, information system, the OSE\RM model, business process, protection mechanism.*

Introduction

Nowadays, the development of any more or less reliable information system involves the use of a particular technology, the initial phase of which consists in modeling of an enterprise's business processes or some area of its activity [1], which should be automated. The aggregate of such business processes is actually a model of the company, which subsequently implemented in the form of an information system. This methodology allows us:

1. To become aware of and build the hierarchy of objectives to be met by a future system;

2. To develop a set of system requirements, sufficient to implement the desired system functionality;

3. To "play" with a simulation model of future business processes with the purpose of their optimizing or better structuring. To do this, today there are a number of tools, such as BPEL, CaseWeise etc.

The authors used a similar approach to the process of designing an *integrated system of protection* (ISP) for IS, i.e. the task consisted in:

a) Designing business processes to ensure the security of information systems and implemented in the form of ISP applications,

b) Finding a way to formalize these business processes.

Problem formulation of IS protection

Problem formulation of IS protection, which is an implementation of the aggregate business processes, should include, according to the authors, the following factors (Figure 1):

1. IS as an object of protection, on the one hand, and as an information business model, on the other hand. At the same time, business relevance of data flows handled by an enterprise business process or of the functions themselves determines the level of protection and damage to businesses inflicted in case of protection violation.

2. The target function for ISP should be stated as ensuring basic properties of security of information system data and computing resources, namely: *confidentiality (K), integrity (C)* and *accessibility (D).* Confidentiality is understood as a restriction of access to resources in their storage, processing or transmission. Integrity is defined by immutability of the resource in the course of its transmission or storage (the possibility of its modification only by authorized persons). Accessibility is the possibility of legitimate users to receive a certain service in a given period. Sometimes this subset includes the nonrepudiation requirement of actions occurring in the system. To evaluate the objective function, the criteria of the same name are introduced, such as security vector $\overline{KS}(C,D,K)$, or $\{\overline{KS}\}=\{C,D,K,N\}$, where N is the nonrepudiation requirement of actions, which measurement is made by means of a linguistic or scoring scale. These scales allow measuring and setting the level of security required, and the values of the level are determined by components' significance of an enterprise business process.

3. External impacts that can disrupt the target function are potentially dangerous threats. Such threats are characterized by the probability of occurrence, which is defined by the presence of an intruder, and by the probability of software and hardware vulnerability implementation.

4. Defense mechanisms (*Mx*) represent control parameters, insuring a predefined level of the target function $\overline{KS}(C,D,K)$.

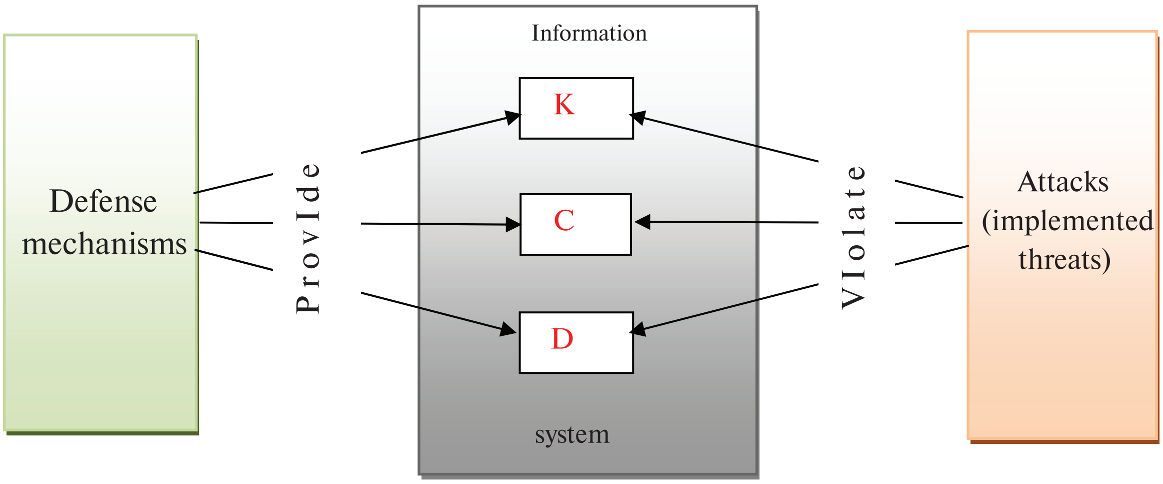


Fig. 1. The layout of the problem formulation of insuring IS security

Next, the task arises of presenting IS as an object of protection in the form of a model, and at that the model should fully reflect IS functionality and allow decomposing the main objectives by the functional groups of protection objects.

To represent IS, we used the Open System Environment/Reference Model (OSE/RM), which describes the reference functionality of the architecture and the structure of information system. This model has been developed by the POSIX group and described in the standard [2, 3].

The model consists of two components. These applications actually implement both the functions of an enterprise business process and business process protection, and the platform that provides operation of applications by the system services that are performed by invoking API functions.

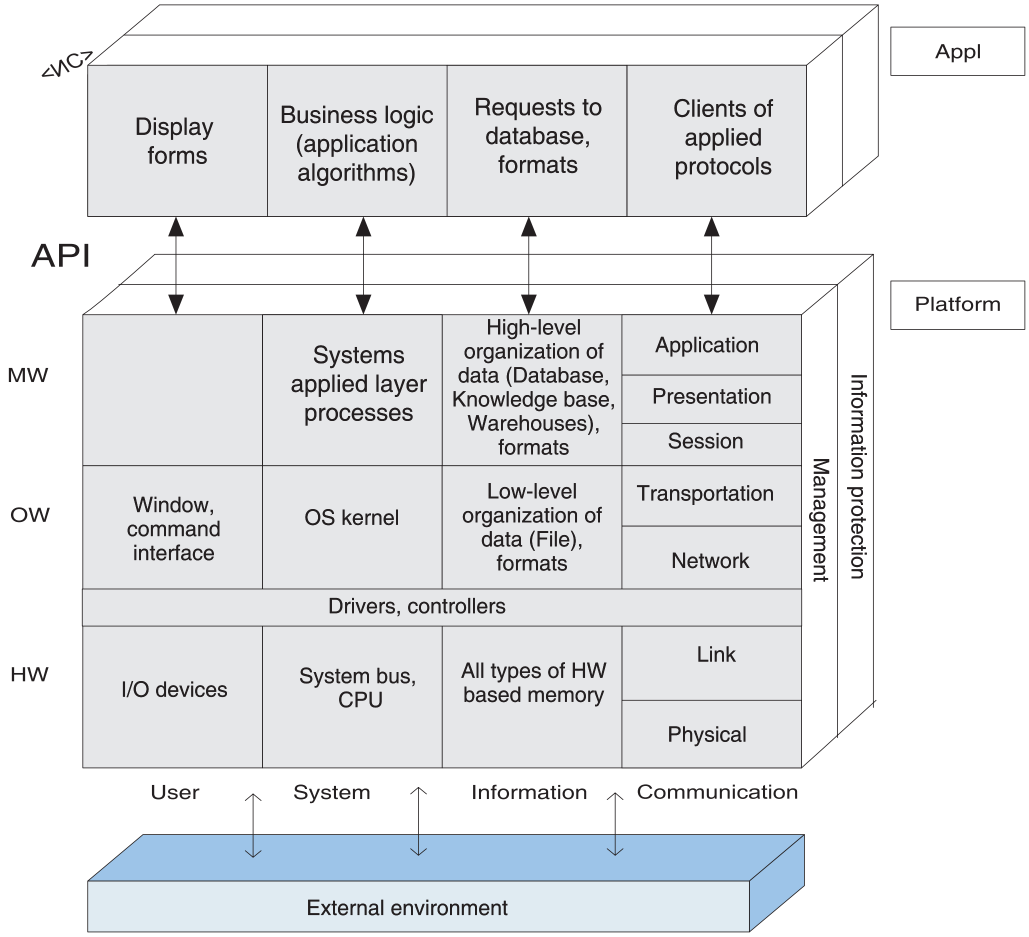

<ИС>
Appl
Display forms
Business logic (application algorithms)
Requests to database, formats
Clients of applied protocols
API
Platform
MW
OW
HW
Systems applied layer processes
High-level organization of data (Database, Knowledge base, Warehouses), formats
Application
Presentation
Session
Window, command interface
OS kernel
Low-level organization of data (File), formats
Transportation
Network
Drivers, controllers
I/O devices
System bus, CPU
All types of HW based memory
Link
Physical
Management
Information protection
User
System
Information
Communication
External environment

Fig. 2. OSE\RM Model

Front reference plane <IS> is intended to structure the functions related directly to the implementation of the IS itself. It comprises of the three levels, and four groups of functional component in each level. These levels include the following:

- service components and utilities of middleware (MW);
- components of the operating systems or operating layer (OW);
- hardware layer (HW).

Functional groups of components in the given model are:

- components that provide the user interface (*User* – “U”);
- components that provide all the necessary processes in the system (*System* – “S”);
- components that support the organization, presentation, access data storage (*Information* – “I”);
- components of telecommunication environment, providing interconnection of information systems (*Communication* – “C”). This level is a model of open systems interconnection (*OSI / RM – Open System Interconnection / Reference Model*).

Furthermore, the model is a three-dimensional one, and it has several planes. Three planes were examined in the study: front basic <IS>, management <M> and data protection <P>, which may reflect, each in its own context, the functionality of the basic plane. Unfortunately, the protection plane in the standard [2] practically is not described; therefore, further presentation of data protection plane is possible in two aspects:

1. "Cells" of the plane <DP> integrate sets of mechanisms insuring protection of implementations of the relevant "cells" of the basic plane <IS> – intercategory aspect (in terms of the standard [2]);
2. Since ISP itself is an information system, its functionality, in turn, can also be structured in accordance with the basic representation of <IS> with correction of the context.

The results presented in this paper are focused on the intercategory aspect. Then the task of providing security for PO presented in the form of the OS/RM model is that the properties of *K, C, D* should be realized for implementations of each model "cell" of information and computing resources. In addition, it also relates to the basic plane of <IS> structuring function of IS and management plane <M>, and the resources of the system security, arranged on a plane protection <P>. Obviously, the objectives *K, C, D* are reference ones, first, because they are applied to the reference functional groups, and secondly, models of their interpretation differ for implementations of various "cells" of the model. Figure 3 shows an example of the interpretation of these properties for the "cells" of "Display forms of applications" and "Process of systems application layer".

Display forms
K : access restriction to the display forms of applications:
- limited physical access of any user computer screen, which displays the form;
- limited access to an application in terms of its display forms

D : the possibility to display the forms on the screen:
- physically possible,
- the possibility opposing spam and viruses,
- non-blocking of form.

C : the ability to save display forms in thevariant, in which they were created

The processes of systems application layer
K : limiting access from the side of relevant API functions of an application to the processes of system-application layer;
D : system processes or API business logic possbility to apply to systems application
C : control of processes' integrity

Fig. 3. An example of an interpretation of security objectives for the various "cells" of the OSE \ RM model

Structuring of protection mechanisms

The next task consisted in the fact that protective mechanisms *Mx* (both, currently existing and potentially possible) should be structured in accordance with the objectives of «cells» in view of the interpretation. This will ensure the requirement for intercategory representation of the plane <P>, declared by the standard [2]. *Mx* analysis led to the conclusion that all the variety of mechanisms can be divided into three groups:

Group 1 – Target protective mechanisms providing a target function $\{\overline{KS}\} = \{C, D, K\}$. These *Mx* should be assigned in correspondence with implementation of "cells" of the three planes; i.e. ideally, each "cell" should be "closed" by mechanisms of access control, integrity monitoring, and accessibility insurance.

Group 2 – Protective mechanisms providing those mechanisms, which carry out additional actions necessary for

a) functioning organization of the target *Mx* and

b) implementation of its own target function on either level of protection mechanism. For example, to ensure the confidentiality of a data file, for which there are certain access rights, the security system should make sure that the subject, for example, a user accessing the system, has a corresponding right. To do this, it is necessary to primarily enable the mechanism to organize a session with IS to give the user a possibility to access to the system. Next the mechanisms of identification, user authentication, and after that a mechanism to control access to the file should be enabled, which will compare the rights of the subject and file. Moreover, in order to ensure a certain level of confidentiality, it is necessary to use encryption mechanism for crypto-operation support of appropriate resistance.

Thus, each *Mx* from the group one requires support for insuring protective mechanisms. Tables 1 and 2 demonstrate an example of the relationship of *Mx*'s target and supporting actions in view of a) and b) (see above). Similar tables can be generated and agreed by experts beforehand.

Table 1. Compliance of target and supporting Mx as for data confidentiality / integrity

Insuring *Mx* **Criterion**	Session organization	Ident., authent	Trusted channel	Crypto -support	Data privacy	Domain split	Residual data cleaning
<IS> data confidentiality / integrity	+\ [+]	+\[+]	+\+	+\+	+		+
<P> data confidentiality / integrity	+\ [+]	+\[+]	+\+	+\+	+	+	+
<M> data confidentiality / integrity	+\ [+]	+\[+]	+\+	+\+	+		+

Table 2. Compliance of target and supporting Mx as for data accessibility

Insuring Mx **Criterion**	Fault tolerance	Serviceability	Data recovery	Data rollback	Backup
<IS>data accessibility	+	+	+	+	+
<P> accessibility	+	+	+	+	+
<M>data accessibility	+	+	+	+	+

It should be noted that each *Mx* (protection mechanism) out of the reference group is a hierarchy of mechanisms-subclasses, possessing many attributes and their actions are directed onto different IS objects. For further structuring, it is necessary to present the internal structure of *Mx* in the form of a model. For this purpose, we used a model in the form of a semantic ontology. Fig. 3 shows the ontology of the overall presentation of the class of protection mechanisms {Mx} and an example of one of the special purpose mechanism – access control.

Next, the idea consists in the fact that to relate leaves of taxonomies of target *Mx* with PO "cells", and leaves insuring *Mx* to collate with target ones in accordance with Tables 1, 2. The implementation of control mechanisms is carried out in the form of application to the protection system. Thus, the reference model of IPS is built for IS. It should be noted that this is the general universal model. However, it gives

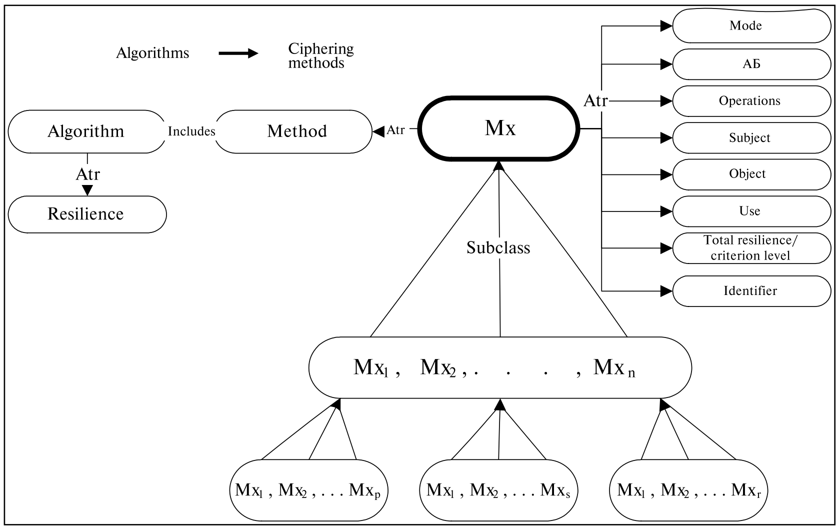


Fig. 3a. Ontology of the “Protection mechanisms” class {Mx}

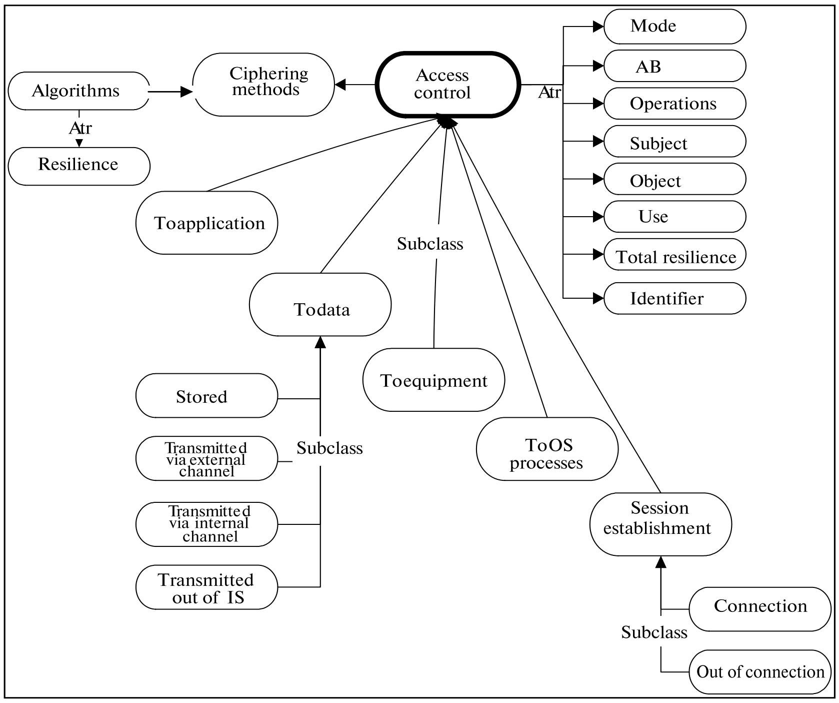


Fig. 3-b. Ontology of the access control mechanism

understanding of how to build business processes for IS protection based on specific needs dictated by IS implementation and organizations’ security policy.

The reference description of the basic subset of business processes protection

In any information system, data is subjected to some typical operations: input / output, storage, processing, transmission to removable data carrier, transmission over a local or wide area network. The national standard for information security [5] is aimed primarily to protect these operations. At the same time, you should consider both user data arrays associated with the basic plane <IS> and the data of system’s management (plane <M>) and security (plane <P>).

All these types of operations are implemented by means of various "cells" of the model and can be represented as a sequence of transitions on the "cells."

1. *Data storage* involves the data organization (high-level or low-level), representation in the form of a format, storage on disk drive and is intended for:

a. User arrays. Their storage is done by means of the column "cells" <IS> <HW> <I>.

b. System data. Its storage is done by means of the column "cells" <M> <HW> <I>.

c. Data of system security. Its storage is done by means of the column <P> <HW> <I>.

It should be noted that all three types of data might actually be stored on the same disk.

2. *Data processing* operation is performed by processes initiated by an application, for example:

a. Computing includes operations carried out on the contents of RAM cells. First, the application algorithm initiated the "cell" <IS> <Appl> <S>, then the process <IS> <OW> <S> addresses to the content of RAM <IS> <HW> <I>, the processor executes the arithmetic on the data (<IS> <HW> <S>) and the result is returned to RAM <IS> <HW> <I>.

b. Modification includes operations carried out on the existing record fields of files, DB.

3. *Data input / output* consists in copying data from an input stream or a file in the RAM cell and data record field from the cells and fields in the output stream or file, implemented by an application.

4. *Data transfer (application, management, security), implemented via removable carriers (cell U, I, HW rows)*. This operation can be carried out by the a user initiative directly, and in this case it is executed by means of OS, such as copying data to a floppy disk or a file output to the printer. This initiation begins in the "cell" <IP> <OW> <U>, then the process in the "cell" <IS> <OW> <S> is triggered which addresses to the file system <IS> <OW> <I>. Next, data reading from the hard drive <IS> <HW> <I> takes place and its recording to a floppy disk or transfer to a printer <IS> <HW> <U> along the dotted arrow.

If the user performs the same operations using an application, the process begins via the form of the application ("cell" <IS> <Appl> <U>), which triggers the algorithm branch <IS> <Appl> <S> and further along the arrows.

Data input chain operates similarly. And data may be both user and service data, In this case they are simply taken from the respective "cells" of planes <M> and <P>.

5. *Data transfer (application, management, security) implemented via a local or external network (column C).* It is executed by setting the interaction between network nodes.

The operation consists of several stages:

- Preparation – establishment of session (connection) is carried out at user request, but can be implemented using OS ("cell" <IS> <OW> <U>) or through the application (<IS> <Appl> <U>).
- Setting up a remote connection to the external IS or LAN is initiated by means of the «cell" <IS> <MW> <S>.
- Data migration from DB for its transmission.

The developed mechanisms *Mx* are intended just for the described above current operations, although it is clear that the availability of appropriate tools for mechanisms implementation, the reference representation of plane functionality <P> allows choosing *Mx* for any operation carried out in the system. Of course, not only these operations occur in the system, but also the charm of novelty is that the reference representation of the plane functionality <S> allows you choosing the *Mx* for any operation carried out in the system.

Therefore, it is the "cells" that are involved in the operation should be "covered" by protection mechanisms, and the sequence of "cells", which are associated with chains of target and insuring mechanisms representing a business process of protection. The following figures 4-6 show a basic subset business processes of protection built on the basis of typical data operations described above.

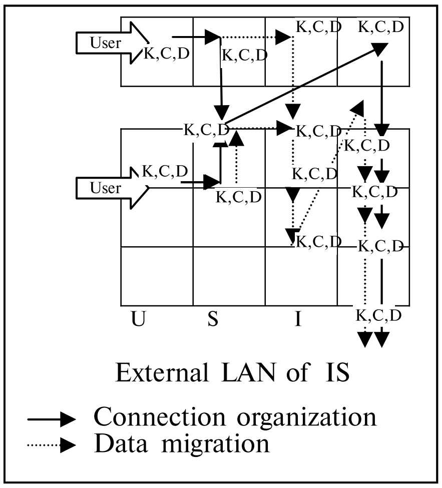
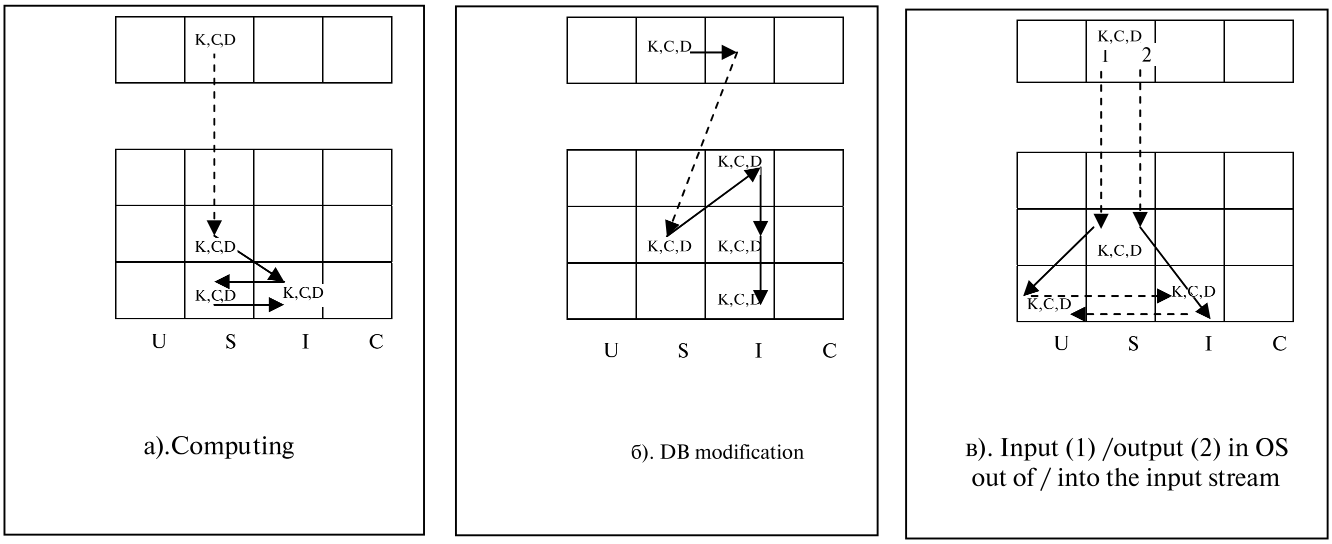


Fig. 4. Data transmission via local or global network



a).Computing

б). DB modification

в). Input (1) /output (2) in OS out of / into the input stream

Fig . 5. Representation of operations of data processing via computing (a), DB modification (b) and input / output from the input stream (c)

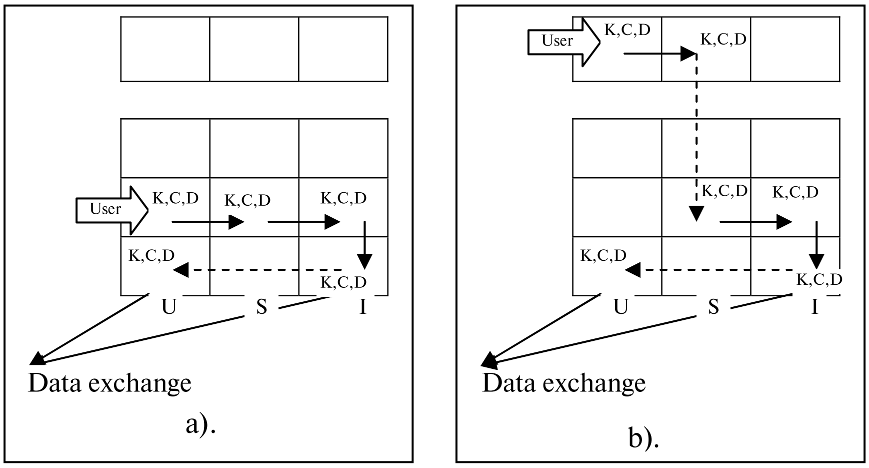


Fig. 6. Data transfer to portable data medium initiated by user with the help of OS tools (a) or an application form (b)

Conclusion

In conclusion, we shall emphasize, what the presentation of information system in the form of the OSE/RM model gives for the design of protection system:

1. *A systematic* comprehensive look at IS as an object of protection.

2. The three-dimensionality of a model allows representing all faces of IS that is the base, management and protective ones in the form of an integrated system.

3. *Systematic representation of IS functionality* of any complexity, from a single computer to a geographically distributed systems, including the protective plane *allows standardizing security system*, i.e. to collate multiple standards or specifications regulating the design of a protection system and its operation to “cells” plane of protection.

4. The specified functionality of a protective component implementation in the form of intercategory services (mechanisms), structured according to OSE/RM, gives the opportunity for security system *to obtain the properties of openness* [3,4], namely, extendability, scalability, mobility of applications, user mobility, interoperability.

5. Decomposition of security objectives $\overline{KS}(C,D,K)$ by the model “cells” makes it possible to design reference business processes of protection, which allow obtaining reasonable requirements for applications within the IPS regarding implementations of the “cells” of IS objects.

References

1. **Kalyanov G.N.** Modeling, analysis, reconstruction and automation of business processes. Moscow: Finance and Statistics, 2006, p. 240.

2. ISO / IEC TR 14252-1996 Guide to the POSIX Open System Environment.

3. ISO/IEC 10000-1-2-3-99. Information technology. Fundamentals and taxonomy of international functional standards.

4. **Boitchenko A.V., Kondratyev V.K., Filinov E.N.** Fundamentals of open information systems. 2nd ed. – Moscow: Moscow State University of Economics, Statistics and Informatics, 2004

5. GOST R ISO / IEC 15408-2009. Information technology. Methods and tools to ensure security. Assessment criteria for Information Technology Security.