National Research Nuclear University

MEPhI

Department of Information security of banking systems (№44)

Development of the regulatory framework and documentation for the continuous operation of the secure information portal "Information Security Management

Executor:

Student gr. M16-508 Sidorenko Aleksander

Scientific adviser: Miloslavskaya Natalya Georgievna

Ph.D., associate professor

Comprehensive project

This research work (RW-1) is part of the final qualification work (WRC) "Development of the regulatory framework and documentation for the continuous operation of the secure information portal" Information Security Management "

which is included in the complex project: "Ensuring information security and continuity of functioning of the secure information portal" Information Security Management "

Goal and tasks

Goal:

Formation of the regulatory framework for information security and the continuous operation of a secure information portal

Tasks:

- Drawing up the list of normative documents
- Development of a threat model for the IS of a secure portal
- Development of the model of the infringer of the IS of the protected portal
- Formation of documentation for the continuous functioning of the portal
- Writing an explanatory note

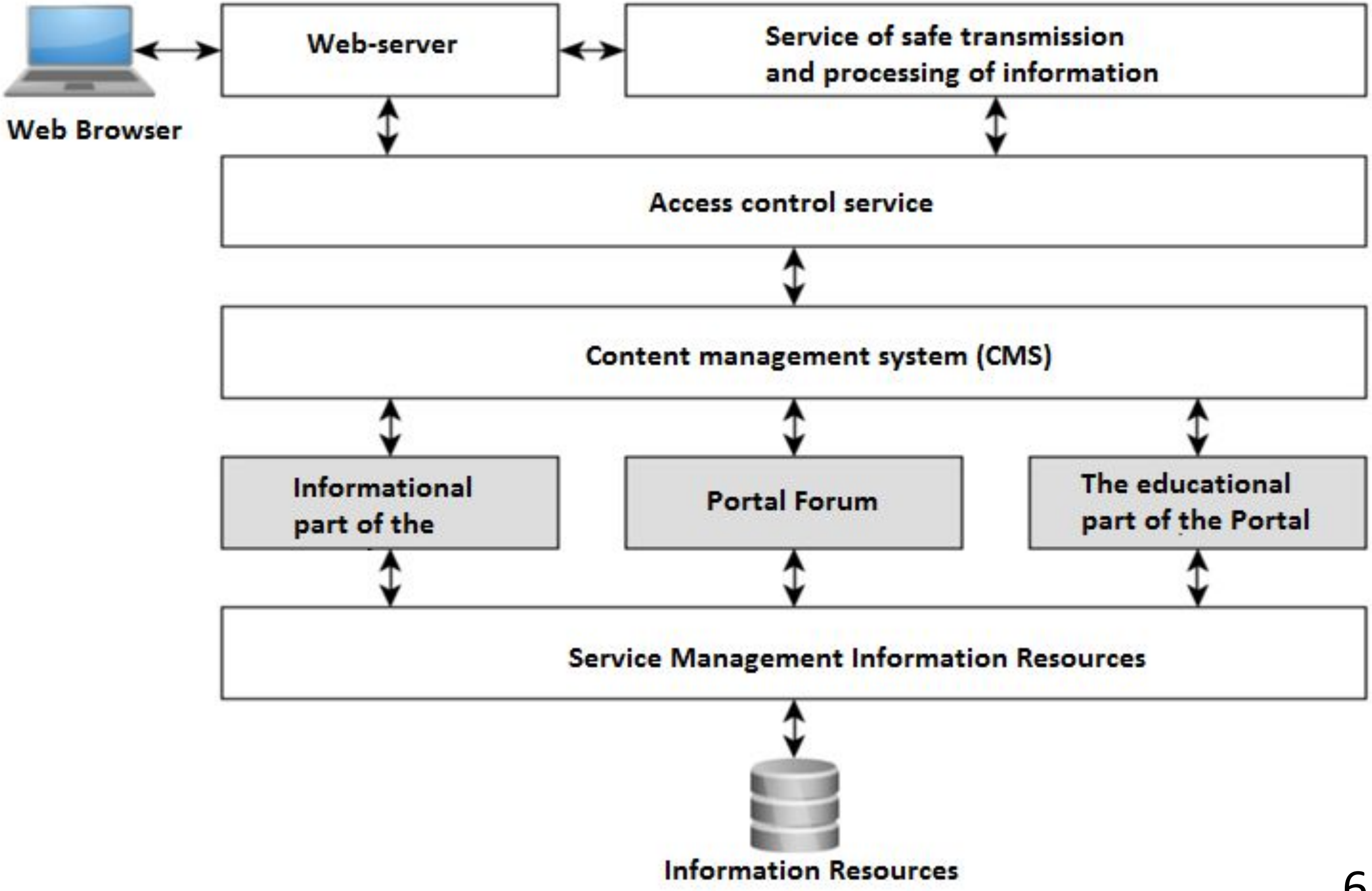
The object of protection

The main object of protection is the secure portal "Information Security Management"

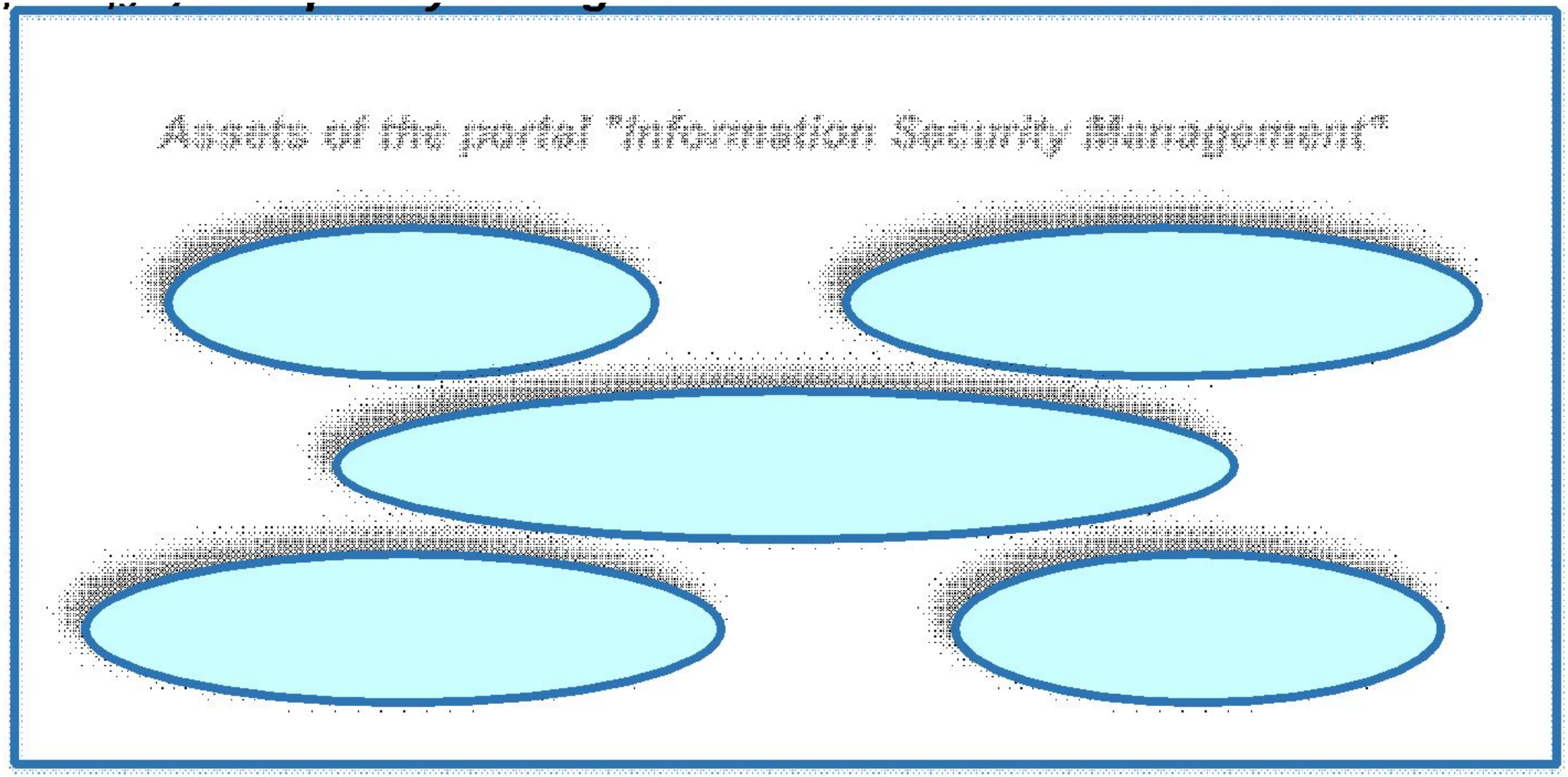
Definition of the Portal:

A complex of hardware and software, represented by a single input in the form of a Web site, and organized to combine various network resources and systems that provide personalized service to the target audience and its collective work

Scheme of interaction between portal services


Web Browser
Web-server
Service of safe transmission and processing of information
Access control service
Content management system (CMS)
Informational part of the
Portal Forum
The educational part of the Portal
Service Management Information Resources
Information Resources

Assets of the portal



IS Portal Threat Model

Name of the IS threat	Source of IS threat	Vulnerabilities Used	Affected objects	Methods for implementing threats	Violated IS properties	Scope of potential damage
Imposing a false network route	Anthropogenic external (intentional)	- Disadvantages of routing protocols (RIP, OSPF, LSP); - Incorrect network management parameters (ICMP, SNMP);	Web server host;	Making unauthorized changes to routing-address tables;	Confidentiality;	-Restricted-address data was changed unauthorized; - The transmitted data is modified; -The false information is tied up;
Threat of revealing the password	Anthropogenic external (intentional)	-Use of unstable passwords; -The presence of malicious software to intercept passwords;	-Host web server; - Client;	-Simple search of all possible values of the password; -Selection using special software (dictionary attack); -Capture password using the network traffic analyzer;	Confidentiality;	-Used to the resources of the Portal;

Model IS Portal Violator

Name of the infringer IB	An experience	Knowledge	Available resources needed to implement the threat;	Motivation	Ways to implement threats
Content Moderator	Medium (use of portal resources in user mode);	- Information about the portal configurations without the right to change them and the administrative settings; - Has information about the vulnerabilities of individual components of IP; - Has information about methods and means of implementing computer attacks published in public sources;	- Legal account of the content moderator; - Access to the Internet;	- Causing property damage by fraud or other criminal means; -Realization of threats IB from revenge; - Implementing threats to the IS unintentionally due to negligence or unskilled actions;	- IMD and (or) impact on objects at the application level (DBMS, browsers, web-applications, etc.); - IMD and (or) impact on objects at the network level (network equipment, network applications, services); - Impacts on users, management group (social engineering).

List of documentation for the continued functioning of the portal

- Model of IS threats;
- Model infringer IB;
- IS policy;
- Model of IS risk assessment;
- Plan for handling IS incidents.

Results of work

- List of documentation support for IS portal
- The IS threat model for the portal
- Model infringer IB for the portal
- Documentation for the continuous functioning of the portal
- Explanatory note

Thank you for attention!