1. Describe the principles of legal support of information security on the base international standards (the main of them are ISO 15408, ISO 17799).

2. Use peer-to-peer method to organize the study of principles of information security threats classification and modeling. This method could be used both on the lecture and seminar, because as a rule the group of international students is no more then 15 persons.

3. Explain organizational methods for information security ensuring by the discussing with students the content of the standard ISO 27001, standards about the information security audit realization (COBIT, SAC, COSO), features of social engineering methods.

4. Use theoretical modeling method to organize discussion of technical methods to ensure information security. These discussion should be build on the knowledge about information security threats classification and modeling.

5. Explain technical methods for information security ensuring

6. Use the problem based learning method and brainstorm method to organize the final seminar of the subject. The theme of this seminar is «Information security vulnerabilities». The main task of this seminar could be connected with development the measures for protection defined information network of organization from impact of different attacks. These measures have to correspond the studied standards.

CLOUD SECURITY FOR FINANCIAL ORGANIZATIONS

S.N. Petrov, Anas Moftah Elbuaishi

Financial institutions are particularly exposed to cyber risk due to their reliance on critical infrastructures and their dependence on highly interconnected networks. By 2016, more than 60 % of transactions in the banking sector worldwide carried out on the basis of cloud technologies, according to Gartner . Banks are among the most advanced IT users, so they are still at the forefront in terms of developing private clouds. Cloud infrastructure technologies provide a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources. The cloud requires few provisions while delivering rapid results.

Among the systems that banks are ready to place in private clouds: information systems such as CORE, ERP, CRM, that is critical for the existence of the entire banking business it solutions, while the least critical, for example, e-mail servers, can be placed in the public cloud.

Therefore, despite the fact that the banking sector is dominated by private clouds, cloud service providers are working to create highly secure public cloud solutions, «sharpened» for banking requirements and problems. In particular, new advances in encryption technology allow an organization to retain control over data even when it is on a remote server. In this case, even if the information is leaked, the key to decryption will remain in the hands of the company.

However the usage of a physically shared infrastructure also introduces new potential vulnerabilities unless the system is tightly monitored and controlled. An effective cloud security and privacy solution requires both the inclusion of key security features in the technology as well as a properly designed governance organization and processes.

Successful attacks on a financial institution could result in significant disruptions, although to date attacks have not caused large damages, based on publicly available information. A common method to disrupt firm business operations is to launch a DDoS attack on the targeted firms' servers. Cyber-attacks can also be used to undermine customers' confidence in an institution. For example, on June 27, 2014, Bulgaria's largest domestic bank FIB experienced a depositor run, amid heightened uncertainty due to the resolution of another bank – following phishing emails indicating that FIB was experiencing a liquidity shortage. Deposits outflows on that day amounted to 10 percent of the banks' total deposits and the bank had to use a liquidity assistance scheme provided by the authorities.

Banks should perform an internal/external risk assessment including PenetrationTesting, Vulnerability Scanning, Social Engineering and business process analysis related to data security. They should also develop a cloud computing roadmap based on business risk exposure (low-high), Cost of Ownership and opportunity of Return on Investment towards moving to the cloud.