– a key/value storage, rather than a relational model provides flexibility for application developers;

– business profits, presented as faster decision making, improved consumer service and higher productivity.

One of the main differentiating properties between NoSQL databases and IMDGs is data consistency. In addition, other feature in IMDGs which really distinguishes them from NoSql databases or IMDBs is actually scalable data partitioning across the cluster. It is significant that in the poorest approach most IMDGs may be considered as distributed hash maps.

Transactional ACID support (Availability, Consistency, Durability and Integrity) is another essential characteristic of IMDGs. Ensuring the data consistency within the cluster is provided by using 2-phase commit protocol (2PC). Different systems will have different locking mechanisms, but commonly more modern implementations will allow concurrent locking mechanisms guaranteeing ACID consistency with very high performance. Data consistency differs IMDGs from NoSQL databases. Moreover, NoSQL databases are mainly created by means of Eventual Consistency (EC) approach.

The typical use case of IMDG is data partitioning across the cluster, when data is send to collocated computational nodes. The combination between Compute Grids and IMDGs is significantly important since computations must be properly deployed, failed-over, or scheduled in parallel or even in distributed way.

All in all, therefore, IMDGs with Computer Grids can be used in a wide range of industries where low latency and high processing speed is a first-class need including gaming services, trading systems, e-commerce, fund risk analytics, reservation systems and cloud applications.

Scientific supervisor: Hurska O.O.,
Senior Lecturer

UDC 004.056.5:65.012.23 (043.2)

Zubilevych A.V.
National Aviation University, Kyiv

CYBER SECURITY IN BUSINESS

Nowadays all spheres of human society depend on new informational technologies. And business is also closely connected with informational technologies. So, human society is confronted with new great challenges due to the developing of high technologies. People suffer from cyberterrorism, hacking, problems of privacy. Cybercrime or computer crime can be divided into two categories: the first comprises crimes that target computers directly such as viruses, attacks and malware; the second focuses on online crime that uses computer networks or devices as means to perform fraud and identity theft through social engineering as well as cyber bullying, cyber stalking and cyber warfare.

It should be mentioned that Informational safety in business is an important part of successful running of business. As The Security Service Of Ukraine confirms the cybercrimes happen much more often than any other crimes today. And these crimes are rapidly increasing every year.

IBM Corp.'s Chairman and CEO President Ginni Rometty said that cybercrime may be the greatest threat to every company in the world. It is said that the cybercrime from 2013 to 2015 years costs $500 billion, and it is supposed to be quadrupled until 2019. So, Cyber Crime will overtake $2 Trillion by 2019.

It is the common knowledge that the informational component of security is the implementation of effective informational and analytical support of business enterprises. Security service performs certain functions that include the process of creating and protecting information component of economic security. The main function of this service is the collecting of all kinds of information activities of the company, the analysis of the information, obtained from mandatory compliance. It is based on generally accepted principles and methods, in scientific, technological, economic and political processes of certain state and in the whole world as well. Informational security service also ensures the three main qualities of information: confidentiality integrity availability.

According to the last researches in sphere of informational security service, the 90 percents of personal and corporate information is in free access in the company`s website, different professional blogs, personal and corporate accounts. Different personal and corporate information is also available in social networks such as Facebook, Twitter, Instargam. Taking into consideration all these facts, we must say that the department of informational safety service should control the content of websites ,blogs, accounts in social networks.

Speaking about informational security we can`t but mention about the safety of your office. There are many targets for crackers in the office. Everybody must take care about office network (Ethernet and Wifi), computers, personal devises of clerks (smartphones, tablets, laptops). Someone must safe the Internet connection by using a firewall and encrypting traffic. Also someone find the most modern protection from virus, malware, spyware and other dangerous code. All software vendors must regularly provide patches and updates for their products to correct security problems and they also must improve their functionality.

It is necessary to educate and train the clerks. They must be involved into the cybersecurity activity. Different trainings and courses must be organized to avoid informational illiteracy.

So, as we live in rapid and changing world, we should react on different problems which are connected with informational technologies and Cybercrime.

Scientific supervisor: Verbylo H P.,
Senior Lecturer