

Methods to improve the effectiveness of the information security management system

Financial university under the Government of the Russian Federation

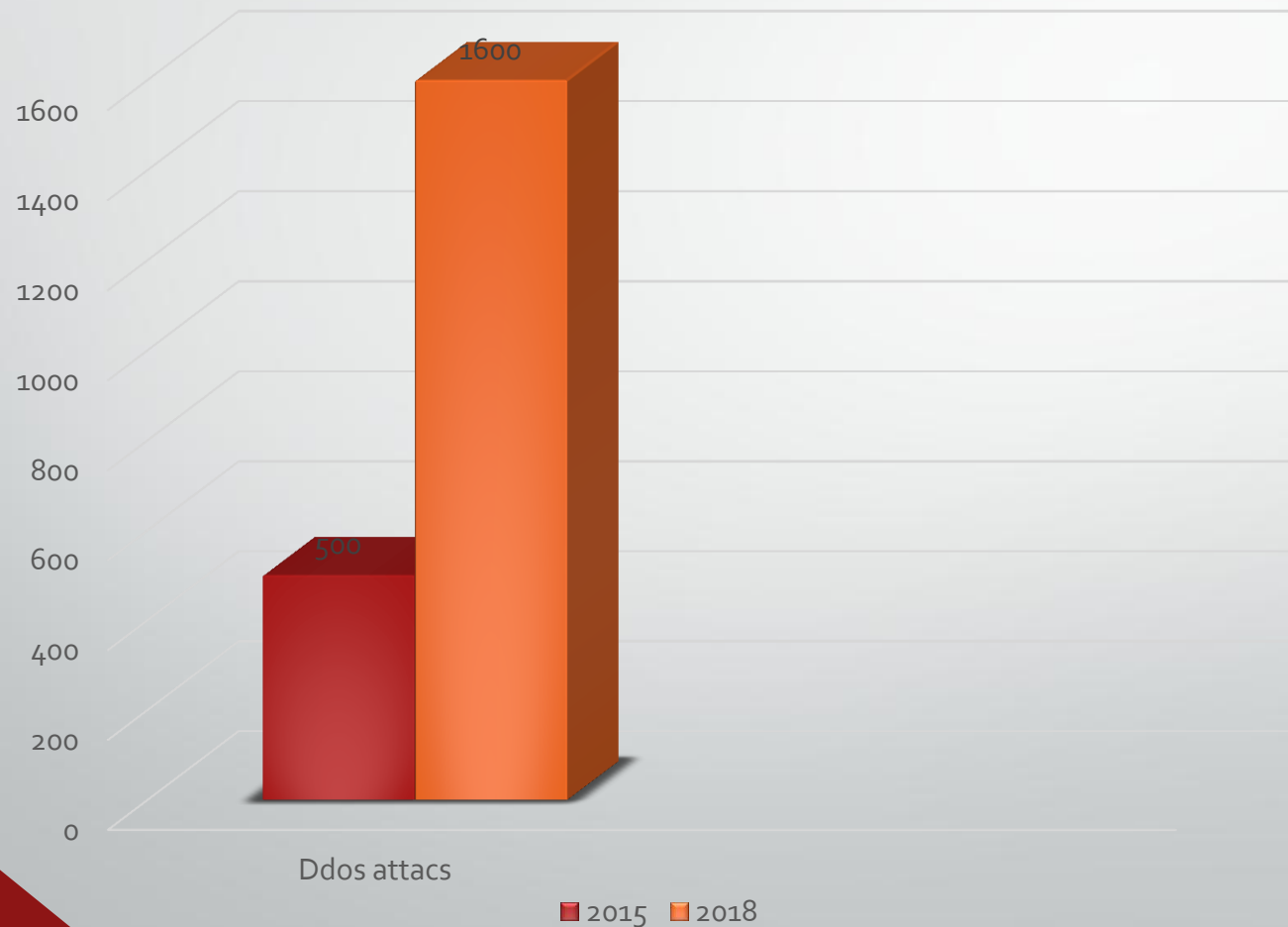
Jibek Sharsheeva

jsharsheeva.rc@gmail.com

RIPE NCC Regional meeting Almaty

25 September 2018

The power of DDoS attacks ↑



In 2015, a record attack was a 500 Gbps attack, and in 2018 the power of attacks exceeded 1.6 Tbit / s already.

- In the first half of 2018, an average of 20 attacks per day on the infrastructure of the telecoms operator and its customers were conducted on average each day.
- The average duration of one attack is 21 minutes, the longest attack for the first half of 2018 is 1200 minutes (20 hours), the shortest is 2 minutes
- The average attack power is 3.14 Gb / s. The maximum attack power is 393.6 Gbit / s

20 attacks daily

$T \sim 21$ minutes

3,14
Gbps

Max
1200 minutes

Min
2 minutes

Max
393,6 Гбит/с

Cost

• \$1 trillion

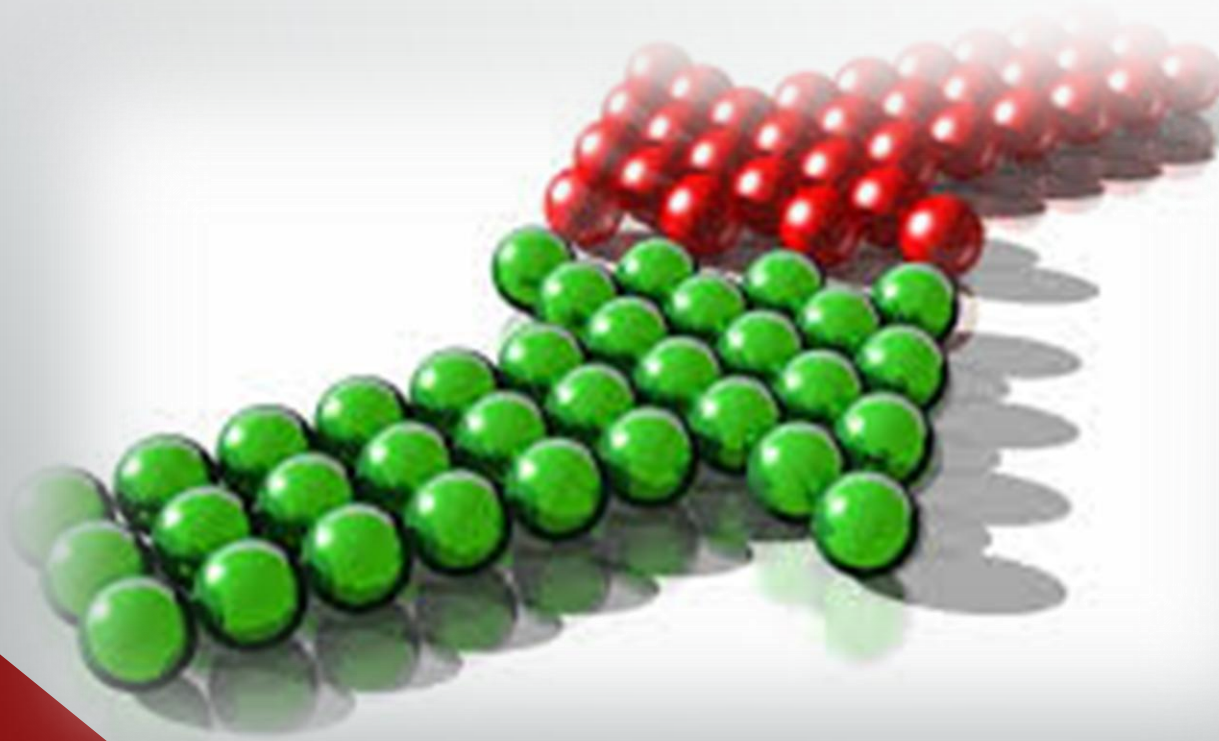
Damage

• 2021 > \$6 trillion

- Over the next couple of years the global cost of cyber security will be about \$ 1 trillion.
- By 2021 the cost of recovering global damage due to extortion attacks might exceed \$ 6 trillion.

*CyberSecurityVentures

The increase in the number and scale of attacks.

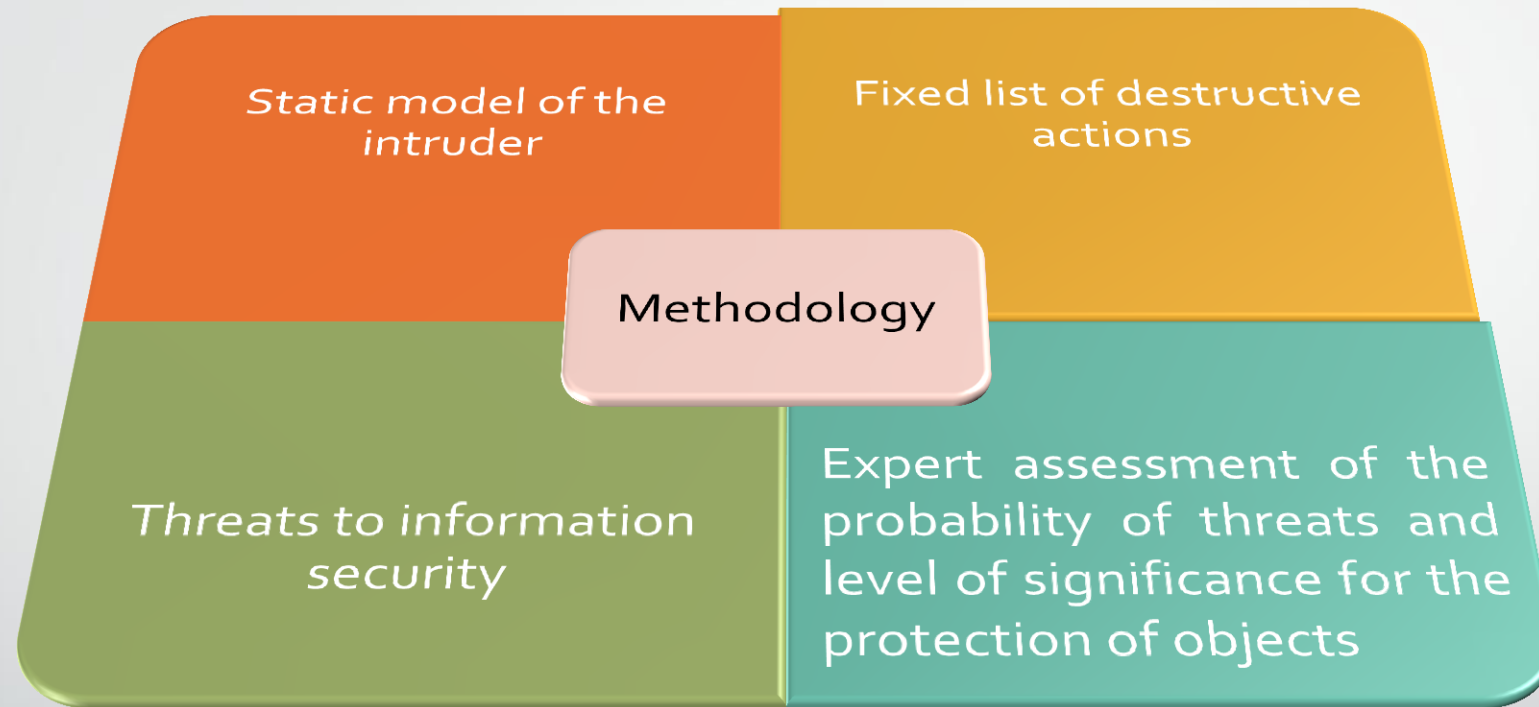


All used methods of information security conflict between the state of the theory ensuring information security and modern standards of practice to ensure information security.

- A significant number of developed standards leads to a variety of versions and options for their application to ensure security.
- *National standards of GOST R do not have time to be updated synchronously with the revision of international standards (for example, ISO / IEC 27001: 2013 and GOST R ISO / IEC 27001-2006).*



Essential general elements in the current methodologies



- Almost never used the approach of risk management based on modern risk-based standards, including residual risks accounting procedures⁷

Disadvantages

Practical lack of a reliable methodical apparatus

- to obtain numerical information security level assessment

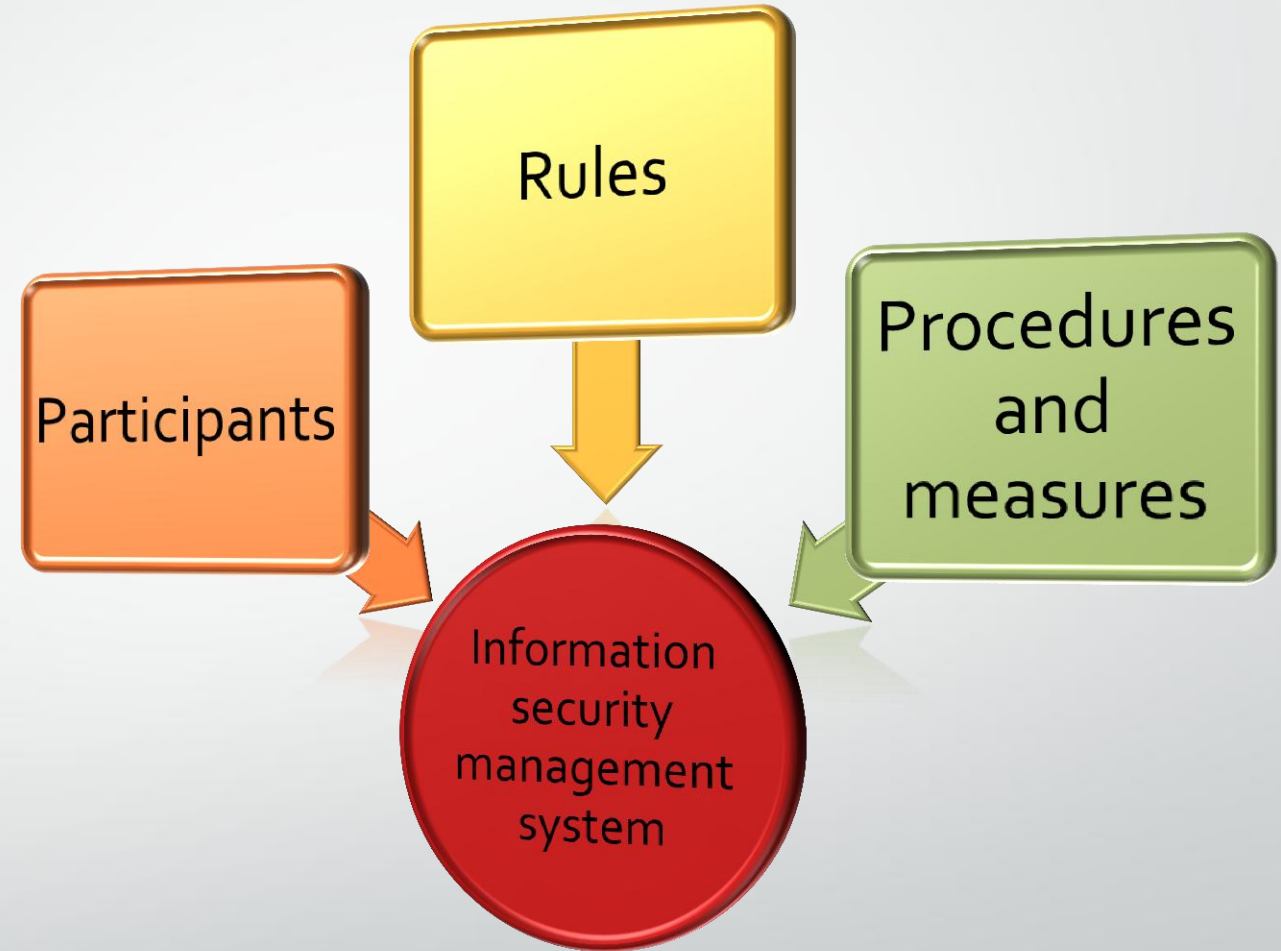
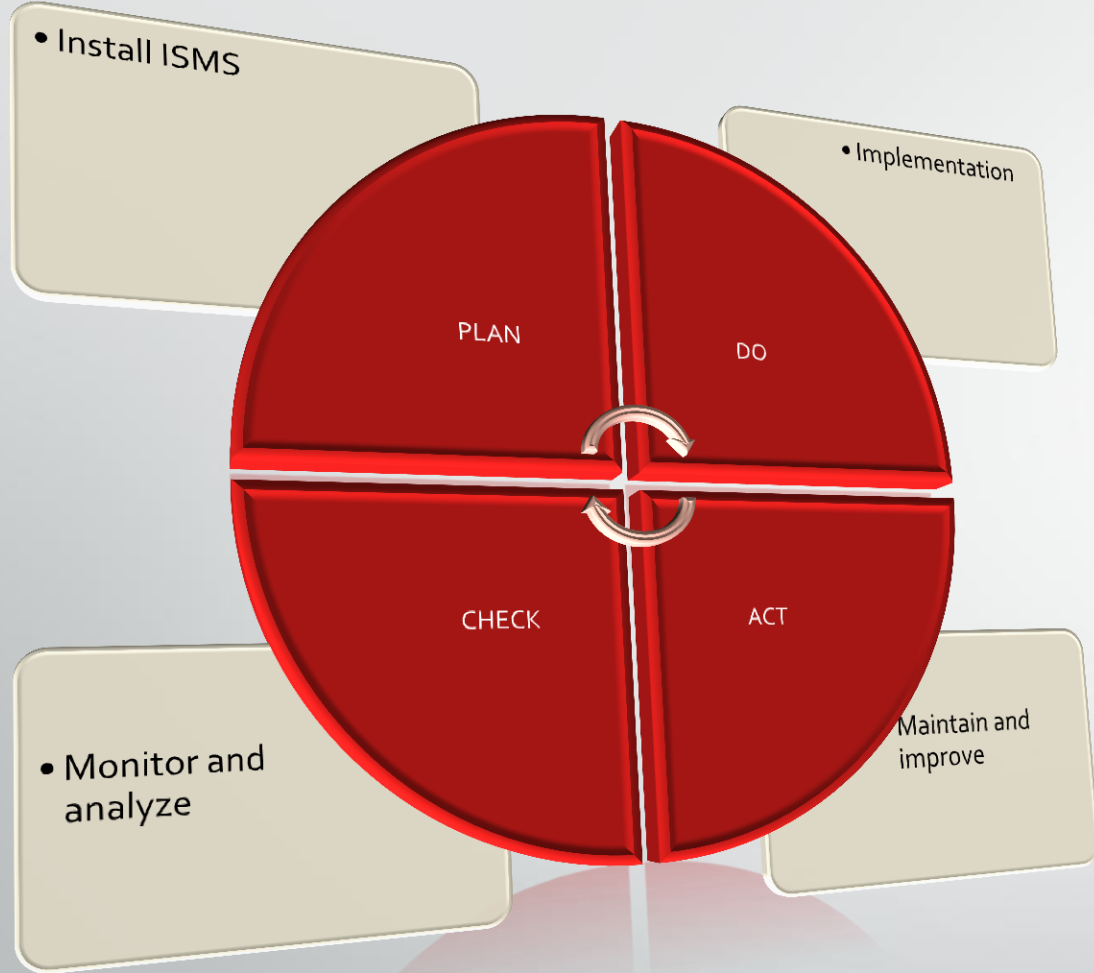
Lack of a common universal concept

- related to the phases of the life cycle and risk management, with the general principles of implementing information security mechanisms in management systems (in the PDCA cycle).

Lack of holistic approach

- for complex counteraction to modern threats of information security

- *Despite the more frequent application of risk-oriented foreign standards and methodologies (ISO, IEC, NIST, ISAGO, IEEE, ITIL, COBIT, TOGAF, etc.)*



No providing an economic balance between the value of the protected assets with a high level of information security

The cost of a complex of technical facilities introduced in strict accordance with the function of cost-effectiveness information security management system



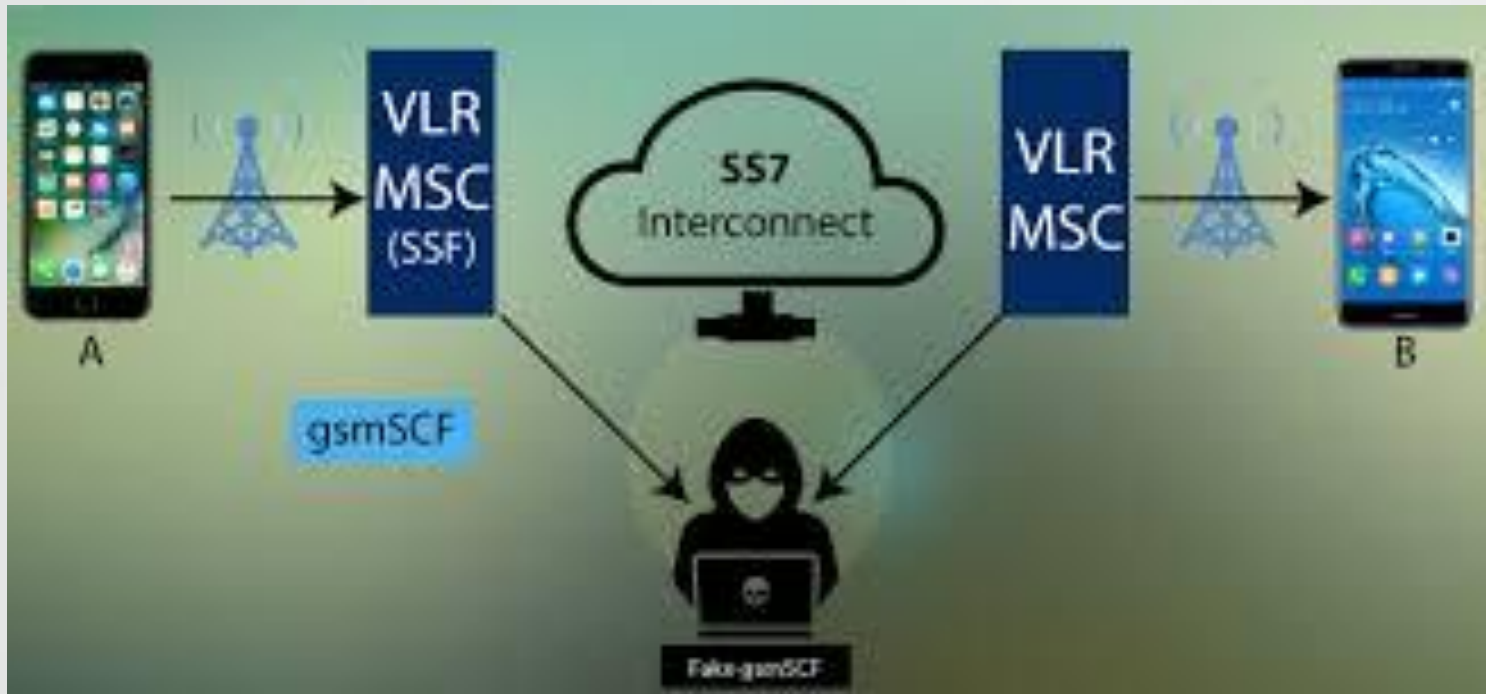
Solutions of leading companies providing secure communication

Company A

- Entered the information security market last year by opening the resources of its own security operation center.


Company B

- Provides for its customers filtering at the backbone network of the operator with the best SLA on the market.



- Operators can not fully provide protection due to the nature of the network architecture
- Despite the emergence of networks of new generations using a different signaling system, as it should support the old standards and the interaction between networks of different generations.

What can be done?



Requires a flexible and simple mathematical apparatus adaptive to dynamically changing requirements in information security management system

Including functions of risk management, joined to the phases of the life cycle and the introduction of appropriate feedback loops would significantly increase the speed of decision-effective management solutions.

Through the use of new models information security management system audit realizing prompt formation quantification level ensuring information security, selection and use of the best set of means to ensure information security risks identified processing efficiency can be improved ensuring information security

Necessary activities

- "It seems promising to implement jointly the functions of risk management, flexible feedback, the "closure" of the PDCA cycle, a simple and effective mathematical apparatus in the "instant audit" model of information security. In the development of this optimization method is the justification of the ability to withstand modern attacks"-Livshis I.

Revision of existing static models of threats to information security and destructive actions

Additional integration of risk management

Accounting requirements for the planning, implementation and improvement of information security audit system

Development of a comprehensive tool for solving the problems of information security of organizations

The method of applying utility functions to work in conditions of uncertainty



20% of all existing security tasks can be solved by technical means

Protection algorithms are in the framework of a large number of random and heavily predictable parameters (the behavior of the attacker, natural disasters, etc.).



80% of all problems are solved through organizational, administrative and procedural means.

Among all areas of protection, the most part is precisely organizational protection, related to human actions.



Thank you!

Jibek Sharsheeva
jsharsheeva.rc@gmail.com