

□ Information security of networks is a "state of security", "Information infrastructure, entities that collect, generate, disseminate and use information, as well as a system for regulating relations arising from the use of communication networks."

□

Due to their openness and accessibility, computer networks and public communication networks are a convenient means for ensuring interaction between citizens, business and public authorities. However, the more open networks, the more they are vulnerable. We can distinguish a number of features that make the network vulnerable, and violators - virtually elusive.


□ the possibility of violators at a distance in combination with the possibility of hiding their true personal data (this feature is typical, in particular, for the Internet, radio networks, cable television networks, illegal use of telephone network resources); ·

□ the ability to propagate and disseminate network security breaches (for example, the distribution in the Internet of software that allows unauthorized access to information resources, violate copyrights, etc.);

- the possibility of repeated repetition of attacking network impacts (for example, the generation in the Internet or telephone networks of call flows leading to disruption of network nodes).

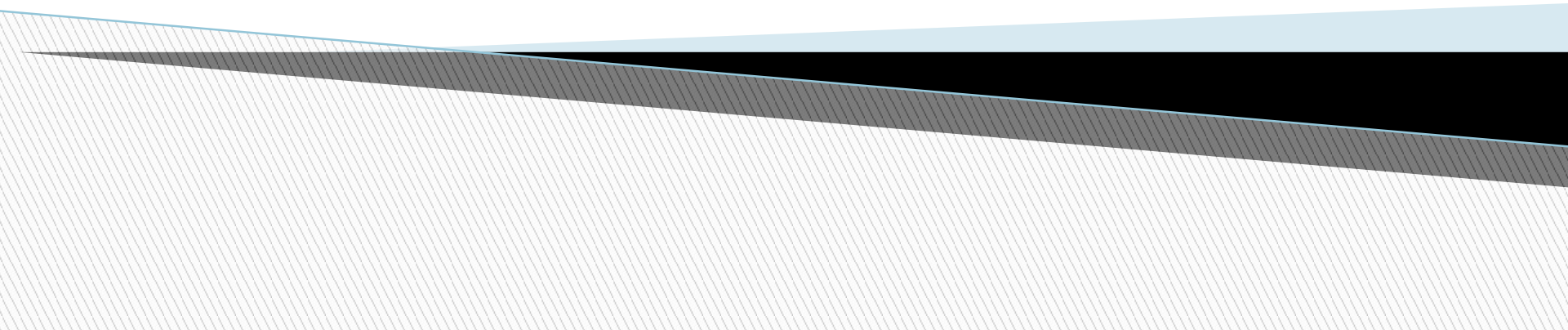
Defining a secure information system

Unlike local corporate networks connected to the Internet, where conventional security solutions to a large extent solve the problems of protecting internal segments of the network from unauthorized access, distributed corporate information systems, e-commerce systems and the provision of services to Internet users have increased requirements in terms of ensuring information security.

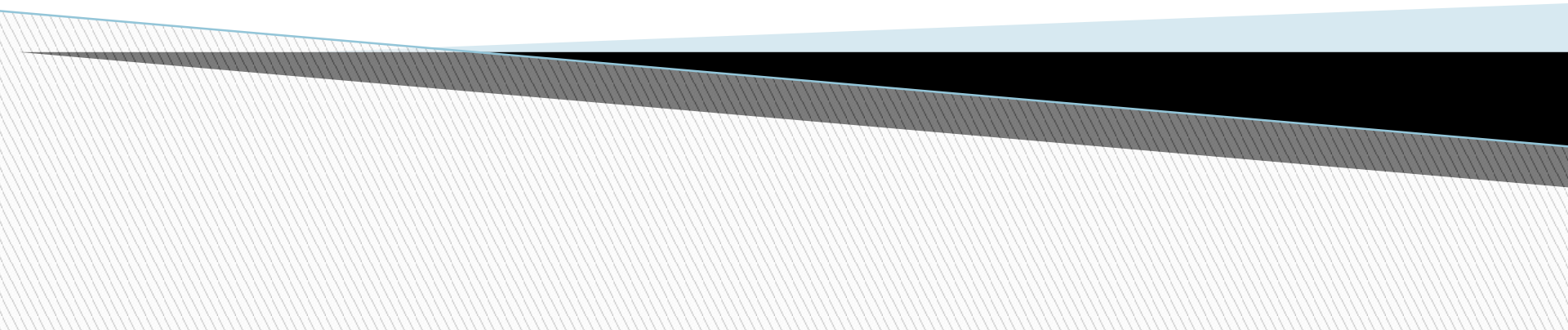


The concept of "Secure Information Systems" includes a number of legislative initiatives, scientific, technical and technological solutions, readiness of state organizations and companies to use them so that people, using devices based on computers and software, feel just as comfortable and safe. In general, we can talk about the degree of confidence, or reliability, of systems evaluated by two main criteria: the existence and completeness of the security policy and the security assurance.

The existence and completeness of the security policy is a set of external and corporate standards, rules and norms of behavior that correspond to the country's legislative acts and determine how the organization collects, processes, disseminates and protects information.



Security assurance is a measure of trust that can be provided to the architecture, infrastructure, hardware and software implementation of the system and methods for managing its configuration and integrity..



Guarantee can result from both testing and verification, and from verification (system or operational) of the overall design and execution of the system as a whole and its components. Guaranteedness shows how well the mechanisms responsible for enforcing the security policy are

