



SFERA

DATA PROTECTION SOFTWARE

SFERA data protection software is designed to prevent unauthorized access to information stored and processed by ATC systems. The software is certified by Federal Service for Technical and Export Control to be in conformance with requirements of “Computing Facilities. Preventing Unauthorized Access to Data. Data Protection Criterion” guidance document. The software provides for class 4 data protection when operating under Windows OS and class 5 data protection when operating under Linux OS.

FUNCTIONALITIES

SFERA data protection software provides:

- Identification, verification, and access control:
 - to the system
 - to terminals, computers, network nodes, communication channels, external computers
 - to volumes, catalogs, files, records, record fields
- Data flow management
- Record-keeping and filing for:
 - logging on/off to/from the system (network node)
 - release of printed/graphic output documents
 - start-up/shutdown of programs and processes (tasks)
 - access of access subjects programs to protected files including their generation
 - deletion and transmission on communication lines and channels
 - access of access subjects programs to terminals, computers, network nodes, communication channels, external computers, programs, volumes, catalogs, files, records, record fields
 - changes of access subjects rights
 - generated protected access objects
- Registration of data media
- Cleaning (zeroing, impersonation) of disposed RAM areas of PCs and external drives
- Attack alarm
- Software and processed data integrity maintaining
- Data protection manager (service) availability
- Periodic testing of data protection facilities
- Availability of data protection facilities recovery tools

STRUCTURE

SFERA information protection software for protected workstations and servers
SFERA information protection software for security manager workstation
Security manager workstation (optional)

Application software includes following subsystems:

- files access control
- LAN integrity control
- files integrity control
- control and settings
- access to confidential information
- data transmission
- printing
- operation with protected information