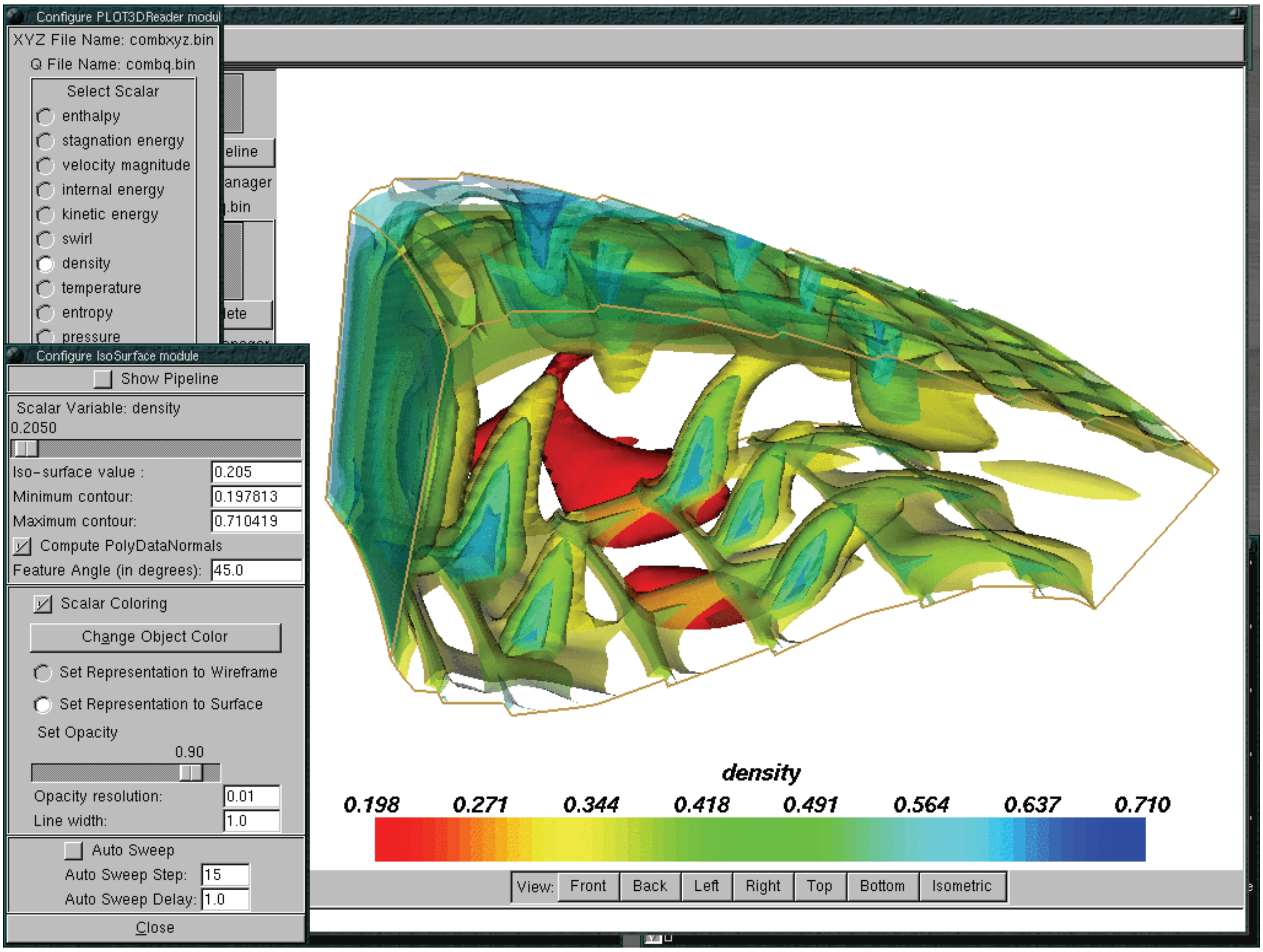
UDC 004.056.53

R.A. Umerov, postgraduate student (National Aviation University, Ukraine),
F. Galindo, Ph.D. (Universidad de Zaragoza, Spain),
A.A. Tikhomirov, Sc.D. (IIA, Russia),
A.I. Trufanov, Ph.D. (Irkutsk State Technical University, Russia),
A. Rossodivita, M.D. (University of Medicine "Life and Health", Italy),
R.N. Memetov (CEPU, Ukraine)

VISUALIZATION'S INSTRUMENTS IN INFORMATION SECURITY TASKS

Mapping and visualization is still not used to meet the challenges of information security - science and practice. In practice, solving problems for constructing complex information security systems are more effective and attractive. Considered prmery solutions using Visualization Toolkit (VTK), Google Public Data Explorer, Logstalgia

One example of solving problems in visualization - MayaVi [1], data visualization tool for Linux to associate with the language Python. For graphics output, it uses a powerful visualization tool Visualization Toolkit (VTK, Fig. 1). The package MayaVi also includes a graphical user interface, developed through a module Tkinter. Tkinter - an interface Tk, most often used in conjunction with Tcl.



Configure PLOT3DReader modul

XYZ File Name: combxyz.bin

Q File Name: combq.bin

Select Scalar

○ enthalpy
○ stagnation energy
○ velocity magnitude
○ internal energy
○ kinetic energy
○ swirl
● density
○ temperature
○ entropy
○ pressure

Configure IsoSurface module

□ Show Pipeline

Scalar Variable: density

0.2050

Iso-surface value : 0.205

Minimum contour: 0.197813

Maximum contour: 0.710419

☑ Compute PolyDataNormals

Feature Angle (in degrees): 45.0

☑ Scalar Coloring

Change Object Color

○ Set Representation to Wireframe

○ Set Representation to Surface

Set Opacity

0.90

Opacity resolution: 0.01

Line width: 1.0

□ Auto Sweep

Auto Sweep Step: 15

Auto Sweep Delay: 1.0

Close

Fig. 1. Visualization Toolkit (VTK).

MayaVi Originally developed as a visualization tool for CFD (Computational Fluid Dynamics, CFD). After it became clear benefits from its use in other areas, it has been redeveloped as a general scientific data visualization tool.

MayaVi package relies on the power of VTK. VTK - a system for data visualization and image processing with open source, which is widely used in the scientific community. VTK offers tremendous opportunities, having, in addition to libraries of C++, interfaces for scripting languages, Tcl / Tk, Java programming language and Python. VTK ported to many operating systems including UNIX, Windows and MAC OS X.

Shell MayaVi to VTK can be imported as a Python module into other Python programs and can be used in scripts that run in the interpreter Python. Graphical user interface tkinter, supplied with MayaVi, allows you to configure and apply filters and manage the lighting effects when rendering.

Search for reliable data and reliable statistical information in various fields is very important. According to Google [2], the most popular requests are: a comparison of educational institutions, unemployment statistics, data on population, size, sales taxes, wages, exchange rates, crime statistics, statistics of oil prices, etc.

Such statistics certainly useful, but only if they are easy to find and easy to work with them. Google has released a new experimental product, Google Public Data Explorer, which allows you to visualize the found statistical information, thereby simplifying the task of understanding the data. Data Explorer can build dynamic charts (with elements of histograms, graphs, bubbles), to track changes over time, zoom, select individual data, etc. Of course, the possibility of sharing such diagrams and instruments posting them on blogs or on Web sites.

In the animated charts are based on technology Trendalyzer (acquired from Gapminder Foundation), which were previously implemented in the Visualization API and the functions of Motion Chart in Google Spreadsheets.

In practice, the visualization allows us to trace changes in the state services or ongoing attack, writing in different colors and geometric shapes and dynamics of state services attacks (processes). Abstract black box «organizer's box» [3], multiple servers, as described in RuCTFE 2010, OpenVPN, PostgreSQL, Failover, Checksystem and Backup server.

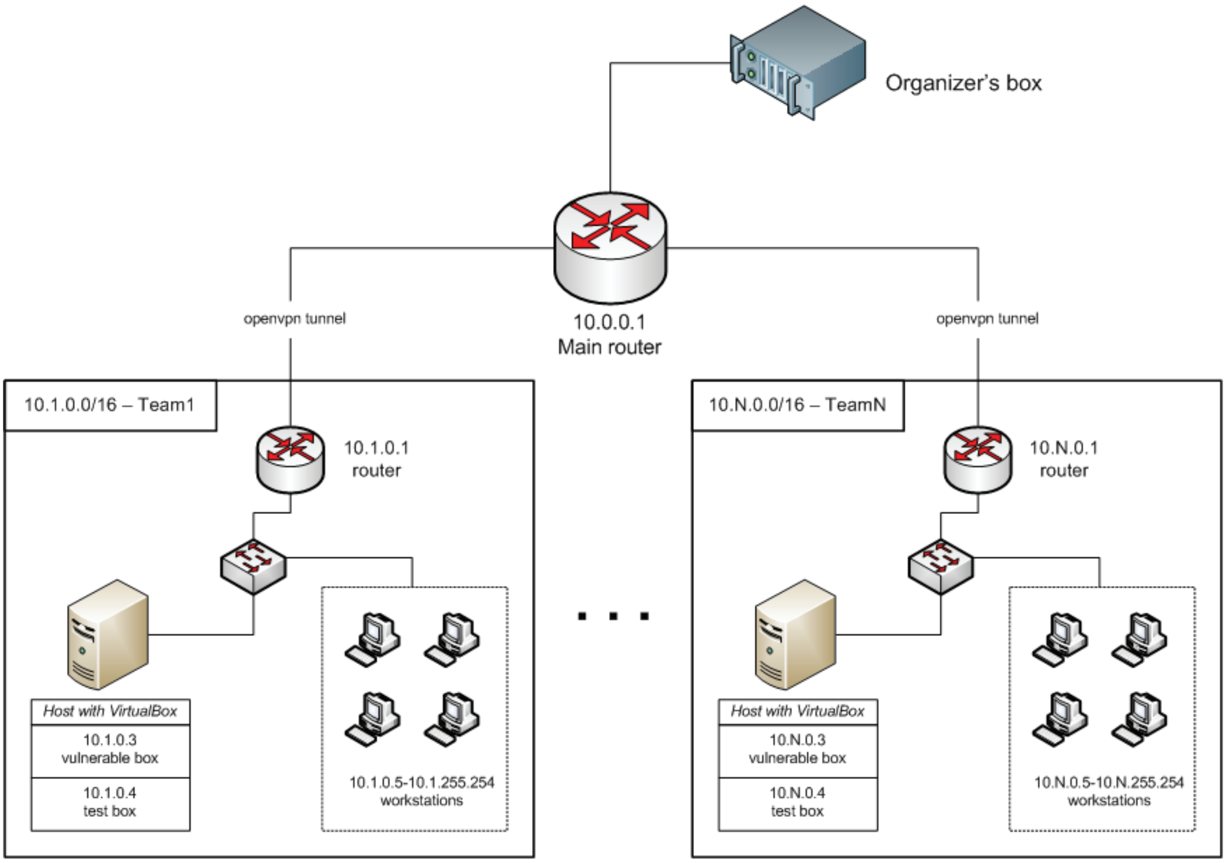


Fig. 2. Schematic diagram of the data collection «organizer's box».

Thus, visualization is more confidently takes its place in the line of tools for building information security. However, the existing standards of FIPS 199, 200 [4] pay little attention to the categorization of mapping and visualization tools, and even fewer -mechanisms,including legal, the use of such tools in an integrated approach.

In some cases, possible replacement of algebra to geometry, when constructing sets of matrices are replaced by a set of values arising from:

- the intersection of planes (the equations of the lines)

- the intersection of curved planes, the result of which may act set of values that lie on an infinite curve, on an endless intersecting curve on the infinite 3D-curve that can describe the relevant functions of the curve

- the intersection of curved planes, which result may be a set of values that lie on a curved circle (make the curve), with a curvilinear circle can give the group sets, obeying a unified description of the original curved planes such as: a set of values very curved circumference of the range of distances to the radius of a curved circumference of the set of values floating curved center of the circle with a radius of a constant.

Visualized help set the perception of the functions at a different angle which can provide visual perception and comprehension tasks in building security systems.

Building Systems IB using mapping and visualization much cheaper "algebraic" analogue, has a more "elegant" architecture. Set of values, comfortably playable using technology mapping and visualization is also possible to extract from the two-and three-dimensional images: the first case, the coordinates of points on the image, randomly arranged in a set. Inability to describe algebraically the set - is applicable to add value or vector color spectrum. In the second case, the problem is complicated by the third dimension. In principle, if necessary, the fourth dimension, variable, kaleidoscopic image should change according to the equation of time curve.

As an example - Logstalgia - a visualization program website traffic, based on the query log Web-server Apache. The program displays the work of the Web server as the game of tennis balls - an endless stream of requests of visitors.

On the screen appear as colored balls (the same color as the concrete visitor) that fly across the screen to arrive on the request. Successful requests discourage racket web server, and the poor (such as 404 - File not found), the server skips.

Visualization at any time can be stopped. During the pause, the individual requests can hover your mouse over and see the details.

Mapping and visualization are still a bottleneck in information security - science and practice.

The principle of comprehensiveness to ensure information security involves the use of all possible measures to counter the threats: ethical, legal, organizational, technical and mathematical. When implementation of this complex is an important and necessary coordinated the interaction of specialists in different subject areas. Among effective tools to enforce consistency, understanding and becomes visible in the perspective of mapping and viualizatsiya at all stages of the Information security [5].

References

1. DeveloperWorks. Data visualization tools for Linux. http://www.ibm.com / developerworks / ru / library / l-datavistools / index.html? S_TACT = 105AGX99 & S_CMP = GR01

2. KO. IT for business - http://ko.com.ua/node/48432

3. Information security. RuCTFE 2010 - http://habrahabr.ru/blogs/infosecurity/110576/

4. Logstalgia - a visualization tool of the Apache - http://www.tumencev.pp.ua/ programming / apache / logstalgia-project.html

5. Chubukov, SG, Elkin V., Fundamentals of Legal Informatics. - Moscow, 2007. - 84s.