10. Chappell L. *Wireshark Network Analysis. Second Edition. Protocol Analysis Institute, dba.* Chappell University, 2012. 461 p.
11. Apache Web Server Project. Available at: http://httpd.apache.org (accessed 20.09.16).
12. Slowloris (computer security) – Wikipedia Available at: https://en.wikipedia.org/ wiki/Slowloris_ (computer_security) (accessed 20.09.16).
13. Torshammer – a slow-rate DDOS attack tool. Available at: http://blog.nexusguard.com/slow-rate-ddos (accessed 20.09.2016).
14. ModSecurity: Open Source Web Application Firewall. Available at: http://modsecurity.org (accessed 20.09.2016).

Received 29.12.2016

ТЕХНОЛОГИИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ

УДК 004.7

WEB APPLICATION OF ESTIMATING PROTECTION SYSTEM EFFECTIVENESS OF THE ENTERPRISE

Bakhareva N.F., Fedorov S.V.
Povolzhskiy State University of Telecommunications and Informatics,
E-mail: fstepan2010@gmail.com

This article describes the WEB-application algorithm that allows to automate the audit of the company and to generate recommendations for the protection of the company in accordance with the requirements of the legislation. Moreover, it deals with the principle of the database formation. The authors describe the database according to the thematic issues of the information security for all the selected groups, private indicators and reference base, which is the master system of the protection. It is also represented the system of the group assessment, performance information security and the current reporting security of the enterprise. In the result, the authors give an algorithm of the visualization of the audit results. Using this application will reduce the resource and time which can be spent on the audit.

Ключевые слова: audit; algorithm; group metrics; private metrics; information security; information system; polar coordinates; Cartesian coordinates

Introduction

The initial step in the constructing comprehensive information protection system in the enterprise is the audit of the information security, which comprises the determination of the baseline level of the information system security.

Nowadays, the information security audit represents one of the most actual and dynamically developing directions of the strategic and operational management in the field of the company's information security. The relevance of the performing the audit is caused by the necessity to ensure information security in the organizations of various forms of ownership.

From the perspective of the audit work, there are three principle steps:

– collecting information and data, interviewing workers and the study of organizational, administrative and technical documentation;

– the analysis of data;

– the recommendations development to harmonize the safety requirements and reporting documents (report or conclusion on the results of the audit).

To automate the audit, to reduce resource and time expenses for it's conducting and visualization of the results together with Information System Technology (IST) a software in PHP language has been developed. The database was created on the basis of MYSQL. JavaScript and a technology for displaying Canvas material were used for visualization of results.

The purpose of the project

Create a WEB-application, which allows to automate the company's audit and to form the recommendations for the system protection of the company in accordance with the requirements of the legislation. The diagram of the WEB-application operation is shown in Picture 1.

The basic tasks of the application

1. To get information about the company, its functioning and security which is realized in the course of specially organized interviews with senior

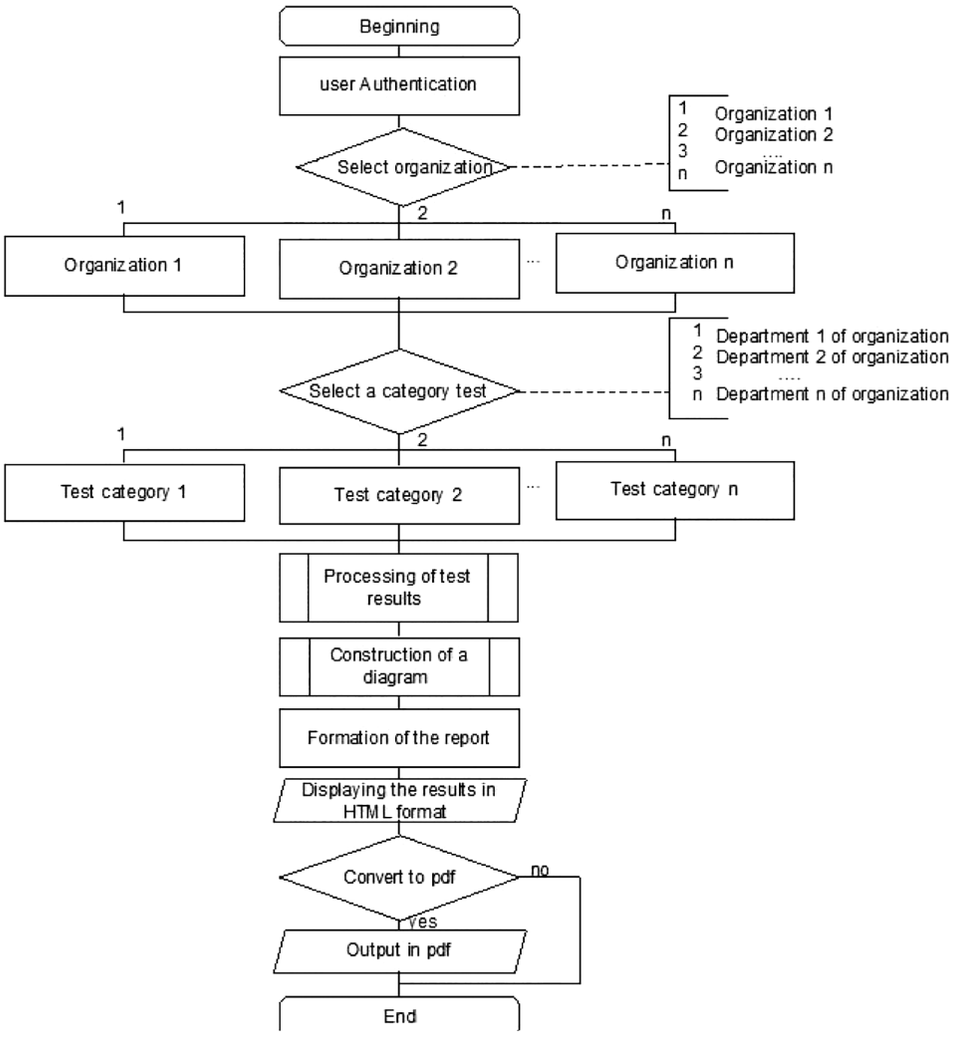
officials of the company, by examining technical, organizational and administrative documentation, as well as the study of the system information with the help of special software;

2. To create a database application. The first database represents the description of group and private information security indicators which are formulated in the form of thematic issues on the information security, and the answers to them will allow to describe the system of information protection in the enterprise in detail. The group indicators are formulated in the basic directions assessment of the state security company. 16 group performances (evaluation areas) are defined. The further stage of the development is to expand the number of group and private indicators depending on the specific of the undertaking, the volume and the area of the survey.

The second database is a reference system protection. The reference system is formed according to the requirements of the Russian Federation legislation in the field of information security. Audit is conducted on the bases of the requirements for public information systems that process personal data. These requirements are regulated in accordance with the Federal service of the Technical and Export Control (February 11, 2013, № 17) «The approval of the data protection requirements which don't constitute a state secret of the state information systems».

The answers to all thematic issues must be evaluated by the unit, which has the full conformity with the requirements. The organizational and technical requirements for the information security are formed according to the class of security information system. The program includes all possible classes of the security, ranging from 1 (the highest) to 4 (the lowest).

After generating report, we compare obtained results with the standard audit protection system, and form recommendations to eliminate vulnerabilities.



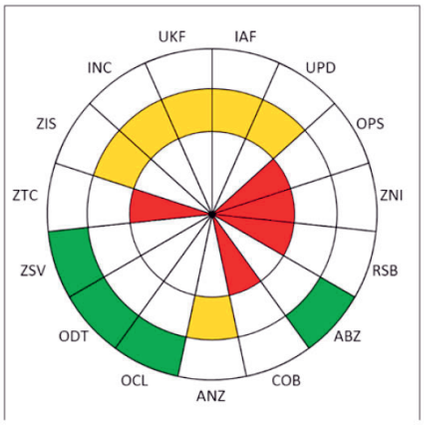
Picture 1. Schematic diagram of the algorithm of the WEB-application

3. The system of group performance assessment. The evaluation of group indicator P_i is computed from the estimates which contain private indicators P_{ij} in it. It's necessary to consider the significance of the coefficients α_i, which define the importance of the private indicators for evaluating group indicators. When counting coefficients of the significance α_i it should be performed the normalization condition: $\sum_{j=1}^{n} \alpha_j$, where n – the number of private indicators in the i-th group indicators. In this work, the coefficients inside each group indicators are equal and their sum is one. The plans of this work development is to build a detailed algorithm for calculating the significant coefficients which define the importance of the private indicators.

4. The formation of audit reports. The obtained test answers (calculation of the group and private indicators, pie chart) are reflected in the conclusion (report) about the results of the audit. The report which is obtained after the audit will allow to organize work about the construction of enterprise protection system. It is a key document describing: parameters and properties of an information system, its organizational and technical description, interaction with other systems, organization of information security (physical security arrangements, software, firmware and hardware protection), tasks and business processes, which enterprise information system carries out. It's also important to determine the most probable threats for the security concerning resources and information system security that makes possible the realization of these threats.

Thus, the construction of current status of company security and the recommendations to harmonize the protection system are formed.

5. The visualization of results. In addition to the reports and recommendations of audit, the results are presented by yet chart, as it is illustrated in Picture 2. All the calculated parameters are displayed in the group chart information of security sectors.



Picture 2. The Diagram of the indicators security enterprise

Where IAF – Identification and authentication;
UPD – Management software access;
OPS – Limits software environment;
ZNI – Protection machine data carriers;
RSB – Registration of events security;
ABZ – Anti-virus protection;
SOB – Intrusion Detection;
ANZ – Analysis of data protection;
OCL – Ensuring the integrity of the information system;
ODT – Providing access to information;
ZSV – Protection virtualization environment;
ZTC – Protection technical means;
ZIS – Protect information system and her means of transmission;
INC – Detection incidents and respond to them.
UKF – Configuration management information system.

In the sector, one of three zones is colored in different colors, depending on the value of indicator. In final evaluation of indicator group red (critical) level is displayed from 0 to 50 percent, yellow (average) level of protection is displayed from 50 to 75, and green (high) level is from 75 or higher. To place text next to the levels, it's necessary to convert the polar coordinates to Cartesian.

The definition zones of the filling one security indicator. This code fragment draws the arc and reduces to the center of the circle line:

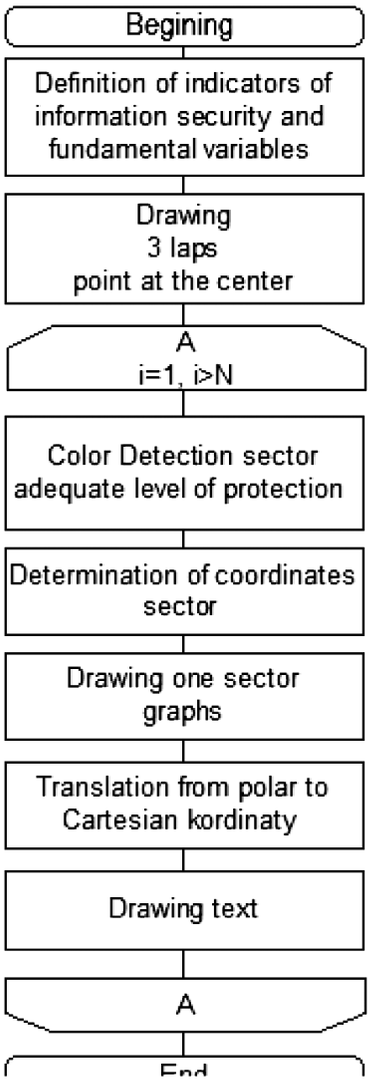
```
var start=(Math.PI/180)*270+(Math.PI/180)*num*i;
context.arc(beginX,beginY,radius3,start,start+(Math.PI/180)*num,false);
```

BeginX – Initial coordinates - X
BeginY – Initial coordinates - And
Radius3 – The radius of the circle
Start – Start coordinates
Num – Number of categories.

For example, to display the name of the measures security next to the indicator in the chart, it is necessary to translate the coordinates from polar to Cartesian. The code snippet of the conversion from polar to Cartesian coordinates to print the text in the chart:

```
x=(beginX-42)*Math.cos (start+(Math.PI/180)*num/2) + (beginX-30);
y=(beginY-50)*Math.sin(start+(Math.PI/180)*num/2)+(beginY+10);
context.beginPath();
context.fillText(«»+arrayKategory[i]+»», x, y);
```

BeginX – Initial coordinates – X
BeginY – Initial coordinates – And
Start – Start coordinates
Num – Number of categories



Picture 3. The scheme of the algorithm for constructing a pie chart indicators enterprise security

In Picture 3, it is a schematic diagram of the algorithm for constructing the indicators enterprise security.

6. The transferring of all the results in PDF-document.

Conclusion

The software is situated at the implementation stage in the IST Company and is used to audit the security state of information system in the enterprise.

References

1. STO BR IBBS-1.2-2014. Metodika ocenki sootvetstviya informacionnoj bezopasnosti organizacij bankovskoj sistemy Rossijskoj Federacii trebovaniyam [The Bank of Russia Standard for Ensuring Information Security of Organizations of the Banking System of the Russian Federation #1.2-2014. Methodology for assessing the compliance of information security of organizations of the banking system of the Russian Federation with requirements]. Moscow, Izdatelstvo standartov Publ., 2014. 101 p.
2. Audit informacionnoj bezopasnosti. Available at https://ru.wikipedia.org/wiki/Аудит_информационной_безопасности (in Russia).
3. Rowell E. HTML5 Canvas Cookbook. Birmingham, Packt Publ., 2011. 332 p.
4. Williams L.J. Learning HTML5 Game Programming. A Hands-on Guide to Building Online Games Using Canvas, SVG, and WebGL. Boston, Addison-Wesley Professional Publ., 2011. 256 p.
5. Hawkes R. Foundation HTML5 Canvas. For Games and Entertainment. New York, friendsofED Publ., 2011. 316 p.
6. Fulton S. Fulton J. HTML5 Canvas. Boston, O'Reilly Media Publ., 2011. 650 p.
7. Flanagan D. Canvas Pocket Reference. Scripted Graphics for HTML5. Boston, O'Reilly Media Publ., 2010. 110 p.
8. Sleverstudents. Available at: http://cleverstudents.ru (in Russia).
9. Hbc. Available at: http://hbc.ru (in Russia).
10. Niisokb. Available at: http://niisokb.ru (in Russia).

Received 15.01.2017

Bakhareva Nadezhda Fedorovna, Povolzhsky State University of Telecommunications and Informatics, 77, Moscovskoe shosse, Samara 443090, Russian Federation; the Head of Department of Informatics and Computer Technics Department, Doctor of Technical Science, Professor. Tel. +78462280013 E-mail: bakhareva-nf@psuti.ru

Fedorov Stepan Vasilevich, Povolzhsky State University of Telecommunications and Informatics, 77, Moscovskoe shosse, Samara 443090, Russian Federation; student of the Department of Informatics and Computer Technics Department. Tel: +79270121993. E-mail: fstepa010@gmail.com

DOI: 10.18469/ikt.2017.15.1.05

WEB-ПРИЛОЖЕНИЕ ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ПРЕДПРИЯТИЯ

Бахарева Н.Ф., Федоров С.В.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: fstepan2010@gmail.com

Аудит информационной безопасности предприятия представляет собой одно из наиболее актуальных и динамично развивающихся направлений стратегического и оперативного менеджмента в области информационной безопасности. Актуальность проведения аудита обусловлена необходимостью обеспечения информационной безопасности в организациях различных форм собственности. При организации аудита выделяют три этапа: сбор информации и сведений, интервьюирование работников и изучение организационно-распорядительной и технической документации; анализ полученных данных; выработка рекомендаций по приведению в соответствие требованиям безопасности и подготовка отчетных документов (отчет или заключение по результатам проведенного аудита). В статье приведены алгоритм WEB-приложения, позволяющего автоматизировать аудит компании и сформировать рекомендации по приведению системы защиты предприятия в соответствие с требованиями законодательства, а также принцип формирования используемой базы данных: базы тематических вопросов по всем выделенным групповым и частным показателям и эталонной базы информационной безопасности, которая представляет собой эталонную систему защиты. Представлена система оценки групповых показателей информационной безопасности и формирование отчета о текущем состоянии защищенности предприятия. Приведен алгоритм визуализации результатов аудита. Построенная диаграмма показателей защищенности системы предприятия наглядно показывает уровень защищенности информационной системы предприятия по основным группам показателей. Использование приложения позволит сократить ресурсные и временные затраты на проведение аудита при соответствии требованиям Приказа Федеральной службы по техническому и экспортному контролю от 11. 02. 2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Ключевые слова: аудит, алгоритм, групповой показатель, частный показатель, информационная безопасность, информационная система, полярные координаты, декартовы координаты

Бахарева Надежда Федоровна, д.т.н., профессор, заведующая Кафедрой информатики и вычислительной техники (ИВТ) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. (8-846) 339-11-31. E-mail: bahareva-nf@psuti.ru

Федоров Степан Васильевич, студент ПГУТИ. Тел. 8-927-012-19-93. E-mail: fstepan2010@gmail.com

Литература

1. СТО БР ИББС-1.2-2014. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям. - Введ. 2014-06-01: Изд-во стандартов, 2014. – 101 с.
2. Wikipedia. Аудит информационной безопасности, 2015 // ru.wikipedia.org (д.о. 22. 12. 2016).
3. Rowell E. HTML5 Canvas Cookbook / Packt Publishing, 2011. – 332 p.
4. Williams L.J. Learning HTML5 Game Programming. A Hands-on Guide to Building Online Games Using Canvas, SVG, and WebGL / Addison-Wesley Professional 2011. – 256 p.
5. Hawkes R. Foundation HTML5 Canvas. For Games and Entertainment / friendsofED 2011. – 316 p.
6. Fulton S. Fulton J. HTML5 Canvas / O'Reilly Media, 2011. – 650 p.
7. Flanagan D. Canvas Pocket Reference. Scripted Graphics for HTML5 / O'Reilly Media, 2010. – 110 p.
8. Cleverstudents Перевод градусов в радианы и обратно, 2015. // cleverstudents.ru (д.о. 23.12.2016).
9. Hbc. Оценка эффективности систем защиты информации, 2015. //, hbc.ru (д.о. 21.12.2016).
10. Niisokb. Аудит информационной безопасности, 2015. // niisokb.ru (д.о. 10.12.2016).

Получено 15.01.2017