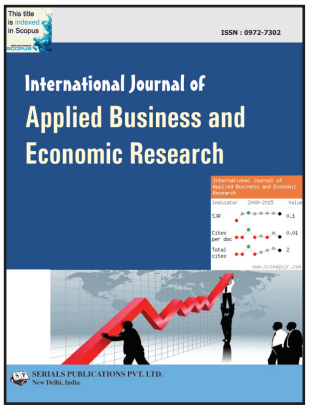

International Journal of Applied Business and Economic Research

ISSN: 0972-7302

available at http: www.serialsjournal.com

Volume 15 • Number 12 • 2017

Verification of Computer Systems of Commercial Bank

Viktor V. Erokhin[1], Valentina V. Fetshchenko[2], Irina S. Panina[3], Natalia P. Kazimirova[4], Sergey P. Novikov[5] and Alexandra V. Novikova[6]

[1,2]*Bryansk State University Named after Academician I.G. Petrovsky, Bryansk, Russia*

[3]*Plekhanov Russian University of Economics (Bryansk branch), Bryansk, Russia*

[4]*Plekhanov Russian University of Economics (Bryansk branch), Bryansk, Russia. Email: kazimirova-natali@narod.ru*

[5]*Financial University under the Government of the Russian Federation (Bryansk branch), Bryansk, Russia*

[6]*Bryansk State Technical University; Bryansk, Russia*

ABSTRACT

This article sets out the main aspects and characteristics of information security technologies in bank telecommunication systems, as well as approaches to the analysis of information security of bank systems. The problems of information verification in computer and economic systems of the bank are solved. The method of software verification that uses logical statements which are directly constructed on the basis of the initial codes of a software tool is shown. Verification of a parameterized model of the bank computer system does not require basic model transformation, which is used in verification with the help of "Model Checking" tools or participation of experts. The presented verification of computer systems allows to explore the following classes of bank information systems parameterized by the number of interacting components: distributed algorithms - wave algorithms, the distribution of resources, mutual exclusion of access to a critical section, leader election, termination detection, distributed commit; network protocols - ring with a marker, routing protocols, protocols of providing quality of service, multicast protocols; hardware circuits - hardware circuits for controlling the access to the bus with a different number of client devices and protocols guaranteeing cache coherence.

JEL Classification: C89, C80, K22, L81, G21.

Keywords: Information security, verification of information, bank.

1. INTRODUCTION

Modern commercial banks frequently face breaches of certain characteristics of software and informational support security due to the unauthorized actions made by bank employees (Averchenkov, 2005; Erokhin,

2015; Ignatiev, 2005). Basic commercial banks of the government set goals to improve technologies and control mechanisms of their information support and software. At present, banks use such integrated information systems and technologies as CALS, ERP, MRP that ensures a significant degree of software and information support protection (Erokhin, 2009). Banks use a number of information systems to avoid and prevent unauthorized use of software, but none of them provides integrated protection of bank systems. The need to ensure integrated protection of software and information systems necessitates the development of a unified system for the protection of bank. The main aim of integrated protected system is prevention of the maximum number of types of 'insider' attacks.

Currently, the following methods can be used to verify reliability of software functioning: testing, theoretical and evidence-based approach, and verification of program models.

Testing is the most frequently used method to verify information in bank systems. During testing, test data prepared in advance are feed to the program and then the results are compared to the expected results. The main feature of testing is the determinacy of the algorithm. In the distributed software using a set of processes and running on multiple computers, the software work is rather ambiguous. In this case, tracing tools can be applied to control the software work in a process of calculating the variables and data.

2. LITERATURE REVIEW

Methods of verification of information aim to prove mathematical theories about the properties of the functioning software or its results. This approach to control the reliability of software functioning was first introduced in scientific publications of A.A. Lyapunov, T. Hoare, E. Dijkstra, Pratt and Floyd.

A significant contribution to the development of methods to solve this problem was made by Russian scientists Parkhomenko P.P., Lipaev V.V., Soghomonyan E.S., Mayorov S.A., Nemolochnov O.F., Ryabov G.G., Seljutin V.A., Kureichik V.M. and many others.

3. METHODS AND MATERIALS

When choosing actions for verification of bank computer systems it is advisable to adhere to the principle that the cost of their implementation must not exceed the value of protected software resources of the bank. The value of information resources consists in their functionality and relevance. Factors that cannot be expressed in monetary terms, such as loss of reputation, should also be kept in mind. Basic control measures from the viewpoint of the legislation of the Russian Federation are (Erokhin, 2015; Kuznetsov, 2010):

- ensuring confidentiality of personal data of bank's employees;
- protection of accounting data of a bank;
- protection of intellectual property rights.

The types of access that should be considered in accordance with GOST R ISO/IEC 17799-2005, are:

- physical - to premises, computer and server rooms;
- logical - to databases an information systems of a bank.

According to the classification system of bank's information resources, which is adopted in the bank, it is necessary to carry out labeling procedures (Erokhin, 2015). Labeling procedures must be carried out for information resources in both electronic and paper form. This article analyzes the labeling of information resources in electronic form. During the marking process, information resources should be taken into account - copying, storage, disposal, transfer, etc. Labeling of information resources is also necessary for the subsequent procedure of authorization of the bank employees.

Methods of verifying software that use the theoretical and evidence-based approach are based on theorem prover tools. The description of software is in the form of a set of logical assertions. Specification of software is also in the form of an assertion. A theorem prover generates proof of feasibility of specifications based on the statements describing tested software.

Using a theorem prover while generating evidence may require the participation of an expert. One of the most difficult tasks that appear in the verification of software with a theorem prover is the task of generating the loop invariant. Loop invariant is required during the control of deductivity of function's postcondition from preconditions.

Verification of software with the use of logical assertions directly generated on the basis of the source code increases the complexity of the proof. Some code fragments might be irrelevant for checking the selected properties of the software. Software properties can be tested on the model of the software, simpler than the original. Methods based on Model Checking use a compromise approach between the full software verification, and testing using formal verification of properties.

An automated system for restricting access to information and software (ASRAIS) has a complex structure. It should solve the problem of leakage of information resources beyond the software of a commercial bank. The basic objects protected by the projected ASRAIS are (Erokhin, 2015; Markov, 2012; Melnikov, 2012):

- information resources of a bank, whose loss or unauthorized changes entails damage or loss of reputation of the bank;
- information and software processing. An example of processing is execution, storage, transmission, display, computation, modification, and disposal;
- software of a bank;

IT architecture - structured integrated automated systems and technologies of a bank. Information Protection and Control (IPC) Technology is a technology of protection of information resources against internal threats. IPC-class solutions are designed to protect information resources against internal threats, prevent of various types of information resources leaks, industrial espionage and intelligence. The task of IPC is to prevent the transmission of information resources beyond the perimeter of the main information system. IPC technology combines three fundamental principles (Erokhin, 2015):

- monitoring of communication channels with the help of Data Loss Prevention (DLP) technology;
- access control to the network, applications, and data;
- encryption of data storage media.

During the work of IPC, the detection of information content is commonly used. Detection of information content might occur through the following methods (Erokhin, 2015):

- manual detection ("Quarantine");
- 'fingerprinting';
- signature method;
- labelling method;
- method of linguistic analysis;
- 'regular expressions' method.

The manual detection method ('Quarantine') is based on the use of manual testing. When a personnel member attempts to access files containing confidential data, information security department of the bank is informed, which decides on further action: granting or refusing access to the requested data (Averchenkov, 2006; Bauer, 2007; Erokhin, 2015).

The advantage of this method is its effectiveness. The drawback is that this method is practically unrealizable in large banks, as it requires a lot of human resources. 'Quarantine' method can be used together with other methods to analyze the behavior of selected 'suspicious' employees.

In the 'Digital Fingerprints' method, the data base of samples (patterns, templates) of confidential files is formed. At the beginning of the work, a file template is created and transferred to the DLP-system, then it is fingerprinted and transmitted to a special 'patterns' database. Afterwards in the file content filtration rules the percentage of matching with the pattern is adjusted. The advantage of this method is the fact that the filtration system of data traffic is able to work with information in any format. Other advantages of the system based on the 'digital fingerprint' technology include (Bauer, 2007; Erokhin, 2015):

- transparency of the algorithm for the staff of the Information Security Department;
- high degree of detecting violations incidents;
- ease of adding new file templates (patterns).

The disadvantages of this method are:

- sensitivity to changes in template files;
- the requirement to provide additional protection of the patterns database (special arrangement of servers, forming the rules of admission of employees to the database);
- reduction in the efficiency of detection if an overflow of patterns data base occurs, which frequently happens in practice;
- a high influence on the performance of the main bank's information system;
- low efficiency of the method working with graphic files.

In large banks, it is difficult to implement this technology because the database of template files grows too fast, and it increases the load on the servers of the DLP system. Moreover, the problems of filling the database and load balancing arise.

The signature method is a search in the data flow of certain character sequences, so-called 'stops' of forbidden character sequences. This method is 'deterministic' because its algorithm is configured to search for 100% matching with 'stops'. Most signature systems are designed to search for multiple words and the frequency of their occurrence. The advantages of the signature method are:

- self-evident principle of its functioning;
- ease of implementation and configuration.

The disadvantages are:

- sensitivity to the intentional replacement of some characters (for example, similar characters from another alphabet);
- inefficiency in working with program code files;
- inapplicability of the method to graphic files;
- dependence of the functioning on language (both natural and artificial).

DLP-systems based on the signature method are well adjusted to the western market but are hardly applicable in Russia. The reason is that Russian is a non-signature language: there are many prefixes, suffixes and endings.

The 'labels' method consists in placing special 'tags' inside the files containing confidential information. The advantages of the method are:

- high detection rates;
- the accuracy of the information provided;
- high speed.

The disadvantages are:

- complexity - this method requires changing the structure of the entire structure of the bank's information system;
- need for additional adjustments when creating a new file with confidential information.

Linguistic methods are the most commonly used in DLP-systems as they provide a flexible tool for detection of information content. Linguistic analysis of a text includes several detection methods:

- parsing;
- semantic analysis;
- morphological analysis, etc.

Their use increases the efficiency of DLP-systems. The disadvantages of linguistic methods:

- sensitivity to rephrasing sentences;
- ineffective for code files;
- inapplicable for graphic files;
- dependency on the language of the information content.

The method of 'regular expressions' (method of 'text identifiers') has only recently been used in DLP-systems. Regular expressions allow to find matches on data type (their form of presentation). The main difference from the method of 'signatures' is the search, which is done not according to the value but to the type of data. In fact, a block of identical information is searched. Such method is effective for searching of (Panasenko, 2009):

- tags of items;
- dates;
- address (MAC, IP, Internet services);
- port numbers;
- credit card numbers;
- account numbers;
- passport numbers;
- classificators, etc.

The advantages of the method are (Panasenko, 2009):

- high efficiency;
- high level of performance;
- ability to detect types of content specific for each bank;
- applicability of the method for graphic files.

The 'regular expression' method of is often used as an additional algorithm in DLP-system.

It should be noted that the methods above, which are used in modern DLP systems, work with open data. If an attacker - a bank employee breaching his official duties and violating the rules of work with the bank's information resources tries to convey the confidential information in an encrypted form, modern DLP-systems will not be able to prevent leakage. The designed ASRAIS provides a solution to this problem by adding a special module with cryptanalysis techniques embedded into its core (Burnet, 2009; Erokhin, 2015).

The main function of the modular subsystem of DLP-class is tracing leaks of information through the network, removable storage media, printers, etc. In other words, threat detection takes place where the bank software contacts with the external environment - WAN, and all 'interfaces-outputs' such as removable storage media, fax machines and printers. DLP-class subsystem is not responsible for monitoring the internal flow of confidential information in the bank. One of the objectives of modular subsystem of DLP-class is to control the work of those who use the bank software through the global network, the Internet. The purpose of the protection of strategically important information and software resources is to prevent or minimize the damage caused (directly or indirectly) to the subjects of information relationships through undesirable influence on the software components of the bank, as well as disclosure (leakage), distortion (modification), loss (loss of accessibility) or illegal replication of information, improper and incorrect use of software resources. Thus, the use of only one of these technologies is not able to solve the problems of

protection of information and software of the bank. It is necessary to use all three subsystems in a single complex to ensure the required level of protection.

As an example of the proposed method of verification of models of different levels, we considered Graph Model of abstract and structured automated conversion scheme, its implementation and the construction of comprehensive coverage of the scheme using the method of intersection of all cubes of sub-scheme singular covers and the method of intersection with restrictions. On the basis of complex cubic coverage of the scheme the transition graph charts has been restored and the conclusion about the isomorphism of the graphs and, consequently, their identity was made. That led to the conclusion about verification of the models of different levels.

4. RESULTS AND DISCUSSIONS

For the models of the same level of abstraction, the method of verification using complex coverage based on # and ∩ operations of cubes of comprehensive coverage of the analyzed schemes is proposed. Let us consider the application of the conditions of necessity and sufficiency in the verification of schematics realized with the method of modeling. Let a certain Boolean function f be set with its coverages $C1(f)$, with $f = 1$, and $C0(f)$ with $f = 0$ which are drawn with in arbitrary way, e.g. the Karnaugh map. It is required to verify a schematic for f as a logic circuit N (with an external output ZN), designed, for example, heuristically on an arbitrary basis with the use of methods of factorization, decomposition or their combination.

The prerequisite for the verification is the coincidence of scheme reactions N ZN = 1(ZN = 0) for ∀ with ∈ $C1(f)$ (® with ∈ $C0(f)$).

A sufficient condition for the verification is the coincidence of scheme reaction ZN = 0 (ZN = 1) for ∀ with ∈ $C0(f)$ (∀with ∈ $C1(f)$).

Thus, the necessary and sufficient conditions for the verification of scheme N is the coincidence of the scheme's ZN reaction with the values of a Boolean function f for all cubes with ∈ $C1(f) \cup C0(f)$. The comprehensive coverage $KP = C1(f) \cup C0(f)$ is the meta-model of scheme N. The verification of scheme N can be carried out in another way different from the method of modeling.

We construct a meta-model scheme for the ZN output values, equal to 0 and 1, in the form of comprehensive coverage $KP = C_0(ZN) \cup C_1(ZN)$. In this case it is required to establish a correspondence between $C_0(f) \cup C_0(f)$ and $C_0(ZN) \cup C_1(ZN)$ coverages which can be done either subtracting cube coverages (#), or by intersecting cube coverages (∩). When using subtraction to verify scheme N, it is necessary that $C_1(f) \# C_1(ZN) = \varnothing$, and sufficient that $C_1(ZN) \# C_1(f) = \varnothing$. It is similar for coverages $C_0(f)$ and $C_0(ZN)$. It follows that when using subtraction it is sufficient to have only one type of coverage - either single $C_1(f)$ and $C_1(ZN)$, or zero $C_0(f)$ and $C_0(ZN)$.

The use of algebraic topology operations of subtraction and intersection of coverages allows to avoid the exact match of the elements of sets during the comparison of sets, that is why $C_1(f) \# C_1(ZN)$ and $C_1(ZN) \# C_1(f)$ are not analogues (not topological) of conventional subtraction of sets (A \ and B \ A).

Having applied subtraction (#) and intersection (∩) of intersections in the verification of objects, we will get four possible relationships:

1. $C_1(f)$ # $C_1(ZN) = \varnothing$ and $C_1(ZN)$ # $C_1(f) = \varnothing$, or $C_1(f) \cap C_0(ZN) = \varnothing$ and $C_0(f) \cap C_1(ZN) = \varnothing$ – conditions of complete verification.
2. $C_1(f)$ # $C_1(ZN) \neq \varnothing$ and $C_1(ZN)$ # $C_1(f) = \varnothing$, or $C_1(f) \cap C_0(ZN) \neq \varnothing$ and $C_0(f) \cap C_1(ZN) = \varnothing$ – is a necessary but insufficient condition for verification.
3. $C_1(f)$ # $C_1(ZN) = \varnothing$ and $C_1(ZN)$ # $C_1(f) \neq \varnothing$, or $C_1(f) \cap C_0(ZN) = \varnothing$ and $C_0(f) \cap C_1(ZN) \neq \varnothing$ – is a sufficient but not obligatory condition for verification.
4. $C_1(f)$ # $C_1(ZN) \neq \varnothing$ and $C_1(ZN)$ # $C_1(f) \neq \varnothing$, or $C_1(f) \cap C_0(ZN) \neq \varnothing$ and $C_0(f) \cap C_1(ZN) \neq \varnothing$ – there are no conditions for verification.

In the 2nd and 3rd cases we can talk about the verification of partially defined functions (objects) with the use of 'fuzzy' sets, in other words, one object 'does' more than the other one. Full verification exists only if there is the ratio of the 1st case. This reasoning is conducted for the case of the single-output scheme N and initial coverage of a Boolean function, which is the simplest case of a meta-model of the highest rank.

Similar methods can be applied for the verification of algorithms of graph-schemes, finite automata (abstract and structural) of multiple-sequential circuits and software.

Two methods of verification of these processes are proposed:

- the method of algebraic-topological subtraction of each coverage from each. If there is an empty value of the result, a conclusion of the equivalence of data is made;
- the method of constructing test sets of complex coverages by intersection of cubes from interval parts of the coverages and cross-testing, the results of which help to conclude about the results of verification.

Let us consider the example of the verification of an acyclic process. Let some interval formula be set:

$$r = \begin{cases} \text{FR1}, & x \le k_1; \\ \text{FR2}, & k_1 < x < k_2; \\ \text{FR3}, & x \ge k_2; \end{cases}$$

which implements calculations of some variable '*r*' for different formulas: FR1, FR2 and FR3 of any type depending on the two Boolean variables that specify certain conditions-predicates in the form of inequalities: *a*: $x \le k_1$ and *b*: $x \ge k_2$.

The transition from the inequalities to Boolean variables in the design of the computational process allows to abstract from the concrete meaning of inequalities and their respective conditions-predicates and to consider the solution of verification tasks in general terms.

GAM calculations of the variable '*r*' are shown in Figure 1. The functional decomposition of Boolean function $f = f(a, b)$ with the initial vertex of a condition-predicate '*a*' (GAM1) is shown in Figure 1, and in Figure 1*b* it is shown with the initial vertex '*b*' (GAM2).

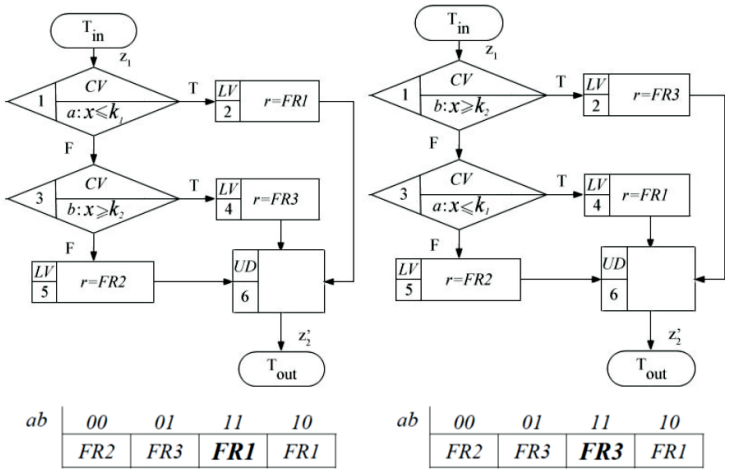

Figure 1: GAM computing of interval formula

Let us construct complex cubic coverages $C_1(r)$ and $C_2(r)$ for the computational variable '*r*' for GAM1 and GAM2:

$C_1(r)=$

z_1	a	b	r	r'	z_2'	$\{c\}$
1	1	×	×	/FR1/	1	c_1
1	0	1	×	/FR3/	1	c_2
1	0	0	×	/FR2/	1	c_3
0	×	×	p	p	0	c_4

$C_2(r)=$

z_1	a	b	r	r'	z_2'	$\{c\}$
1	×	1	×	/FR3/	1	c_1
1	0	0	×	/FR2/	1	c_2
1	1	0	×	/FR1/	1	c_3
0	×	×	p	p	0	c_4

Using coverages $C_1(r)$ and $C_2(r)$ let us construct tests $T_1(r)$ and $T_2(r)$ with the intersection of cubes from the interval parts of coverages $C_1(r)$ and $C_2(r)$ coatings, respectively. We get the following tests:

$T_1(r)=$

z_1	a	b	r	r'	z_2'	$\{t\}$
1	1′	0	×	/FR1/	1	t_1
1	0′	0	×	/FR2/	1	$\tilde{t}_1$
1	0	1′	×	/FR3/	1	t_2
1	0	0′	×	/FR2/	1	$\tilde{t}_2$
1′	0	1	p	/FR3/	1	t_3
0′	0	1	p	p	0	$\tilde{t}_3$

$t_1/\ \tilde{t}_1 \in c_1 \cap c_3$ из $C_1(r)$

$T_2(r)=$

z_1	a	b	r	r'	z_2'	$\{t\}$
1	0	1′	×	/FR3/	1	t_1
1	0	0′	×	/FR2/	1	$\tilde{t}_1$
1	1′	0	×	/FR1/	1	t_2
1	0′	0	×	/FR2/	1	$\tilde{t}_2$
1′	1	0	p	/FR1/	1	t_3
0′	0	1	p	p	0	$\tilde{t}_3$

$t_1/\ \tilde{t}_1 \in c_1 \cap c_3$ из $C_2(r)$

For the formulas the conditions / FR1 / ≠ / FR2 / ≠ / FR3 / ≠ *p* must be satisfied, i.e calculated and stored values should vary at different test sets. The values of actively changing conditions-predicates are marked with hatches in the tests.

In view of the removal of ab = 11 verification by coverages gives $C_1 \# C_2 = \varnothing$ and $C_2 \# C_1 = \varnothing$, that indicates the equivalence of computational processes. It can be clearly seen in the Karnaugh map shown in Figure 1.

Cross-testing yields the following result: $R_1(T_1) = R_2(T_1)$ and $R_1(T_2) = R_2(T_2)$, which also confirms the equivalence of computational processes. If the variable '*r*' is calculated according to different simplified formulas FR1, FR2 and FR3, then the method of cross-testing is preferred because it does not require the formulas to be reduced to a canonical form.

5. CONFIRMATIONS

The described method of verification, which was used in the architecture of the experimental bank system, where its application for verification of parameterized model of the Resource Reservation Protocol (RSVP) was carried out. The verification of this protocol helped to identify the main problems in the application of the method and bottlenecks in its implementation. In the course of the protocol's verification, the relation of half-modular simulation and technology of its optimization were proposed.

The practical significance of the work consists in methodological support of the development of hardware and software to protect the bank's automated systems, created using the results of the analysis of the merits and shortcomings of the existing technological solutions. The work bears a theoretical nature. However, its results can be used in the design of computer systems and in studying the problems of their reliability.

References

Averchenkov, V. (2005). *Security System of Russian Federation* (1st ed.). Bryansk: Bryansk State Technical University.

Averchenkov, V. (2006). *Organizational Management Systems* (1st ed.). Bryansk: Bryansk State Technical University.

Bauer, F. (2007). *Decrypted secrets. Methods and Maxims of Cryptology* (1st ed.). Moscow: Mir.

Burnett, S. (2009). *Cryptography. Official RSA Security Manual* (2nd ed.). Moscow: Binom-Press.

Erokhin, V. (2015). *Information System Security* (1st ed.). Moscow: Flinta.

Erokhin, V. (2015). *Protection of Software and Verification of Information in the Bank's Information and Telecommunication Systems* (1st ed.). Moscow: MSU.

Erokhin, V. (2009). *Systems of Management of Production Process* (1st ed.). Bryansk: Bryansk State Technical University.

Ignatiev, V. (2005). *Information Security of Modern Commercial Enterprise* (1st ed.). Stary Oskol: OOO "TNT".

Kuznetsov, S. (2010). *Modern Technologies of Document Management* (1st ed.). Moscow: MEI.

Markov, A. (2012). *Methods of Assessment of Discrepancies of Information Security* (1st ed.). Moscow: Hotline Telecom.

Melnikov, V. (2012). *Information Security* (1st ed.). Moscow: Academia.

Panasenko, S. (2009). *Encryption Algorithms. Special reference-book* (1st ed.). St.Petersburg: BHV-Petersburg.