NEWS
OF THENATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 1, Number 335 (2021), 14 – 18 **https://doi.org/10.32014/2021.2518-1726.2**

UDC 004.056.53
IRSTI 81.93.29

N. Baisholan[1], K.E. Kubayev[2], T.S. Baisholanov[3]

[1,2,3] Al-Farabi Kazakh National University, Almaty, Kazakhstan.
E-mail: baisholan@mail.ru, kubaev.k@mail.ru, btstalgat@mail.ru

MODERN TOOLS FOR INFORMATION SECURITY SYSTEMS

Abstract. Efficiency of business processes in modern organizations depends on the capabilities of applied information technologies. The article describes and analyzes the role and features of audit tools and other methodological tools and models in ensuring the quality and security of information systems. The standard's principles are reviewed, as well as the importance of meeting business needs. In order to protect virtual values in a company's system environment, the importance of using information security models is revealed. Practical proposals in risk management and information security in information technology are analyzed through the COBIT standard.

Measures for protecting the information system of an organization from accidental, deliberate or fake threats are considered. The possibility of using one of the real information security models by the information recipient or provider in accordance with the requirements of external processes is reported.

Furthermore, in connection with increase in the number of attack methods and techniques and development of their new tools and vectors, the need to improve and ways to ensure information security are being considered.

The essential tasks of security audit are considered, and the stages of their implementation are described. With regard to security of information systems, an analytical model is proposed for determining vulnerability's numerical value.

Key words: COBIT methodology, ITIL library, ISO 20000 standard, information technology, information audit, information security, risk, vulnerability, COBIT ® 2019 Framework.

Digital technology advances automate everything from all social areas of society to the activities of large industrial organizations, including active implementation in the businesses, increased introduction of innovations in general. However, justifying the costs spent on them, rational budget planning for the development of information technologies in organizations and self-completion of new introduced IS in terms of functionality, and the process of improving the quality of control of the (digital) trend of digitalization – such events create the need to audit its IT and increase its relevance.

Although generally, the basis of the IT structure depends on the software, it is largely dependent on technology means, moreover, trends in development, introduction, application, maintenance, etc. require implementation through efficient solutions, which, in turn, requires information technology competence and knowledge to support various regulatory requirements.

Therefore, a number of ITIL libraries, COBIT methodology, ISO 20000 service management standards for managing information services and ensuring their security is applied on the IT market.

Concurrently, the COBIT (Control Objectives for Information and related Technology) methodology which was developed and proposed by ISACA in 1992, is a tool that is necessary directly for the IT audit service, which will gain demand on the modern IT market [1,2]. This abbreviation stands for a set of documents that define the principles of information technology management and audit.

The emergence and formation of this methodology can be described using figure 1 [3.4].

Today, the enhanced COBIT Version 5 standard greatly impacts improvements to meet the requirements of the information technology market, especially large institutions and risk management. As A.V. Repin indicated this, based on the works [1,5], this can be justified by the following principles:

1. Focus on meeting the needs of related party;
2. Coverage of all activities of an enterprise;

3. Reliance on the application of a single integration structure;
4. Ability to implement a seamless method;
5. Its focus on the separation of IT management from management in an institution.

Table 1 – Evolutionary stages of CobiT standards

Years	Versions	Name
1996	CobiT 1	Audit
1998	CobiT 2	Control
2000	CobiT 3	Management
2005/2007	CobiT 4	Information Technology Management
2012	CobiT 5	Company information technology management
2018	COBIT ® 2019	ENTERPRISE GOVERNANCE OF INFORMATION AND TECHNOLOGY (EGIT)

The COBIT standard, which has passed the indicated stages of development, is a combination of about 40 international standards of control, audit and management, information security. In other words, the COBIT standard is based on the generally accepted method, the BSC balanced scorecard, the improved SEI CMM/CMMI model, PMBoK (project management methodology) and the methods of PRINCE2, TickIT, ITIL® and other standards [5,6]. After Version 5, the COBIT ® 2019 Framework: Governance and Management Objectives version covering the ITIL, CMMI and TOGAF structures [7] is now applied more rationally. It is processed as a methodology for management and governance of corporate information and technologies that fully support institutions, and is aimed at managing this information, its security and risks.

Its principle lies in formation of compatibility of mutual understanding between management on the way to achieving the key business goals and IT service, as well as elimination of possible discrepancies. In this regard, a company operating in the COBIT electronic environment offers its managers, users of information systems and related auditors a set of measurements, trends and top practices approved to increase the benefits of information technology, and also creates IT guidelines and rules for a specific company and helps to rationally control the activities.

COBIT predicts which information in information technology management is reliable to achieve the most effective business goals of a company. Along with that, COBIT describes the relationship between business strategy and information technology, subsequently defines and supports IT values and implements control measures. The essential task is that information technologies should fully support and actively increase the competitive advantages defined in a company's strategy and, through the advancement of business requirements for information for the timely rationalization of costs, participate in building its prerequisites. According to this standard, having turned into a business tool, IT presents practical proposals for risk management and information security systems in IT.

In accordance with requirements of the Approach to Information Technology Management international standard (Cobit), the information system verification procedure consists of four stages:

- identification and documentation (planning and organization);
- management mechanisms assessment;
- identity test;
- detailed testing.

When describing the information security system in any institution, protection measures against accidental, intentional or fake threats to its information system based on such widespread information security properties as confidentiality, integrity, and availability [8] are also considered. To do this, regarding external processes requirements the information recipient and/or provider can apply one of the following models: CVSS3.1., Investigation Process, Diamond, Cyber Kill Chain, etc.

If the property of information security means a restriction in access to hidden indicators in the military industry, financial indicators in the economic industry, or to patient data in the medical industry, then the integrity property ensures the exclusion of a violation of reliability and authenticity of

information. The last property ensures unhindered use of any information available to the users of the information system at any time.

Therefore, in the course of reliable use of IS in an institution, the problem of correct choice of the necessary methodological tool arises, which can be solved through the management and control system.

On the practical side, this not only solves information technology problems, but also can ensure that the business needs are met. One of the key values of a company's system environment is virtual value, i.e., information sources in the form of intellectual property need to be protected and secured. For example, there is a need to use MITER ATT&CK (arising from the attacker's point of view) [11], CIA (Confidentiality-Integrity-Availability) models, since the security vulnerability of information systems might allow attacks. Thus, in a virtual environment, one of the ways to remotely use a company assets - the Papa Smurf attack, causes vulnerability of the network receiving ping packets and interferes with its conductive ability. Another attacked called SYN Flood is the action of server's TCP connections half-open on the server and its consequences lead to the closure of access to the server for legal users. Besides, attacking methods and techniques are being improved, as well as their new tools and vectors are being developed.

The main tasks of security audit are:

- Analysis of the risks associated with the likelihood of a threat to the security of IS resources;
- Assessment of the current level of IP security;
- Localization of narrow paths in IP security system;
- Assessment of IS compliance with standards applied in information security;
- Introduction of new techniques for IS security and development of proposals to improve current profitability.

In this regard, when performing these tasks, the IS security audit covers a number of the following stages such as:

- Conduct of a survey;
- Collection of information;
- Analysis of received data;
- Development of proposals;
- Preparing a survey report.

Security audit methods can be based on risk analysis, application of information security standards, or a combination thereof.

The risk magnitude is determined depending on the cost of resources, the likelihood of a threat and the scope of vulnerability based on the following formula [12]:

$$R = \frac{(p*d)}{v}, \quad (1)$$

where R – risk; p – fund cost; d – threat probability; v – vulnerability value.

The goal of risk management is to select proper countermeasures in order to reduce risk levels to a favorable level. While the cost of implementing countermeasures should not exceed the amount of the possible loss. The difference between the cost of countermeasures and the amount of possible damage should be directly proportional to the likelihood of damage.

The vulnerability v magnitude is defined as the probability of inability of the protected item to resist actions of the threat sources, and if the force used from the threat source is stronger than the ability of the protected item to withstand it, then vulnerability v appears. In actual practice, it can arise through factors such as the likelihood of the threat and the level of protective measures. In this case, the vulnerability v magnitude can be determined using the following expression:

$$v = \frac{\sum_{i=1}^{n} P(U_i)}{Z} \quad (2)$$

where $P(U_i)$ – expected threat probability; $i = \overline{1,n}$; – number of expected threats; Z – strength of security $(0 < Z \leq 1)$.

While using this expression and calculating the binding of numerical values with qualitative properties can performed using the following table 2 [13].

Table 2 – Asset value, risk and vulnerability levels

The degree of probability of occurrence of threats		Low			Average			High		
Value of assets	0	0	1	2	1	2	3	2	3	4

The growth of riskiness with an increase in the vulnerability magnitude is determined and analyzed through an audit from a legislative point of view. As a result of the analysis, measures to prevent riskiness should be proposed.

Thereby, the methodology for assessing the quality of IT activity management in relation to business processes in a company is based on the abovementioned ITIL library, COBIT methodology and ISO 20000 standards according to service management through information technology. Its results affect the efficient management of information security using the abovementioned security models.

Н. Байшолан[1], К.Е. Кубаев[2], Т.С. Байшоланов[3]

[1,2,3] Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІҢ ҚАЗІРГІ ЖАБДЫҚТАРЫ

Аннотация. Қазіргі ұйымдардағы бизнес-үдерістердің тиімді жүргізілуі онда қолданылатын ақпараттық технология мүмкіндіктеріне тікелей тәуелді. Мақалада ақпараттық жүйе сапасын, қауіпсіздігін қамтамасыз етудегі аудит жабдықтарының орны мен ерекшеліктері және басқада да әдістемелік жабдықтар, модельдер сипатталып, талданған.

Қазіргі қолданыстағы COBIT (ақпаратты және оған қатысты технологияларды бақылау нысандары) әдістемесінің ақпараттық технология нарығындағы сұранысқа ие болатын ақпараттық аудит қызметіне тікелей қажетті құрал екендігі сипатталады.

COBIT стандартының принциптеріне шолу жасалып, сонымен қатар оның бизнес қажеттіліктерін қанағаттандырудағы маңыздылығы негізделеді. Компанияның желілік ортасындағы виртуалды құндылықтарды қорғау мақсатында оған ақпараттық қауіпсіздік модельдерін қолдану маңызы баяндалады. COBIT стандарты арқылы ақпараттық технологиялардағы тәуекелдерді басқару мен ақпараттық қауіпсіздік жүйесін басқару-дағы тәжірибелік ұсыныстар талданады.

Мекемедегі ақпараттық жүйені кездейсоқ немесе қасақана, жасанды қателіктен сақтау немесе қорғау шаралары қарастырылады. Ол үшін ақпаратты қабылдаушы немесе жеткізіп беруші сыртқы үдеріс талап-тарына сәйкес нақты ақпараттық қауіпсіздік модельдерінің бірін қолдануға болатыны баяндалады.

Сонымен қатар, шабуылдардың әдістері мен әдістерінің көбеюіне және олардың жаңа құралдары мен векторларының дамуына байланысты ақпараттық қауіпсіздікті жақсарту және қамтамасыз ету жолдары қарастырылады.

Қауіпсіздік аудитінің негізгі міндеттері қарастырылып, оны атқару кезеңдері баяндалады. Ақпараттық жүйелердегі қауіпсіздікке қатысты осалдық (увязимость) шамасының сандық мәнін табудың аналитикалық моделі ұсынылады.

Түйін сөздер: COBIT әдістемесі, ITIL кітапханасы, ISO 20000 стандарты, ақпараттық технология, ақпараттық аудит, ақпараттық қауіпсіздік, тәуекел, осалдық, COBIT ® 2019 Framework.

Н. Байшолан[1], К.Е. Кубаев[2], Т.С. Байшоланов[3]

[1,2,3] Казахский национальный университет имени аль-Фараби, Алматы, Казахстан

СОВРЕМЕННЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. Эффективное ведение бизнес-процессов в современных организациях напрямую зависит от возможностей применяемых в них информационных технологий. В статье описываются и анализируются роль и особенности средств аудита, а также прочих методических средств и моделей в обеспечении качества, безопасности информационных систем.

Современная действующая методика COBIT (Формы контроля информации и смежных технологий) описывается как средство, необходимое непосредственно для информационной службы аудита, которая завоюет спрос на рынке информационных технологий.

Проводится обзор принципов стандарта, а также значение удовлетворения его бизнес-потребностей. В целях защиты виртуальных ценностей в системной среде компании ей излагается о значении использования моделей информационной безопасности. Посредством стандарта COBIT осуществляется анализ практических предложений в управлении рисками и системой информационной безопасности в информационных технологиях.

Рассматриваются мероприятия по охране или защите информационной системы в учреждении от случайных или умышленных, мнимых угроз. Сообщается о возможности использования получателем или поставщиком информации одной из моделей реальной информационной безопасности в соответствии с требованиями внешних процессов.

Кроме того, в связи с увеличением количества методов и приемов атак и разработкой их новых средств и векторов рассматривается необходимость совершенствования и путей обеспечения информационной безопасности.

Рассматриваются основные задачи аудита безопасности и излагаются этапы выполнения этих задач. В отношении безопасности в информационных системах предлагается аналитическая модель определения числового значения меры уявзимости.

Ключевые слова: методология COBIT, библиотека ITIL, стандарты ISO 20000, информационные технологии, информационный аудит, информационная безопасность, риск, уязвимость, COBIT ® 2019 Framework.

Information about authors:

Baisholan N., PhD Student of the Al-Farabi Kazakh National University, baisholan@mail.ru, https://orcid.org/0000-0002-8134-0466;

Kubayev K.E., Dr. Sci. Economy, professor Al-Farabi Kazakh National University, kubaev.k@mail.ru, https://orcid.org/0000-0002-9083-4257;

Baisholanov T.S., master's degree student, Al-Farabi Kazakh National University, btstalgat@mail.ru, https://orcid.org/0000-0002-3413-0087

REFERENCES

[1] Podgornaya GN Information audit in the general system of AUDIT, 2015. Pp.30-41. http://edoc.bseu.by:8080/bitstream/edoc/30461/1/Podgornaya_G._N.._s._30_41.pdf (in Russ.).

[2] Sitnov, AA Audit of information systems: monograph. / A. A. Sitnov, A. I. Urintsov. M .: UNITY-DANA,

[3] 2014. 240 p. *ISBN*:978-5-238-02535-3 (in Russ.).

[4] A COBIT 5 Overview: [Electronic resource], 2020 // www.isaca.org. URL: http://www.isaca.org/Info/CertificationExams2014/CISA/CISA.html?cid=1005075&Appeal=SEM&gclid=CKuN8a25hb8CFUINcwo dZHgAaw.

[5] Martin Andenmatten. COBIT 2019 – DAS NEUE ENTERPRISE GOVERNANCE MODELL FÜR INFORMATIONEN UND TECHNOLOGIEN. https://blog.itil.org/2018/11/cobit-2019-das-neue-enterprise-governance-modell-fuer-informationen-und-technologien/

[6] Repin A.V. COBIT 5 and its Place in Enterprise Information Security // Science, technology and education, 2014. No1 (1). Pp. 52-57. https://cyberleninka.ru/article/n/standart-cobit-5-i-ego-mesto-v-informatsionnoy-bezopasnosti-predpriyatiya/viewer (in Russ.).

[7] ITIL and COBIT: Is It Worth Implementing? 2016. http://citforum.ru/consulting/articles/itil_cobit/ (in Russ.).

[8] Danby S. A Quick Overview of COBIT 2019, 2019. https://itsm.tools/a-quick-overview-of-cobit-2019/

[9] Cobit Mapping: Overview of International IT Guidance. 2nd edition. USA: IT Governance Institute, 2006. ISBN 1-933284-31-5

[10] Khanin P., Gamayunov D. General overview of vulnerability assessment systems (CVSS 2.0/3.0), 2018. https://safe-surf.ru/specialists/article/5211/596644/ (in Russ.).

[11] Andy Ju An Wang. Information security models and metrics ACM-SE 43: Proceedings of the 43rd annual Southeast regional conference. Vol.2, March 2005. P. 178–184. https://dl.acm.org/doi/10.1145/1167253.1167295

[12] Nosarev A. Models in information security, 2019. https://habr.com/ru/post/467269/ (in Russ.).

[13] Astakhov A. Information systems security audit, 2002. http://www.iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti/audit-bezopasnosti-informacionnyh-sistem (in Russ.).

[14] National standard of the Russian Federation GOST R ISO / IEC 27005-2010 "Information technology. Methods and means of ensuring security. Information security risk management" (approved by order of the Federal Agency for Technical Regulation and Metrology of November 30, 2010 N 632-st). https://dokipedia.ru/print/5173680