TECHNICAL SCIENCES

ANALYSIS OF INFORMATION SECURITY THREAT ASSESSMENT OF THE OBJECTS OF INFORMATION ACTIVITY

Yevseiev S.,
Doctor of Technical Science, professor
Simon Kuznets Kharkiv National University of Economics, Ukraine
Laptiev O.l.,
Doctor of Technical Science, Senior Researcher
Taras Shevchenko National University of Kyiv, Ukraine
Korol O.,
PhD, Associate Professor,
Simon Kuznets Kharkiv National University of Economics, Ukraine
Pohasii S.,
PhD, Associate Professor,
Simon Kuznets Kharkiv National University of Economics, Ukraine
Milevskyi S.,
PhD, Associate Professor
Simon Kuznets Kharkiv National University of Economics, Ukraine
Khmelevsky R.
Senior Lecturer, State University of Telecommunications, Kyiv, Ukraine

АНАЛІЗ ОЦІНКИ ЗАГРОЗ ІНФОРМАЦІЙНЇЙ БЕЗПЕКІ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Євсеєв С.П.,
Доктор технічних наук, професор, Харківський національний економічний університет ім. С. Кузнеця, Харків, Україна
Лаптєв О.А.,
Доктор технічних наук, старший науковий співробітник, Київський національний університет імені Тараса Шевченка, Київ, Україна
Король О.Г.,
Кандидат технічних наук, доцент,Харківський національний економічний університет ім. С. Кузнеця, Харків, Україна
Погасий С.С.,
Кандидат економічних наук, доцент, Харківський національний економічний університет ім. С. Кузнеця, Харків, Україна
Мілевський С.В.,
Кандидат економічних наук, доцент Харківський національний економічний університет ім. С. Кузнеця, Харків, Україна
Хмелевський Р.М.
Старший викладач, Державний університет телекомунікацій, Київ, Україна

Abstract

Due to the growing role of information technology in modern society, as well as the reality of the many threats to their security, the problem of information security requires increasing attention. The systemic nature of the impact on information security of a large set of different circumstances lead to the need for an integrated approach to solving this problem. In these conditions, the assessment of information security threats needs special attention as a necessary component of an integrated approach to information security of the organization. Therefore, the article is devoted to the analysis and assessment of the main threats to information security of information objects, as well as the principles of information security of the organization. The article summarizes the existing scientific approaches to determining the nature of threats and sources, vulnerabilities, classifications of possible threats and areas of information security of the organization.

Анотація

У зв'язку із зростаючою роллю інформаційних технологій у житті сучасного суспільства, а також через реальності численних загроз з точки зору їх захищеності проблема інформаційної безпеки вимагає до себе все більшої уваги. Системний характер впливу на інформаційну безпеку великої сукупності різних обставин призводять до необхідності комплексного підходу щодо вирішення даної проблеми. Особливої уваги в цих умовах потребує оцінка загроз інформаційної безпеки як необхідна складова комплексного підходу до забезпечення інформаційної безпеки організації. Тому стаття присвячена аналізу та оцінці основних загроз інформаційної безпеці об'єктів

інформаційної діяльності, а також засадам забезпечення інформаційної безпеки організації. В статті узагальнено існуючі наукові підходи до визначення сутності загроз та джерел, уразливостей, розглянуто класифікації можливих загроз та напрями забезпечення інформаційної безпеки організації.

Keywords: *threats, methods, tools, information security, threat assessment.*
Ключові слова: *загрози, методи, засоби, інформаційна безпека, оцінка загроз.*

Вступ. У сучасному суспільства різко зросла роль інформаційної складової у забезпечені безпеки підприємств та держави у цілому. З підвищенням значності та цінності інформації відповідно зростає і важливість її захисту. Крім того, інформація коштує грошей. Значить витік або втрата інформації спричинить матеріальний збиток. Тому захист інформації є актуальним науковим завданням.

Суспільна трансформація та загальна нестійкість, заплановані біфуркації та неочікувані переміни сторіччями несуть з собою превентивну функцію підготовки до зустрічі з несподівано складними емерджентними проблемами, ставлячи у тому числі задачі пошуку нових підходів до оцінки загроз інформаційної безпеки (ІБ) об'єктам інформаційної діяльності (ОІД). В умовах бурхливого розвитку інформаційних технологій (ІТ), коли вони стали основою для формування глобального інформаційного суспільства, у свою чергу ІБ стає життєво необхідною умовою забезпечення інтересів людини, суспільства та держави і найважливішою ланкою всієї системи національної безпеки країни.

Постановка проблеми. Стан інформаційної безпеки істотно залежить від загроз, прояв яких може завдати непоправної шкоди як державному так і комерційному секторам національної економіки. Саме тому дослідження основних загроз та засад щодо оцінки інформаційної безпеки обїектів інформаційної діяльності для побудови ефективних систем захисту інформації є актуальним.

Аналіз публікацій. Інформаційная безпека набула обрису нового державно-громадського інституту, становленню якого, як і в інших країнах світу, притаманна низка проблем. Так наприклад, у взятому Україною курсі на входження у європейський простір (підкріплений Указом Президента України Про Стратегію кібербезпеки України від 27 січня 2016 року [2]) акцентується увага на посиленні значення та ролі ІБ, як складової національної безпеки України. Одним із пріоритетів забезпечення ІБ визначено при цьому створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них. Дослідженню цих питань присвячено роботи: В.Л. Бурячка, Ю.В. Богдановича, П.О. Балашова, С.В. Кавуна, С.В. Казмірчук, О.Г. Корченко, О.А.Лаптєва, В.О. Хорошко тощо. Використання різних методик з метою оцінювання захисту інформації в організаціях розглядали у своїх роботах: В.В. Бут, О.В. Гребенюк, В.В. Домарєв, М.О. Живко, І.Р. Конєв, В.В. Микитенко, А.А. Садердинов, О. А. Сороківська, М. Ю. Танцюра, В. С. Цимбалюк.

Метою статі є аналіз сучасних вітчизняних та зарубіжних підходів у визначенні оцінки основних загроз щодо об'єктів інформаційної діяльності.

Викладення основного матеріалу

Інформаційна безпека – це, як відомо [3], «стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання і розвиток в інтересах громадян, організацій». Основу ІБ становлять політика ІБ, законодавча, нормативно-правова та наукова база ІБ, структура органів, які здійснюють захист інформації, а також методи, способи і засоби, які вони для цього застосовують. Напрями ІБ та етапи її формування подано на рис.1. Зважаючи, що заходи забезпечення ІБ в організації спрямовуються головним чином на те, щоб не допустити збитків від втрати інформації, правомірно перш за все сконцентрувати увагу на визначенні загроз – сукупності умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства та держави в цілому в інформаційній сфері. Передумовою появи загроз ІБ є як об'єктивні (недосконаліть засобів захисту), так і суб'єктивні фактори (промислове шпигунство, карні елементи, несумлінні співробітники тощо).

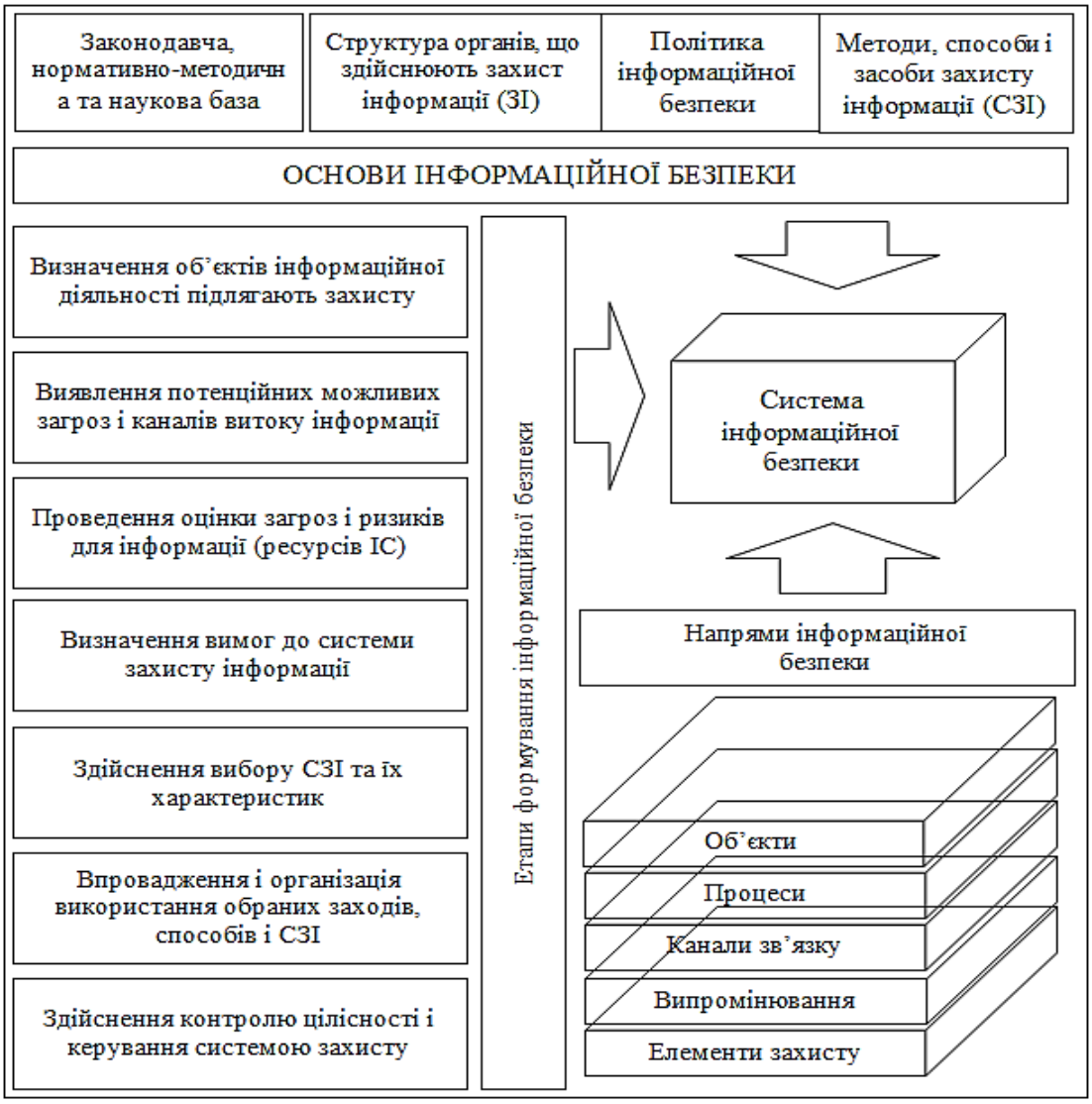

Рис. 1. Основи, етапи та напрями формування ІБ

Природа походження загроз ІБ може бути при цьому випадковою (збої, помилки, побічні впливи тощо), або навмисною (злочинні дії соціуму), табл.1.

Таблиця 1.

Типи загроз інформаційній безпеці в інформаційних системах

ТИП ЗАГРОЗИ		Причини або спонукальні мотиви
Навмисні загрози	**Ненавмисні загрози**	
Розкрадання носіїв інформації	–	Прагнення використовувати конфіденційну інформацію (КІ) у своїх цілях
Застосування програмних пасток	–	
–	Несправність апаратури, що може ініціювати несанкціоноване зчитування ІР	Недостатня кваліфікація обслуговуючого персоналу, застосування несертифікованих технічних засобів
Використання програм «троянський кінь»	–	Завдання збитків шляхом НСД в інформаційну систему (ІС)
Помилки в програмах обробки інформації	–	Завдання збитків шляхом внесення програмних закладок у процесі розробки програмних систем
Впровадження комп'ютерного вірусу	–	Руйнування ІС з метою завдання збитків
–	Помилки в програмах обробки інформації	Застосування несертифікованого програмного продукту
–	–	Недотримання персоналом вимог ІБ, порушення технологічної послідовності роботи з ІС
Помилкова комутація в мережі ЕОМ	–	З метою створення каналу для витоку КІ
–	Помилкова комутація в мережі ЕОМ	НКВ обслуговуючого персоналу
–	Паразитне електромагнітне випромінювання (ЕМВ)	Недостатнє урахування вимог безпеки на етапі проектування ІС або її створення
–	Перехресні наведення за рахунок ЕМВ	
Примусове ЕМВ	–	Вивід з ладу ІС з метою завдання збитків
Використання акустичних випромінювань	–	Одержання конфіденційної інформації
Копіювання за допомогою візуального і слухового контролю	–	
Маскування під користувача, підбор паролю	–	Несанкціоноване втручання в роботу системи в злочинних цілях
–	Помилка в роботи оператора	Недостатня кваліфікація, застосування несертифікованого ПЗ
–	Помилки користувача	Використання недостатнього захисту
Помилки програміста: опис, перекручування програмного захисту, розкриття кодів, паролів	–	З метою добування особистої вигоди або завдання збитків
Помилки технічного персоналу: опис і перекручування схем захисту, помилкова комутація	–	–
–	Помилки персоналу: перекручування схем захисту, помилкова комутація	Недостатня кваліфікація обслуговуючого персоналу, порушення технології

Засобами реалізації загроз як правило є: шкідливе та потенційно небезпечне ПЗ (computer virus; worm; trojan horse; rootkit; spyware тощо), Internet-шахрайство (phishing, carding, pharming, sms phishing тощо), несанкціонований доступ (НСД) до ІР та ІС (hacking, deface), DoS та DDoS-атаки тощо. За наслідками своєї дії загрози ІБ спрямовані на порушення *конфіденційності, цілісності та доступності до інформації* (рис.2). Оцінку можливих актуальних загроз ІБ в організації доцільно починати з аналізу джерел загроз, обумовлених різними факторами.

Рис. 2. Ознаки загроз конфіденційності, цілісності та доступності інформації

Джерелами загроз можуть виступати: *людина, технічні пристрої, моделі, алгоритми, програми; технологічні схеми обробки; зовнішнє середовище.* Прикладом цьому можуть слугувати статистичні дані, оприлюднені аналітичним центром компанії InfoWatch. Фахівці компанії стверджують, що останнім часом більше половини інцидентів, зафіксованих в компаніях, а саме біля 65,4%, пов'язані з внутрішніми порушниками. При цьому витік інформації відбувається з їх вини або по необережності. Причиною більше 32% витоку інформації на ОІД стають зовнішні зловмисники. У 51,2% випадків винуватцями витоків інформації були нинішні та колишні робітники – 48,9% і 2,3% відповідно. Тобто, як видно, нині саме людський фактор є одним з основних чинників ризику з точки зору ІБ організації. Наступний крок має полягати в проведенні аналізу факторів, які можуть вплинути на реалізацію певної загрози та визначенні низки актуальних загроз (рис.3).

Рис. 3. Загальний порядок визначення актуальних загроз

Одним із найважливіших етапів цього процесу є проведення якісно-кількісної оцінки можливості реалізації кожної загрози. Більшість відомих підходів до оцінювання ймовірності реалізації загрози ґрунтуються на *апостеріорних*, *апріорних* та *експертних* методах (рис.4).

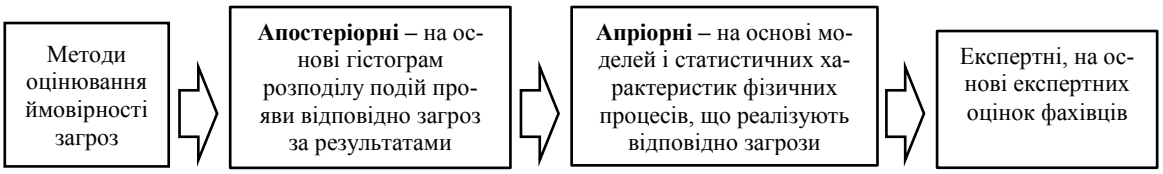

Рис. 4. Методи визначення ймовірності реалізації загроз

Зробимо припущення, ймовірність реалізації кожної *i*-ої загрози по відношенню до *j*-го активу визначатимемо, використовуючи рівняння (1):

$$d_{rj} = 1 - p_{ri} \times \prod_{i=1}^{m}(1 - p_{rji}), \qquad (1)$$

де *n* – кількість загроз;
m – кількість активів;
p_{ri} – можливість здійснення *i*-ої загрози;
d_{rj} – можливість реалізації хоча б однієї загрози *j*-му активу.

При цьому: $p_{ri} = p_{ti} \times p_{vi}$

де p_{ti} – можливість появи *i*-ої загрози;
p_{vi} – можливість появи уразливості щодо реалізації *i*-ої загрози.

Наступним етапом буде обчислювання ціни ризику *Rj* для кожного *j*-го активу:

$$R_j = d_{rj} \times p_j, \qquad (2)$$

Ціна повного ризику дорівнює сумі цін ризику для всіх активів за формулою:

$$R_{\text{ПОВН}} = \sum_{j=1}^{n} R_j, \quad (3)$$

При визначенні коефіцієнта нейтралізації загроз вибирається система захисту інформації (СЗІ). При вирішенні щодо доцільності використання прийнятої СЗІ організації, наприклад, якщо 0,8 ≤ КНЗ – СЗІ рекомендується використовувати як основну [10].

Відповідно до іншого підходу, сценарії реалізації загроз об'єкту захисту можуть бути представлені байесовськими мережами довіри (БСД) [11]:

$$BN_{O3} = \langle A, Tab_{O3} \rangle, \quad (4)$$

де $A = \{a_i\}_{i=1}^{N_A}$ множина дій порушників;

N_A – кількість всіх дій порушників;

Tab_{O3} – множина таблиць ймовірностей кожного з дій a_i з «батьківськими» діями *parents*(a_i).

Такий підхід дозволяє з більшою точністю визначати ймовірність реалізації. Вузлами БСД в цьому випадку будуть атакуючі дії порушників. Таблиці умовних ймовірностей описуються наступним чином:

$$Tab_{O3} = \{P(A_1 | parents(A_1)), ..., P(A_n | parents(A_n))\}, \quad (5)$$

З дії A_i порушник починає реалізацію загрози. Використовується безумовна ймовірність $P(A_i)$. Компонент моделі загроз об'єкта захисту, що представляє дії порушника, в загальному вигляді включає в себе: $A = \{a_i\}_{i=1}^{N_A}$ – множина дій порушників, N_A – число всіх дій порушників; $F^{УДН}$ – множина функцій даного компонента.

Дії порушника представляємо таким чином:

$$a_i = \langle aid_i, pur_i, T_{ra}, Y_{\text{maxi}}, P_i^{Б}, RE_i \rangle \forall i \in N_A, i \le N_A, \quad (6)$$

де aid_i – ідентифікатор дії порушника;

$pur_i \in Pur$ – мета реалізації дії порушника;

T_{ra} – час для успішної реалізації дії;

Y_{maxi} – ймовірний збиток системі;

$P_i^{Б}$ – ймовірність виконання порушником даної дії;

$RE_i = \{re_i\}_{i=1}^{N_{re}}$ –рекомендації щодо виявлення, затримки і реагування СЗІ;

Nre – число рекомендацій відомих системі.

Імовірність реалізації загрози (Р (В)) обчислюється за формулою повної ймовірності події. Це дає більш точні значення показників ймовірності реалізації загрози за певним сценарієм. Сумарний збиток (Y) від реалізації сценарію визначається як сума збитків всіх дій з даного сценарію. Тоді, з урахуванням виразу $R = YP$, ризик від [11]:

$$R = YP(B), \quad (7)$$

Відносна оцінка втрат у разі реалізації *i*-ої загрози – d_i. Для кожної загрози визначається рівень значимості, що дорівнює добутку можливості реалізації на відносну оцінку утрат:

$$z_i = p_{ri} \times d_i, \quad (8)$$

де z_i – рівень значущості загрози.

Висновки. У зв'язку із зростаючою роллю інформаційних технологій у житті сучасного суспільства, а також через реальності численних загроз з точки зору їх захищеності проблема ІБ вимагає до себе все більшої уваги. Системний характер впливу на ІБ великої сукупності різних обставин призводять до необхідності комплексного підходу щодо вирішення даної проблеми. Особливої уваги в цих умовах потребує оцінка загроз ІБ як необхідна складова комплексного підходу до забезпечення інформаційної безпеки організації.

Зважаючи на те, що прояв загроз ІБ може завдати шкоди будь-яким державним або комерційним структурам. Дослідження загроз ІБ організації доцільно проводити за напрямами, які складаються з трьох блоків: *дії до атаки, під час атаки так і після неї*. При цьому головну увагу слід зосереджувати як на повному переліку загроз, так і передусім на множині актуальних внутрішніх та навмисних загрозах ОІД. Оперування низкою притаманних загрозам параметрів дасть можливість визначити ймовірність реалізації кожної загрози, отримати повне уявлення про варіанти її деструктивного впливу та їх наслідки.

СПИСОК ЛІТЕРАТУРИ:

1. Хмелевський Р.М. Тези. «Інформаційна безпека, як одна з основ забезпечення ефективності роботи державного управління». Матеріали міжнародної науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології» Том IV «Сучасні технології інформаційної безпеки» Київ, ДУТ. 17–20 листопада 2015 р. С.155–158.

2. Касперский Е. Основные классы угроз в компьютерном сообществе 2003 года, их причины и способы устранения.Информационный бюллетень «Jet Info». № 12 (127)/2003.

3. Классификация угроз Digital Security (Digital Security Classification of Threats). – [Електронный ресурс]. – Режим доступа: http://www.dsec.ru/products/grif/fulldesc/classification

4. Кузнецов И.Н. Учебник по информационно-аналитической работе. Информация: сбор, защита, анализ. М.: Изд. Яуза, 2001.

5. Christopher Alberts, Audrey Dorofee «OCTAVE Threat Profiles»; Software Engineering Institute, Carnegie Mellon University.

6. Нурдинов Р.А., Батова Т.Н. Подходы и методы обоснования целесообразности выбора средств защиты информации. Современные проблемы науки и образования. – 2013. – № 2.

7. В.И. Аверченков, М.Ю. Рытов, О.М. Голембиовская . Автоматизация проектирования комплексных систем защиты информации: монография.Брянск: БГТУ, 2012. 139 с.

8. Malik Shahzad Awan, Peter Burnap, and Omer F. Rana. Estimating risk boundaries for persistent and stealthy cyber-attacks. In Proceedings of the 2015 Workshop on Automated Decision Making for Active Cyber Defense, SafeConfig '15, pp. 15–20, New York, NY, USA, 2015. ACM.

9. Ross Brewer. Advanced persistent threats: minimising the damage. Network Security, 2014(4):5–9, 2014.

10. David Miller, Shon Harris, Allen Harper, Stephen VanDyke, and Chris Blask. Security information and event management (SIEM) implementation. McGraw Hill Professional, 2010.

11. Kyle Wilhoit. Who's really attacking your ics equipment? Trend Micro, 2013.

12. Khmelevskoy R.N. "Investigation of the assessment of threats to the information security of information activity objects" . Modern information protection 2016.. No. 4. .pp 65–71.

13. Хорошко В.О., Хохлачова Ю.Є. Інформаційна війна. ЗМІ як інструмент інформаційного впливу на суспільство. Т. 22. Частина 1: Безпека інформації. 2016.DOI: 10.18372/2225-5036.22.11104

14. Лаптєв О.А. Методика визначення ймовірності негласного отримання інформації потенційним порушником. Science and Education a New Dimension. Natural and Technical Sciences. Budapest, Hungary, VII(24), Issue: 200, 2019. ISSN 2308-5258, С.27 – 31.

15. S. Toliupa, N. Lukova-Chuiko, O. Oksiuk. "Choice of Reasonable Variant of Signal and Code Constructions for Multirays Radio Channels", Second International Scientific-Practical Conference Problems of Infocommunications. Science and Technology. IEEE PIC S&T 2015. pp. 269 – 271.

APPLICATION OF CLOUD COMPUTING IN MEASURING INFORMATION AND CONTROL COMPLEXES OF AN AUTOMATIC OPERATIONAL MANAGEMENT SYSTEM

Temerbekova B.,
Doctor of Philosophy (PhD) in Technical Sciences,
Head of the Department "Automation of Technological Processes and Production" of the National Research Technological University "MISIS" in Almalyk, Republic of Uzbekistan
Mamanazarov U.
Assistant of the Department "Automation of technological processes and productions" of the National Research Technological University "MISIS" in Almalyk, Republic of Uzbekistan

ПРИМЕНЕНИЕ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ В ИЗМЕРИТЕЛЬНЫХ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ КОМПЛЕКСАХ АВТОМАТИЧЕСКОЙ СИСТЕМЫ ОПЕРАТИВНОГО УПРАВЛЕНИЯ

Темербекова Б.М.,
доктор философии (PhD) по техническим наукам,
заведующий кафедрой «Автоматизация технологических процессов и производств» Национального исследовательского технологического университета «МИСиС» в г. Алмалык, Республика Узбекистан
Маманазаров У.Б.
ассистент кафедры «Автоматизация технологических процессов и производств Национального исследовательского технологического университета «МИСиС» в г. Алмалык, Республика Узбекистан

Abstract

This article presents the applications of cloud computing in measuring information and control systems of the technological process. Various users of computing levels, a utility model of service provision, approaches to the development of a web service computing architecture, a platform in technological processes for the development of various algorithms for measuring and information control systems are presented. The role of the API for defining functions or methods that is used in the development of cloud computing, and ways to establish communication between two software systems over a unified network with an automatic operational dispatch control system are given. The tasks of measuring measurement information in industrial areas and setting the measured technical and economic indicators of production in the cloud have been solved. The application of the advantages of cloud computing in complex technological processes of enterprise management is justified.

Аннотация

*В данной статье приведены применения облачных вычислений в измерительных информационно-управляющих системах технологического процесса. Приведены различные пользователи вычислительных уровней, **п**олезная модель предоставления услуг**,** подходы развития веб-сервиса вычисляющую архитектуру, платформу в технологических процессах для разработки разных алгоритмов при измерительно-информационно управляющих системах**.** Дано роль API определения функций или методов, который используется при разработки облачных вычислений, и способы установки связи между двумя системами программного обеспечения по объединенной сети при автоматической системы оперативного диспетчерского управления. Решены задачи по измерению измерительной информации в промышленных сферах и выставление измеренных технико-экономических показателей производства в облаке. Обоснован применения преимущества облачных вычислений, в сложных технологических процессах управления предприятием.*