International scientific conference

"Innovative technologies, models

Cyber Security Management, ITCSM-2023

ANNUAL SCIENTIFIC CONFERENCE

ITCSM-2023

Part 1

Aprilr 18-20, 2023

Kyiv Ukraine
Book of Abstracts

«ІННОВАЦІЙНІ ТЕХНОЛОГІЇ, МОДЕЛІ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ІТМК-2023»

Міжнародна наукова конференція

Дніпро 2023

«ІННОВАЦІЙНІ ТЕХНОЛОГІЇ, МОДЕЛІ УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ІТМК-2023»

Міжнародна наукова конференція

Голова: Стеблянко П.О.

ПРОГРАМНИЙ КОМІТЕТ ITCSM-2023

Бабешко М.О. Богданов В.Л., Бочаров Д.О., Волосова Н.М., Галішин О.З., Гачкевич О.Р., Григоренко О.Я., Гудрамович В.С., Дзюба А.П., Дьомічев К.Е., Корнєєв М.В., Крилова Т.В., Круковский О.П., Кушнир Р.М., Лобода В.В., Назаренко В.М., Пилипенко О.В., Пошивалов В.П., Приймаченко Д.В., Савченко В.Г., Сохацький А.В., Стрельнікова О.О., Тимошенко В.І., Черняков Ю.А.(США), Ченцов В.В., N. Choudhary (Індія)

З 2020 року в *Університеті митної справи та фінансів* проводиться Міжнародна науково-практична конференція «Інноваційні технології, моделі управління кібербезпекою ІТМК». В роботі конференції приймали участь представники США, Польщі, Індії, Лівії.

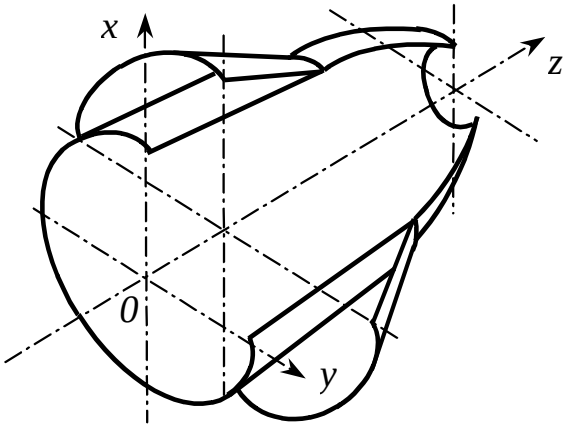
Співорганізатором конференції є *Інститут механіки ім. С.П.Тимошенка НАН України.*

У цій частині збірки матеріалів Міжнародної IV наукової конференції «Інноваційні технології, моделі управління кібербезпекою ІТМК-2023» (том 1) зібрано матеріали доповідей фахівців з технічних, фізико-математичних, соціальних та освітніх наук.

Публікація другої частини матеріалів конференції планується на листопад 2023 року.

СЕКЦІЯ

МАТЕМАТИЧНІ ПРОБЛЕМИ ТЕХНІЧНОЇ МЕХАНІКИ 2023



ON THE APPLICATION OF THE SHELL THEORY IN RESEARCH OF NON-ISOTHERMAL CREEP OF HOLLOW CYLINDERS

[1] O.Galishin, [2] S.Sklepus
[1]S.P. Timoshenko Institute of Mechanics, NASU
[2]A.N. Podgorny Institute for Mechanical Engineering Problems, NASU

In the present work the spatial problem of definition of the axisymmetric stress-strain state of non-uniform heated hollow cylinder under creep conditions is considered. The research are performed in the assumption that elastic characteristics of material, the coefficient of linear temperature expansion and all parameters of creep in the constitutive equations depend on temperature. The creep problem for a hollow non-uniform heated cylinder under internal pressure was solved. The numerical results generated by the proposed spatial model have been compared for this example with analogous results based on the first-order shear deformation theory (FSDT) of shells. The comparison showed that FSDT provides a satisfactory coincidence with the spatial solution.

MATHEMATICAL MODELING OF DEFORMATION PROCESSES IN THE BOUNDARY PROBLEMS OF THERMOVISCOPLASTICITY TAKING INTO ACCOUNT THE STRESS MODE AND DAMAGE TO THE MATERIAL STRUCTURE

M.O.Babeshko, V.G.Savchenko
S.P.Timoshenko Institute of Mechanics, NASU

The inelastic stress-deformed state of layered bodies of rotation made of isotropic materials in the processes of thermo-force loading is investigated. The constitutive equations are presented in the form of a generalized Hooke's law with additional terms that take into account the damage to the material structure due to creep and loosening, the dependence of deformation diagrams on temperature and the stress mode. Linearization of the nonlinear problem of thermoviscoplasticity is carried out by the method of successive approximations. Representation of given loads and unknown functions in the form of trigonometric series in

the circular direction is used. For spatial bodies of rotation, the variational Lagrange equation and the finite element method are used. The spatial problem is reduced to the solution in each approximation at each loading stage of systems of algebraic equations, the coefficients and right-hand sides of which are determined by the results of the previous approximation. For thin shells of rotation, the problem is reduced to the solution in each approximation of each load stage of the system of ordinary differential equations, the coefficients and free terms of which are calculated based on the results of the previous approximation. The numerical results are given.

NONLINEAR MODEL OF THE BEHAVIOR OF PSEUDO-ELASTIC-PLASTIC ALLOYS

[1] P.O.Steblyanko, [2] O.Petrov, [2]Yu. Chernyakov
[1]S.P. Timoshenko Institute of Mechanics, NASU
[2] Oles Honchar Dnipro National University

The report formulated a nonlinear model for describing the properties of alloys at a certain point. The deformation at a point is represented as the sum of the elastic component, the jump of deformation during the phase transition, the plastic deformation that obeys the flow theory with kinematic-isotropic strengthening, and the deformation caused by temperature changes. It is assumed that the properties of the material depend on the temperature. The results of calculations of the tangent modulus of the integral diagram of the alloy at each time integration step are given.

COMPUTER SIMULATION OF THE STRESS-STRAIN STATE OF THIN-WALLED CYLINDRICAL AND CONICAL SHELLS WITH HOLES AND INCLUDES

E.L.Hart, A.A.Semencha
Oles Honchar Dnipro National University

On the basis of computer simulation using the finite element method, the influence of mechanical and geometric parameters of inclusions on the stress concentration around holes in thin-walled cylindrical and truncated conical shells with circular holes in the presence of band inclusions from another material around them is studied.A comparative analysis of the results with the results for cases of shells withoutinclusions has been carried out. Rational parameters of band inclusions have been established to reduce the stress concentration factor. The mechanical effect associated with the displacement of the stress concentration zone at certain parameters of the inclusions is revealed.

ЧИСЛОВЕ МОДЕЛЮВАННЯ ДИНАМІКИ СКЛАДНИХ СИСТЕМ З ЗАСТОСУВАННЯМ КОМПЮТЕРНИХ ТЕХНОЛОГІЙ

А.В. Сохацький
Університет митної справи та фінансів, Україна

Необхідність швидкого розв’язування задач в різноманітних сферах спричинило широке використання комп’ютерної техніки. Вирішення проблем удосконалення та створення нових типів різноманітних технічних, в тім числі і транспортних апаратів в

короткі терміни пов'язують з удосконаленням комп'ютерних технологій. Оптимізація технічних характеристик, параметрів стійкості та керованості потребують використання не тільки досконалих математичних моделей, але й високопродуктивної обчислювальної техніки. Математичні моделі, алгоритми, комплекси програм, електронно-обчислювальні машини (ЕОМ) та системи їх підтримки є важливими елементами комп'ютерних технологій. Сукупність вказаних елементів створює технологічний ланцюг комп'ютерного моделювання: математична модель - чисельні алгоритми – програмування – ЕОМ – розрахунки - аналіз результатів - прийняття рішення. Значна потреба в високопродуктивних комп'ютерних технологіях зумовлена такими чинниками, як: складність досліджуваних задач, дорожнеча експериментального обладнання, зростання цін на енергоресурси, необхідність скорочення термів досліджень, успіхи розвитку ЕОМ, потреби в автоматизованих систем управління на виробництві та різноманітних галузях людської діяльності.

Проблеми розробки комп'ютерних технологій. Розробка та створення ефективних комп'ютерних технологій пов'язана з рівнем підготовки фахівців та потребами суспільства (рис.1). З розповсюдженням комп'ютерної техніки з'явились і виникла потреба в програмних комплексах для розв'язування прикладних задач.

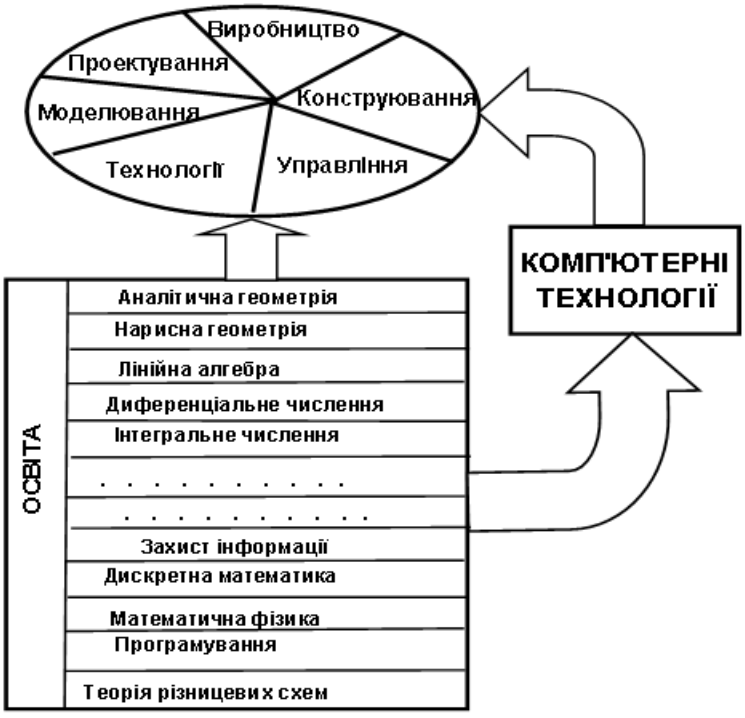


Рис. 1. Взаємозв'язок освіти, комп'ютерних технологій та потреб суспільства

Сучасні комп'ютерні технологій можна класифікувати наступним чином:

1. Початковий рівень (MsWord, Ms Exel, PaverPoint, CorelDraw та ін.).
2. Загальноматематичні пакети (MathCad, Maple,MatLab та ін.).
3. Пакети проектування та обробки даних (AutoCad, SolidWorks, CyrveExpert, DataFit, Statgraphics, SPSS та ін.).
4. Комплекси програм для моделювання технологічних процесів та оптимізації (MathConnecs, Simulink, Lindo LolverSuite та ін.).
5. Комплекси та пакети програм для моделювання складних фізичних процесів (Dynamik Adams, CFX, Ansys, FlowVision, STAR-CD, Fluent та ін.)

Для використання комп'ютерних технологій початкового рівня достатньо середньої освіти. Застосування більш складних комп'ютерних технологій вимагає більш високого рівня освіти з фізико-технічного та математичного напрямку. Особливо складним

рівнем комп'ютерних технологій є моделювання складних фізичних процесів. Ці комплекси програм будуються на числових методах розв'язування рівнянь математичної фізики. Нелінійність цих рівнянь та наявність малих параметрів при старших похідних створюють серйозні труднощі їх розв'язування. Чисельне моделювання таких процесів характеризується використанням великої кількості параметрів, різних типів рівнянь, областей задання змінних, межових та початкових умов, методів розв'язування рівнянь і т.д. Одночасний вибір того чи іншого методу розв'язку при заданих та початкових умовах впливає на побудову обчислювального алгоритму, структура якого визначається множиною мінливих значень "схемних" факторів: типом розрахункових сіток, порядком апроксимації рівнянь при переході від модельної форми до алгебраїчної, способами інтерполяції при розробці різницевих схем, методами розв'язку одержаних алгебраїчних рівнянь та інше. Вказані особливості задач та "схемних" факторів в різних роботах здійснюються на різних рівнях точності та складності. Окрім математичних проблем розв'язування дискретних аналогів диференціальних рівнянь необхідно побудувати адекватну реальному процесу фізичну модель. Для прикладу на рис.2 представлено схему моделювання зв'язаної задачі аеродинаміки та динаміки транспортного апарата. Зі схеми видно, що розробка комплексу програм складається з цілого ряду процесів.

Таким чином проблема розробки комп'ютерних технологій на основі числового розв'язування рівнянь математичної фізики з придатною точністю, особливо в тривимірних випадках, на сьогодні залишається вельми актуальною. Необхідність розв'язування складних задач вимагає розробки математичних моделей різного рівня складності, які б описували закономірності досліджуваних явищ з потрібною точністю. Динаміка зростання продуктивності ЕОМ говорить про те, що необхідні якісно нові математичні моделі, які б дозволяли не просто моделювати явище, а виступали б експертною системою для прийняття рішення. Так, наприклад, для проведення досліджень властивостей води в малорозмірних системах в Аргонській Національній Лабораторії (США) використовується суперкомп'ютер продуктивністю – 557 трильйонів операцій в секунду (терафлопс).

Запропоновано класифікацію комп'ютерних технологій за рівнем складності. Розроблено методики, алгоритми та програмне забезпечення моделювання аеродинаміки транспортних апаратів з використання осереднених за Рейнольдсом рівнянь Нав'є-Стокса. Виконано тестування алгоритмів та програм. В подальших дослідженнях необхідно удосконалювати методики, алгоритми та програмний комплекс з урахування особливостей фізичних процесів та властивостей середовища.

NUMERICAL ANALYSIS OF THE BEHAVIOR OF PLATE-SHELL STRUCTURAL ELEMENTS WITH CIRCULAR HOLES THE PRESENCE OF RADIAL INHOMOGENEOUS INCLUSIONS

E. L. Hart, B. I. Terokhin
Oles Honchar Dnipro National University

As a result of the numerical study of the behavior of thin plates and cylindrical shells with a circular hole and an annular inclusion made of a functionally graded material (FGM), the effect of the modulus of elasticity of the FGM inclusion on the stress concentration factor in the plate and shell is analyzed. Rational parameters of a radially inhomogeneous FGM inclusion are established, at which the stress concentration coefficient decreases by almost 50%. The corresponding deformations also decrease proportionally.

In the presence of FGM inclusions with certain mechanical properties and geometric parameters, it becomes possible to influence not only the magnitude of the stress

concentration factor in the plate-shell structural elements near local stress concentrators, but also the stress distribution over the surface.

SIMULATION OF THE STRESSED STATE OF GAS-BEARING SANDSTONES WITHIN THE ZONE OF LONGWALL INFLUENCE

O.P. Krukovskyi, V.V. Krukovska, A.O. Kostrytsia
M.S. Poliakov Institute of Geotechnical Mechanics of the National Academy of Sciences of Ukraine

The results of stress field calculations were compared in two cases: deformation of gas-bearing rock without taking into account the gas component and with the influence of gas pressure. It is shown that taking into account the participation of the methane filtration process in the unloading of gas-bearing sandstone leads to a decrease of parameter P^* values. That is, gas pressure drop within the filtration area, degassing of gas-bearing rocks cause their more significant unloading. The calculation error reaches 80% in the case when the gas component of the deformation process is neglected. Thus, while calculating the stress state of gas-bearing rocks at great depths, it is necessary to consider the coupled processes of their deformation and filtration of the gas contained in the fracture-pore space.

НАПРУЖЕНО-ДЕФОРМОВАНИЙ СТАН ПРУЖНОЇ ОСНОВИ ІЗ ЗАХИСНИМ ПОКРИТТЯМ ТА ПОЧАТКОВИМИ НАПРУЖЕННЯМИ ПРИ ДІЇ РУХОМОГО НАВАНТАЖЕННЯ

Ю. П. Глухов
Інститут механіки імені С.П. Тимошенка НАН України

Дане дослідження спрямовано на вивчення закономірностей хвильових процесів в шаруватих пружних тілах при врахуванні ряду ускладнюючих факторів: різних моделей шаруватого покриття, початкових напружень, різних швидкостей руху поверхневого навантаження. Розв'язок вказаних задач передбачає встановлення закономірностей впливу початкових напружень, швидкості руху навантаження, геометричних та механічних характеристик покриття на напружено-деформований стан пружної основи. Актуальність результатів дослідження пов'язана з можливістю їх використання при розв'язанні актуальних проблем геофізики, нафторозвідки, проектуванні залізничних магістралей, придорожніх споруд, магістрального трубопровідного транспорту. Метою роботи є постановка динамічних задач для різних моделей попередньо напруженої шаруватої основи, розробка методів, побудова алгоритмів та створення програмного забезпечення для розв'язання задач даного класу.
В даній роботі розглядається попередньо напружений півпростір з неоднорідністю у вигляді тонкого поверхневого шару. Граничні поверхні плоскі і паралельні між собою. Матеріал півпростору – ізотропний в ненапруженому стані. Початковий напружено-деформований стан півпростору вважається однорідним. Зосереджена сила інтенсивності P рухається по вільній поверхні захисного шару на протязі великого проміжка часу. Передбачається, що картина деформацій інваріантна відносно часу в системі координат, що рухається разом з навантаженням.Також передбачається, що напруження, що виникає за рахунок дії навантаження, значно менше за початкові напруження. Вказане припущення дозволяє застосовувати лінеаризовану теорію пружності [1] для опису додаткового напруженного стану, викликаного дією навантаження. Шар товщиною h моделюється зосередженими масами з густиною ρ_1.

Таким чином, нормальна і дотична складові навантаження будуть $(P\sin\alpha+\varrho_1 hii_1)\delta(y_1)$ і $(P\cos\alpha+\varrho_1 hii_2)\delta(y_1)$. Тут u_1, u_2 - переміщення точок півпростору. Розв'язок задачі отримано за допомогою інтегрального перетворення Фур'є по змінній y_1. Розв'язок представлений в загальному вигляді для випадків нерівних і рівних коренів характеристичних рівнянь, для різних матеріалів елементів багатошарового середовища, умов їх сполучення і для будь-якої швидкості руху поверхневого навантаження.

1. Гузь А.Н. Упругие волны в телах с начальными (остаточными) напряжениями. – Киев: "А.С.К", 2004. – 672 с.

SEQUETIAL APPROXIMATION METHOD USING FOR NUMERICAL METHOD RESULT INTERPRETATION OF GEOMECHANICAL TASKS

O.P.Krukovskyi, G.I.Larionov, V.O.Hvorostyan, S.A.Golovko, U.V.Zemlyana
M.S. Poliakov Institute of Geotechnical Mechanics of the National Academy of Sciences of Ukraine

In the case of using numerical methods to obtain mathematical model (MM), the approximation procedure cannot avoid. A special place in the processes of mathematical modeling belongs to a wide class of methods based on variation methods - the finite element method (FEM). A well-designed interface contributes to its widespread use in various areas of technical applications. As a rule, obtaining many two-dimensional drawings and graphs satisfies the interest of most researchers. However, the analytical expression of the sought functions is not given. The classical approximation procedure solves this problem. However, the procedure leads to a large expenditure of computer time, which sometimes makes it impossible to obtain it. In the work, instead of obtaining an approximation on the mesh of parameters, a simplified procedure for it obtaining is used. The sequential approximation method (SAM) consists in finding a solution in multiplicative form, where the product functions are one-dimensional representations of the intersections of the function space by the corresponding planes.

The results of the comparison of the surfaces of the shear stress intensity function obtained by the FEM method and the interpolation surfaces of the numerical results of the stress-strain state solution determining near the circular cross-section open in a rock mass presented. Conclusions about the satisfactory accuracy of the obtained results of using the SAM method made.

ABOUT ONE MODEL OF PROTECTIVE COVERING FOR HALF-SPACE WITH INITIAL STRESSES. COMPLEX POTENTIALS METHOD

Yu.P.Glukhov
S.P.Timoshenko Institute of Mechanics, NASU

In the work with the use of complex potentials in a general form for compressible and incompressible elastic bodies, this formulation is given and the solution of the two-dimensional problem of the action of the moving load on the free surface of a prestressed half-space with heterogeneity in the form of a thin surface layer is given.

To solve the problem, the Muskhelishvili method is used, based on Cauchy-type integrals for the half-plane. In this case, the problem is reduced to the solution of two ordinary inhomogeneous linear differential equations with constant coefficients relative to unknown

analytical functions. The order of the equations depends on the conditions of contact between the protective coating and the base.

Analytical results are given in general form for compressible and incompressible materials with arbitrary elastic potential, for cases of unequal and equal roots of characteristic equations, for different conditions of combination of elements of a layered medium and for any speed of load movement.

Applying the method of complex potentials, we obtain results similar to those obtained by the method of integral Fourier transformations.

ON THE CONSTRUCTION AND NUMERICAL SOLUTION OF DYNAMIC PROBLEMS OF ELIPSOIDAL SHELLS INHOMOGENEOUS IN THICKNESS UNDER NONSTATIONARY LOADS

[1]Yu.A. Meish, [2]N.V. Mayborodina, [2]V.P. Gerasimenko,
[1]National Transport University, Kyiv
[2]Separate subdivision of the National University of Bioresources and Nature Management of Ukraine "Nizhyn Agrotechnical Institute"

Problems of the dynamic behavior of three-layer ellipsoidal shells under the action of non-stationary loads are considered. The processes of forced vibrations of a three-layer ellipsoidal shell are considered a system of nonlinear differential equations of the theory of shells of the Timoshenko type. The stress-strain state of an elastic structure is described using a geometrically nonlinear version of the theory of shells in the quadratic approximation. To solve the problems posed, a numerical algorithm was constructed based on finite-difference approximation of the original equations in space and time coordinates. Numerical results are presented for the cases of the dynamic behavior of single-layer and three-layer ellipsoidal shells, their comparative analysis is carried out.

SUPPORTING OF A MINE WORKING AND A SHELTER IF THEY ARE LOCATED IN UNSTABLE ROCKS

O.P. Krukovskyi, V.V. Krukovska, A.O. Kostrytsia
M.S. Poliakov Institute of Geotechnical Mechanics of the National Academy of Sciences of Ukraine

In cases of emergency power outages with the stop of ventilation and degassing, during fires or explosions of a methane-air mixture, shelters are used to protect miners in coal mines. To ensure non-repair operation of the mine working and the shelter for a long time, it is necessary to choose their supporting correctly. In this work, a numerical simulation of the stress state of rock mass with a mine working and a shelter was performed under conditions when the host rock is weak. It is shown that, over time, near-contour rocks are unloaded from rock pressure, and an area of increased difference of the stress tensor components expands around the mine working and the shelter. This leads to cracks formation with different degrees of intensity. If the host rock is weak, it is necessary to strengthen supporting of the mine working and the shelter with rock bolts. In the bolted area, the rocks are in triaxial compression conditions, a rock-bolts arch is formed above the mine working and the shelter, which prevents the displacement of the roof rocks into the mine working and increases its stability.

TO THE SOLUTION OF DYNAMIC PROBLEMS OF SUPPORTED CYLINDRICAL SHELLS IN THE SPACE OF GENERAL FUNCTIONS

[1]Yu.A. Meish, [2]N.V.Arnauta
[1]National Transport University, Kyiv
[2]National University of Bioresources and Nature Management of Ukraine, Kyiv

This work aims to use the apparatus of generalized functions in solving problems of the dynamics of reinforced cylindrical shells, as well as in constructing effective difference schemes in the space of generalized functions for solving the problems posed. The question of the correctness of the extension to generalized functions of the classical initial boundary value problem for reinforced cylindrical shells is considered. The correctness of this extension is proved under the condition that the ends of the shell are rigidly fixed, which corresponds to zero boundary conditions. The shell and reinforcing edges are described by the linear theory of shells of the Timoshenko type. The conditions for the conjugation of an edge with a shell of a general form are used to construct difference schemes. The proposed approach can be used to solve an arbitrary linear system of partial differential equations, which includes functions that are not differentiated in the classical sense at some points of their domain of definition and have variable coefficients.

MATHEMATICAL MODEL OF THE CALCULATION OF THE MELTING PROCESS OF A CYLINDRICAL FORM OF DEOXIDIZER USING A CURVILINEAR GRID

R.V.Voloshyn
Dniprovsky State Technical University

The paper presents a mathematical model and calculation of the duration of melting of a cylindrical ingot located at the slag-metal interface. To solve the problem, a coordinate grid is formed, for this, half of the cross section of the cylinder is considered, which is divided into M semicircles with radii r_i, where $1 \le i \le M$ and rays j, where $1 \le j \le N$ into N sectors. As a result, control volumes with coordinates i,j are obtained. M0 is set - the initial number of nodes along the radius of the cylinder. The value M>M0 and takes into account the maximum possible number of frozen layers of metal or slag.
The presented work presents a mathematical model of the melting of aluminum-containing additives of a cylindrical shape using a curvilinear mesh (by radius r and angle) in a steel pouring ladle.

MATHEMATICAL MODELING OF ROTATIONAL FLOWS OF A VISCOUS FLUID NEAR SOLID SURFACES

Degtyarev I.D., Tonkoshkur I.S.
Oles Honchar Dnipro National University

The paper considers the problem of the flow of a viscous fluid in a region bounded by two solid surfaces rotating around a common axis with different angular velocities. It is assumed that the axis of rotation is vertical, and the fluid flow is stationary, waveless, and axisymmetric. The problem is solved in the boundary layer approximation. The system of equations of continuity and momentum with the help of self-similar variables is reduced to a system of ordinary differential equations. The solution of the one-dimensional boundary value problem is found numerically using the Matlab package. We considered systems of bodies

consisting of two disks, as well as a disk and a cone. The results of calculations are given for different values of geometric and physical parameters.

NUMERICAL SIMULATION OF CONTAMINANT SPREAD IN GROUNDWATER

D.E.Prozor, I.S.Tonkoshkur
Oles Honchar Dnipro National University

In this paper, we consider the problem of the interaction of a polluted groundwater flow with a clean water flow from injection wells. It is assumed that the thickness of the water reservoir is small compared to its length and width, and the fluid flow does not depend on the vertical coordinate (planned problem). For mathematical modeling of the pollution propagation process, a convective-diffusion transport model is used, based on the equations of filtration and pollution transport. For the numerical integration of differential equations, the finite difference method and the method of establishing a solution for the filtration equation were used. Calculations were made using the Matlab mathematical package. The results of calculations are given for different values of geometric and physical parameters.

СЕКЦІЯ
ІННОВАЦІЙНІ ТЕХНОЛОГІЇ В КІБЕРБЕЗПЕЦІ ТА МЕТОДИЦІ НАВЧАННЯ

ПІЗНАВАЛЬНІ АСПЕКТИ ІНФОРМАЦІЇ ТА ЇЇ БЕЗПЕКИ

[1]О.І.Панченко, [2]П.О.Стеблянко, [3] Ю.С.Тарасенко
[1]Дніпровський національний університет імені Олеся Гончара;
[2]Інститут механіки ім. С.П. Тимошенка НАН України
[3]Дніпро, Університет митної справи та фінансів

Очевидно, що поняття інформації у кожного з нас складалося індивідуально в процесі пізнання навколишнього світу. На даний момент (розуміючи, що з латини information – «відомості, роз'яснення, викладення») кожен з нас вкладає у це слово власне понятійне трактування, сформовану у процесі життєдіяльності (учбової, виробничої, культурної, соціальної і т.д.), яку розширює по мірі свого професійного і культурного зростання, не зменшуючи значення діючої парадигми. У якості додаткового підтвердження її актуальності цілком достатньо прикладу розвитку сучасних телекомунікаційних систем з гарантованою якістю обслуговування QoS (Quality of Service). Причому зі створення цифрових мереж інтегрального обслуговування і технології асинхронного методу передачі (АТМ – Asynchronous

Transfer Mode) почалася реалізація транспортного механізму для передачі усіх видів інформації з QoS. Їх представлення у єдиному цифровому форматі з виділенням потрібних ресурсів мережі, які гарантують QoS перед початком передачі інформації користувача, є обов'язковими компонентами технологій IP/MPLS (Internet Protokol / Multiprotocol Label Switching – мультипротокольна комутація за мітками) і ATM. З 2003 року, коли було озвучено «Архітектуру безпеки для систем, що забезпечують зв'язок між кінцевими пристроями», фактично вперше було визначено методологію організації інформаційної безпеки телекомунікаційних систем [1]. Дана Архітектура безпеки передбачувала розподілення усіх ресурсів телекомунікаційних систем (канали зв'язку, програмно-апаратні комплекси, додатки і т.д.) на незалежні модулі захисту інформації. При цьому кожен модуль повинен задовольняти задекларованим параметрам інформаційної безпеки.

Відповідно, у рамках державної політики забезпечення безпеки інформаційних ресурсів, при створенні і розвитку сучасної методології ефективного забезпечення безпеки інформації необхідно використовувати загальновизнану парадигму захисту інформації. Реалізацію останньої прийнято забезпечувати у відповідності до державних (на рівні ДСТУ) і міжнародних (на рівні ISO/IEC) правовими документами. У наш час існує більше 30 міжнародних стандартів ISO/IEC 2700 [2, с.183], що пов'язані з інформаційною безпекою (ІБ). Хоча ці європейські стандарти і не є обов'язковими, їх значимість у вітчизняному соціумі складно переоцінити. Ці стандарти відображають особливості сучасного рівня інформаційних технологій (принципи, підходи, реалізації), але, нажаль не містять наскрізних шкал цінності і переліків вимог безпеки до використовуваних систем захисту інформації. Реалізація же безпеки останніх, як правило, починається з побудови моделі пізнання гіпотетичних інформоб'єктів з апріорним їх захистом від можливих кібератак і інцидентів, тобто від різноманітних загроз природнього та штучного походження. Фактично парадигма інформації і її безпеки, як вихідної концептуальної схеми і моделі постановки проблем, зводиться до реалізації алгоритмів їх рішень і оптимізації запропонованих методів і засобів захисту інформації. При цьому, відносно тенденції розвитку ІБ, можна стверджувати, що поняття інформації немислиме без поєднання об'єкта її виникнення, засобів зв'язку і підтримуючої інфраструктури, захищених від навмисних або випадкових впливів природнього або штучного походження. Очевидно, що від характеру таких впливів можливими є негативні наслідки як безпосередньо для самої інформації і об'єктів її первинного виникнення, так і відповідної підтримуючої інфраструктури. Навіть при використанні стандарту ISO/IEC 15408, який визначає профіль захисту для підтримуючої інфраструктури з необхідним її рівнем, ймовірні втрати виражаються лише у лінгвістичній формі вигляду «ризик середній».

Викладене вище дає підставу також у лінгвістичній формі озвучити і своє понятійне трактування «інформації», не дивлячись на те, що список існуючих варіантів є вагомим. Тим не менш, без чіткого понятійного трактування інформації ускладнено побудову будь-якої моделі пізнання (забезпечення) безпеки інформаційної системи. Отже, у нашій редакції інформація – це результат опосередкованого впливу у вигляді пізнавально-нематеріального вихідного представлення (субстанції) у фундаменті буття соціуму, що забезпечує достовірність і цілісність в науково-технічній, виробничій, побутовій та інших сферах життєдіяльності людини. Будь-яке її (інформації) перетворення або спотворення, випадкове (несвідоме) або не випадкове (завчано продумане) доцільно розглядати як повідомлення. Причому у другому випадку, - випадку свідомого спотворення, можна вважати таку дію хакерською атакою на інформацію.

Очевидно, що наступні трансформації (перетворення) інформації до вигляду повідомлень потребують відповідних фіксацій (від лат. fixus – міцний, закріплений), реалізованих за допомогою поля (у першу чергу електромагнітного, що забезпечує

телекомунікацію різноманітних видів повідомлень) або за допомогою матеріально-речових носіїв, наприклад, у вигляді газет, документів, дискет, флешек і тому подібних. При цьому будь-яку особистість можна також розглядати з позицій як джерела, так і носія інформації. Відповідно, саме матеріальні носії потребують, у першу чергу, захисту від несанкціонованого допуску до них. Тому, як правило, інформаційну безпеку ототожнюють із захистом її носіїв. Причому прийнято вважати, що основою забезпечення безпеки інформаційної системи є три складові у вигляді конфіденційності, цілісності, доступності, а сам процес успішного захисту інформації в інформаційній системі залежить від рівня апаратного забезпечення, програмного забезпечення і рівня комунікації (забезпечення зв'язку). Використовувані процедури (механізми) захисту від потенційних загроз розділяють на фізичний рівень захисту, на рівень захисту персоналу і організаційний рівень. Саме ж поняття «інформаційна безпека» використовують як вид або діяльності, що направлена на забезпечення захищеного стану об'єкту (у цьому значенні частіше за все використовується термін «захист інформації»), або стану (як якості) конкретного об'єкту. При цьому, у якості об'єкта може виступати і інформація, і дані, і ресурси автоматизованої системи, і сама автоматизована система, і інформаційна система підприємства, суспільства, держави і т.д. Звідси, інформаційна безпека – це стан захищеності інформаційного середовища, а захист інформації являє собою діяльність по запобіганню витоку інформації, що захищається, тобто є процес, який направлений на досягнення цього стану [3].

Нажаль, першоджерело виникнення (появи) безпосередньо самої інформації, на відміну від процесу її поширення і обробки, прийнято замовчувати. Хоча наступні її (інформації) сприйняття, поширення, обробка, зберігання і оцінка як змісту пізнавальної корисності і об'єму, тобто якості і кількості, завжди затребувані і досить важливі при виборі засобів безпеки і захисту від випадкових і навмисних загроз безпосередньо як для самої інформації, так і для відповідної підтримуючої інфраструктури (див. рис. 1). Фактично маємо стійку взаємну кореляцію між об'єктом-джерелом інформації, безпосередньо самою інформацією і об'єктом сприйняття і наступної обробки інформації. Даний процес є аналогічним методам радіолокаційного виявлення, виміру, дозволу, розпізнавання об'єкту спостереження [4] (наприклад, у вигляді орієнтирів на місцевості, злітно-посадкової смуги, авіалайнеру і т.д.) з додатковою інфраструктурою безпеки. Ось і в нашому випадку, розмірковування о виникненні поняття інформації не доцільно здійснювати у відриві від першоджерела (об'єкта), що створює цю інформацію.

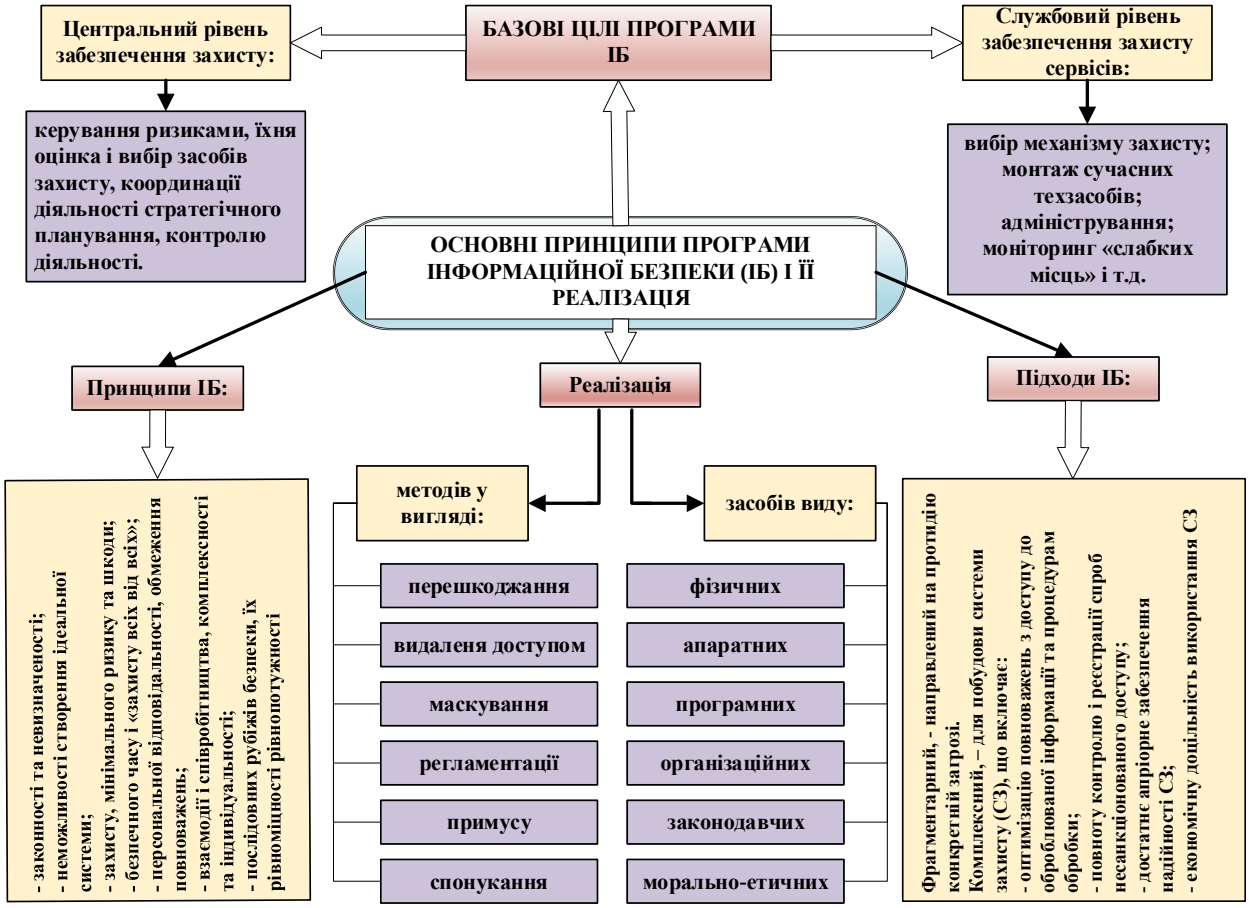


Рисунок 1 – Формування та забезпечення процесу реалізації програми інформаційної безпеки (ІБ)

Залишаючи біологічну сторону виникнення інформації біонікам, методи яких, наприклад [4], уже привели до рівня розробки моделей штучних нейронних мереж, зазначимо тільки матеріальні аспекти появи і наступної реалізації безпеки інформації. Очевидно, що в основі даного процесу лежать фізіологічні (зорове, слухове, дотику і т.д.) сприйняття будь-якого впливу (включаючи і інформаційні загрози), який йде від оточуючого нас світу, у тому числі і соціуму, у якому ми знаходимося. При цьому кожна адекватна людина такий вплив оцінює на основі порівняльної характеристики з раніше існуючими асоціаціями, що були отримані ним у процесі своєї життєдіяльності. Таким чином створюється підсумковий опосередкований результат, який виступає у вигляді першоджерела інформації, оскілки був отриманий безпосередньо у процесі порівняльної лінгвістичної оцінки тих «впливів», які людина набуває протягом свого життя. Звідси, будь-яка первинна інформація є суб'єктивною, а її об'єктивність встановлюють відповідними (у тому числі і метрологічними) експертизами. Подальша обробка первинної інформації (її оцінка, зберігання, поширення і т.д.) у процесі трансформації у вторинну потребує (див. рис. 1) адекватних захисних заходів. Відповідно, запропоноване лінгвістичне трактування інформації, (яке має невизначеність за аналогією з радіолокаційною [5]), без уточнювального прив'язування до об'єкту або суб'єкту, (що створив її з наступною реалізацією над нею дій у вигляді: розпізнавання, розповсюдження, зберігання, додаткової обробки з метою трансформації у інші види представлення і захисту від випадкових або навмисних загроз її існуванню), є цілком виправданим. Завдяки цьому сутність поняття (терміну) «інформація» доцільно розглядати з позицій критично важливого об'єкта, і, відповідно, до неї (інформації) може бути застосовано увесь арсенал технічних і програмно-

апаратних засобів захисту як гіпотетично критичному об’єкту пізнання, частковий арсенал якій приведень у раніше опублікованих матеріалах [6,7].

Список використаних джерел:

1.UTI-T Recommendation X.805 Security Architecture for Systems providing end-to-end Communications, 2003.

2.Вострецова Е. В. Основы информационной безопасности: учебное пособие для студентов вузов / Е. В. Вострецова. – Екатеринбург: Изд-во Урал. ун-та, 2019. 204 с.

3.Алпеев А.С. Ежемесячное приложение к журналу «Стандарты и качество». Экологические аспекты проблем надежности и безопасность технических систем. «Основные понятия безопасности». М., 1994.

4.Субботін С.О., Олійник А.О., Олійник О.О. Неітеративні, еволюційні та мультиагентні методи синтезу нечітко логічних і нейромережних моделей: Монографія / Під заг. Ред.. С.О.Субботіна. – Запоріжжя: ЗНТУ, 2009. – 375 с.

5.Тарасенко Ю.С. Фізичні основи радіолокації [Текст]: навч. посіб. Т 19 / Ю.С. Тарасенко. – Д.: «Пороги», 2011. – 487с.

6.Клим, В., & Тарасенко, Ю. (2022). Методология построения познавательной модели безопасности критической инфраструктуры. *European Science*, *1*(sge11-01), 38–50. https://doi.org/10.30890/2709-2313.2022-11-01-009. Выпуск № sge11-01 (2022): Перспективные мировые научные тренды ‘2022.

7.Yu.S. Tarasenko, V.Iu. Klym. Safety of critical infrastructure objects from the positions of risk effectiveness reduction. Vol. 4 No. 141 (2022): System technologies. Pp. 158-168. Published: 2023-03-04. Дніпро, 2022. – 205с. /Безопасность объектов критической инфраструктуры с позиций снижения эффективности рисков. // Системні технології. Регіональний міжвузівський збірник наукових праць. – Випуск 4 (141). Дніпро, 2022. – 205с. DOI: https://doi.org/10.34185/1562-9945-4-141-2022-13

SECURITY OF ACCESS MANAGEMENT IN INFORMATION SYSTEMS OF ELECTRONIC GOVERNMENT UNDER THE CONDITIONS OF WAR

[1]I. I. Zhulkovska, [1]V.Yu. Klym, [2]O. O. Zhulkovskyi
[1]University of Customs and Finance
[2]Dniprovsky State Technical University

The goal of the information systems (IS) of electronic governments (EG) is to ensure a high-quality level of access, efficiency and obtaining by individuals or businesses of state services and information about the activities of state institutes. In the conditions of emergency situations and martial law the work of the EG in certain territories of the country is especially important for the population, when certain links of logistical communication are disrupted, or people are forced to be outside the country. Currently, the state institutes of Ukraine work under martial law conditions, and therefore the work of the electronic government IS is under greater stress along with the increase in cybersecurity requirements. It is clear that access management as a mechanism of control, supervision and monitoring of access to information resources in computer systems and networks takes priority in emergency situations.

The occurrence of force majeure is usually accompanied by many factors that affect the operation of IS and which include the following: power failure, termination or absence of mobile communication, physical damage or destruction of hardware equipment. The consequences of the influence of the specified factors have a different scale and nature. The main problems for the IS are the restoration of the operational capacity of technical equipment, software in the minimum time interval and checking the integrity and completeness of information resources. Thus, for the EG, the main goal in certain cases is to

ensure remote permanent protected high-quality access to relevant public services for the majority of the population, regardless of location, as well as guaranteeing reliable storage of national information resources: their integrity, relevance, confidentiality [1] .

With a high probability of occurrence of force majeure, an effective method of preventing the loss of information for both objects and IS subjects are the establishment of a multi-factor authentication process and the use of backup and replication of information resources with an increased value of the process execution frequency [2]. This applies not only to large volumes of data included in the IS, such as state registers of taxpayers, voters, court decisions, and others, but also to data which contain user logins and passwords.

Thus, the implementation of the specified security measures increases the level of security of access management to state IT resources, helps to restore it faster in working mode, allows to significantly reduce the risks of unauthorized access to confidential information of the subject and object, the integrity and completeness of information resources of electronic IT government during emergency situations at minimal financial costs.

1. Verkhovna Rada of Ukraine. (2017). Zakon Ukrainy №°2163-VIII «Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny». Holos Ukrainy. – Voice of Ukraine, 208 (2017).

2. ND TZI 3.6 -004-21 The procedure for implementing the information security system in state bodies, enterprises, and organizations whose information and communication systems process information whose protection is required by law and does not constitute a state secret. Kyiv, 2021.

ШЛЯХИ УПРАВЛІННЯ РИЗИКАМИ У ПРОЦЕСІ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПРОЄКТУ

А. В.Пінчук, Т.М.Рудянова
Університет митної справи та фінансів

Розробка програмного забезпечення – це складний процес послідовних дій, який вимагає великої уваги до деталей та пильного контролю над кожним етапом. Існує кілька моделей такого процесу: каскадна (водоспадна), ітераційна та спіральна [1]. Проте, незалежно від обраної моделі існують ризики, які необхідно виявити, знайти шляхи їх усунення або мінімізації та проводити моніторинг наявних ризиків на кожному етапі розробки проекту. Розглянемо основні етапи управляння ризиками. Управлінні ризиками проєкту починається з системного аналізу. Аналіз ризиків у розробці програмного забезпечення повинен включати оцінку потенційних ризиків та їх вплив на проєкт. Оцінка ризиків повинна проводитись на кожному етапі розробки програмного забезпечення, щоб команда розробників мала можливість вчасно виявити проблеми та прийняти відповідні заходи. Для проведення аналізу ризиків можна використовувати різні методи. Одними з найпоширеніших методів є SWOT-аналіз та FMEA (Failure Mode and Effects Analysis). SWOT-аналіз дозволяє оцінити сильні та слабкі сторони проєкту, а також можливості та загрози, що виникають під час його розробки.

FMEA дає можливість ідентифікувати потенційні помилки та визначити їх вплив на проєкт. Після проведення аналізу ризиків необхідно розробити план дій, який включатиме заходи для зменшення ризиків. Ці кроки дозволять збільшити ймовірність успішної реалізації програмного забезпечення. Успішна реалізація програмного забезпечення являє собою створення програмного забезпечення у встановлені терміни відповідно до технічних вимог, встановленого бюджету та реалізації усіх функціональних можливостей. Це проілюстровано на рис. 1.

Рис. 1. Складові успішної реалізації програмного забезпечення

Отже, в цілому більшість ризиків при реалізації проєкту пов’язана з недотримання термінів розробки, запланованих витрат або відсутністю реалізації необхідних функцій програмного забезпечення.

Також слід зазначити, що існує досить багато інших зовнішніх ризиків, на які команда розробки не завжди може вплинути. Ці ризики слід проаналізувати перед початком розробки та періодично під час розробки проводити їх дослідження для прийняття управлінських рішень стосовно проєкту. Перелічимо деякі з них:

- ризик витоку даних та інформації;
- ризик втрати ключових співробітників в команді розробників програмного забезпечення;
- ризик юридичної відповідальності через порушення авторських прав або невідповідність стандартам безпеки даних;
- ризик відсутності прогнозованого попиту на програмне забезпечення;
- ризик непередбачених змін у галузі розробки програмного забезпечення або в економіці в цілому.

Команді проєкту перед початком розробки та на кожному етапі процесу розробки слід обов’язково аналізувати вищезазначені ризики та аналізувати шляхи для зниження настання небажаних наслідків для проєкту. Основними шляхами для зменшення ймовірностей настання небажаних наслідків, на ймовірність яких може вплинути команда розробки є:

- детальний аналіз технічних вимог замовника на розробку програмного забезпечення;
- використання методології Agile при плануванні проєкту для можливості постійного відстеження прогресу розробки [1];
- тестування програмного забезпечення на різних етапах процесу розробки для вчасного виявлення та усунення проблем;
- застосування штучного інтелекту та методів машинного навчання для управління ризиками [2]. Це дозволить в режимі реального часу виявляти закономірності та своєчасно реагувати на ризики. Прикладом можуть бути експертні системи, перевага застосування таких систем полягає в можливості прийняття рішень в

унікальних ситуаціях, для яких алгоритм заздалегідь не відомий і формується за вихідними даними у вигляді правил прийняття рішень із баз знань. Причому рішення завдань передбачається здійснювати в умовах неповноти, недостовірності, багатозначності вихідної інформації і якісних оцінок процесів [3].

У підсумку, аналіз ризиків у розробці програмного забезпечення є важливим етапом управління проєктом, який дозволяє вчасно виявляти та зменшувати ризики. Для успішної реалізації програмного забезпечення проєкту необхідно дотримуватись наданих рекомендацій стосовно зменшення ризиків, а також шукати нові шляхи для управління ризиками. Одним з таких є використання штучного інтелекту та методів машинного навчання.

1. Мартін Р. Чистий Agile: назад до основ / Мартін Р., В. Луненко. Харків: Вид-во «Ранок» : Фабула, 2021. 224 с.

2. Wagner D. Artificial Intelligence and Risk Management [Електронний ресурс] / D. Wagner, K. Furst // rmmagazine. 2018. Режим доступу до ресурсу: http://www.rmmagazine.com/articles/article/2018/09/17/-Artificial-Intelligence-and-Risk-Management.

3. Методи та системи штучного інтелекту: Навчальний посібник для студентів напряму підготовки 6.050101 «Комп'ютерні науки» / Уклад. : А.С. Савченко, О. О. Синельніков. К. : НАУ, 2017. 190 с.

АНАЛІЗ РИЗИКІВ ЗАСТОСУВАННЯ СУЧАСНИХ ТЕХНОЛОГІЙ У КОРПОРАТИВНОМУ УПРАВЛІННІ КІБЕРБЕЗПЕКОЮ

В.М. Гайдаржийський, Т.М. Рудянова
Університету митної справи та фінансів

Кібербезпека – це заходи, що вживаються для захисту комп'ютерних систем, електронних пристроїв, мереж і даних від несанкціонованого доступу, викрадення, пошкодження або знищення. У корпоративному секторі кібербезпека є важливим питанням, оскільки компанії зберігають і обробляють значну кількість конфіденційної інформації, такої як фінансові дані клієнтів, інтелектуальна власність, плани розвитку та бізнес-стратегії. Якщо ця інформація потрапить у руки зловмисників, це може призвести до значних фінансових втрат, репутаційної шкоди та втрати довіри клієнтів. Крім того, корпоративний сектор також залежить від інформаційних технологій для забезпечення ділової продуктивності та ефективності.

Тому, забезпечення кібербезпеки є ключовим аспектом успішної діяльності корпоративного сектору, який повинен приділяти достатню увагу та ресурси для захисту своїх систем та даних від кіберзагроз.

Сучасний корпоративний сектор використовує різні технології для забезпечення кібербезпеки. Деякі з них включають:

1. *Мережеві заходи безпеки:* такі як відключення непотрібних служб, захист мережевого трафіку, використання брандмауерів та вірусних сканерів.
2. *Кіберзахист:* такий як шифрування даних, автентифікація користувачів та застосування політик доступу до даних.
3. *Розпізнавання аномальних поведінок:* такі як машинне навчання та аналіз даних, що дозволяють виявляти зловмисні дії на ранній стадії.
4. *Перевірка цілісності програмного забезпечення:* така як сканування вразливостей та виявлення потенційних шляхів атак.

Загалом, забезпечення кібербезпеки в корпоративному секторі - це складне завдання, яке вимагає постійної уваги та вкладення ресурсів[1].

Також цікавим питанням є застосування штучного інтелекту в кібербезпеку. Штучний інтелект в кібербезпеці може бути використаний для виявлення, захисту та відновлення від кібератак. Ось деякі зі способів, які можуть використовуватися для впровадження штучного інтелекту в кібербезпеку:

1. *Виявлення кібератак:* штучний інтелект може використовуватися для аналізу даних про підозрілу активність в мережі, що може вказувати на кібератаку. Алгоритми машинного навчання можуть використовуватися для виявлення змін у трафіку, які можуть вказувати на атаку.
2. *Захист від кібератак:* штучний інтелект може використовуватися для захисту від кібератак, наприклад, за допомогою системи машинного навчання, яка може виявляти та блокувати зловмисні програми та шкідливі веб-сайти.
3. *Відновлення від кібератак:* штучний інтелект може використовуватися для відновлення даних, які були пошкоджені під час кібератаки. Наприклад, система машинного навчання може автоматично виявляти та відновлювати дані, що були пошкоджені шкідливим кодом.

Загалом, штучний інтелект може використовуватися в кібербезпеці для автоматизації процесів виявлення, захисту та відновлення від кібератак. Це дозволяє більш швидко та ефективно виявляти та реагувати на кібератаки, що допомагає зменшити ризик втрати даних та інших негативних наслідків [2].

При впровадженні штучного інтелекту в кібербезпеку, може бути пов'язане з ризиками, а саме *помилкові спрацювання:* алгоритми машинного навчання можуть зробити помилку, яка може призвести до неправильного виявлення кібератаки або блокування легітимної активності, що може привести до збитків. *Атаки на систему штучного інтелекту:* штучний інтелект може бути скомпрометований або атакований хакерами, що може призвести до того, що атаки на систему будуть незамітними, а також до крадіжки конфіденційної інформації, що може призвести до небезпеки для безпеки та конфіденційності даних. *Недостатній рівень захисту:* у зв'язку з тим, що штучний інтелект є новою технологією, може виникнути ситуація, коли системи кібербезпеки не будуть достатньо захищені від нових видів кібератак, які здатні обійти існуючі системи. *Питання конфіденційності:* використання штучного інтелекту в кібербезпеці може призвести до збору значної кількості даних, що може ставити питання про конфіденційність та захист цих даних від несанкціонованого доступу.

Загалом, впровадження штучного інтелекту в кібербезпеку вимагає ретельної оцінки ризиків і прийняття заходів забезпечення безпеки для зменшення можливості виникнення небезпеки для даних та систем.

Кібербезпека є важливою складовою корпоративного управління, оскільки кіберзагрози можуть привести до серйозних наслідків, таких як витоки даних, порушення бізнес-процесів та навіть загроза життю та здоров'ю людей. В цьому контексті використання сучасних технологій може бути ефективним засобом забезпечення кібербезпеки в корпоративному секторі. Однак, при цьому виникають ризики, пов'язані з можливими наслідками в разі витоку даних, злому мережі та інших кібератак. Крім того, використання сучасних технологій може бути дорогим та складним процесом, який вимагає постійного моніторингу та оновлення.

Незважаючи на це, використання сучасних технологій може відкривати перед корпораціями нові можливості, такі як автоматизація заходів з кібербезпеки, захист від нових типів кібератак та забезпечення високої ефективності заходів з кібербезпеки.

1. Chapter 15 – Corporate Cybersecurity Strategy to Enable Artificial Intelligence and Internet of Things URL: https://www.sciencedirect.com/science/article/pii/B9780128185766000150 (дата звернення: 08.04.2023).

2. The Security Concerns On Cyber-Physical Systems And Potential Risks Analysis Using Machine Learning. URL: https://www.sciencedirect.com/science/article/pii/S1877050922004811 .

РИЗИК-ВПЛИВ НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Ю.С.Тарасенко
Університет митної справи і фінансів

Очевидною є актуальність захисту інформації (ЗІ) для штатної роботи будь-якого об'єкта критичної інфраструктури (ОКІ) і його (об'єкта) кібербезпеки [1-4]. Причому до доказового аргумента вищезазначеного необхідно віднести і наказ МОНУ № 311 від 20.03.2023 року «Про апробаційне проведення єдиного Державного кваліфікаційного іспиту за спеціальністю 125 Кібербезпека у 2022/2023 навчальному році», далі - ЄДКІ. Проведення цього кваліфікаційного іспиту відбудеться 27.04.2023 р. за програмою ЄДКІ зі спеціальності «Кібербезпека» на першому (бакалаврському) рівні вищої освіти, затвердженою наказом Міністерства освіти і науки України від 04.11.2022 № 980 у комп'ютерному форматі у формі зовнішнього незалежного оцінювання із організацією очного контролю (прокторингу) в належно облаштованих комп'ютерних аудиторій. А оскільки ризики існують у будь-якій професійній діяльності (у якості прикладу: - як при оптимізації вибору засобів захисту ОКІ, так і для процесу організації і проведення ЄДКІ), то додаткова деталізація можливостей впливу інформаційних ризиків стає виправданою.

Зокрема, не дивлячись на відсутність загальноприйнятого формулювання терміну «інформації», але враховуючи єдиний процес її обробки (від джерела виникнення до споживача, реалізуючи, як правило, декілька етапів: виявлення, розпізнавання, оцінки і т.д., включаючи і заключний – у вигляді архівування), можна стверджувати, що: *інформація – це результат опосередкованого впливу у вигляді пізнавально-нематеріального початкового представлення (субстанції) у фундаменті буття соціуму, що забезпечує достовірність і цілісність в науково-практичній, виробничій, побутовій і інших сферах життєдіяльності людини*. У такому контексті, інформаційна субстанція може бути представлена як у вигляді електронних носіїв, так і у вигляді візуальної або печатної продукції. Фактично таким чином здійснюється певний «життєвий» процес інформації, яким, за аналогією з логістикою, можна керувати. Очевидно, що будь-якому динамічному процесу (у тому числі і інформаційному) властиво відчувати різноманітні види впливу, причому не завжди позитивного призначення і енергетичного рівня. Тому, у даному випадку для отримання кінцевого результату, близького до істинного (первинного), може знадобитися вибіркове або загальне нівелювання інформаційних етапів. Як правило, це потребує оптимізації неблагонадійних ризик-впливів у рамках сучасних досягнень інформаційних технологій і виділеного на це бюджету. Отже, як і будь-який процес, інформаційний ризик може також піддаватися аналізу, встановлюючи його якісне, кількісне або комбіновані (у залежності від числа і видів впливів) значення. Таким чином, ризику і його проявленням властива операція керування, основною ціллю реалізації якої є попередження згубних впливів на об'єкт захисту, куди звичайно входить і інформаційна субстанція.

Вищевикладене, особливо в освітньому середовищі (наприклад, при вивченні курсу Програмно-технічні засоби захисту інформації), доцільно реалізувати (особливо на перших ввідних лекціях) у вигляді структурних схем з різними ступенями складності: від збільшеної (з метою першочергового спрощеного сприйняття) до схемо-технічної (з програмно-логічним функціоналом), - у сукупності вузлові аспекти

наступного викладення дисципліни. Так на рис. 1 наведена збільшена схема методології пізнання (представлення) інформації як об'єкта критичної інфраструктури (ОКІ) з її можливими (гіпотетичними) супутніми ризик-впливами, що надалі деталізовані у відповідності з європейськими стандартами серії ISO/EC 27000 [4].

Рис.1. Представлення інформації як ОКІ із супутніми ризик-впливами

Зокрема, використовуючи зміст вибору засобів захисту з позицій ризик-інформаційної безпеки у межах застарілого ISO/IEC TR 13335-4:2000, складно помилитися з перерахуванням основних видів ризик-впливів на інформацію, - як об'єкта критичної інфраструктури (ІкОКІ). У відповідності з чим (див.рис.2) – підсистему вибору засобів захисту (ЗЗ) ІкОКІ можна розглядати з позицій:

- організаційних та фізичних засобів захисту загального застосування;
- специфічних засобів захисту інформаційної системи;
- засобів конфіденційності;
- засобів контролю цілісності;
- засобів захисту доступності;
- засобів захисту з позиції спостережності, автентичності та надійності.

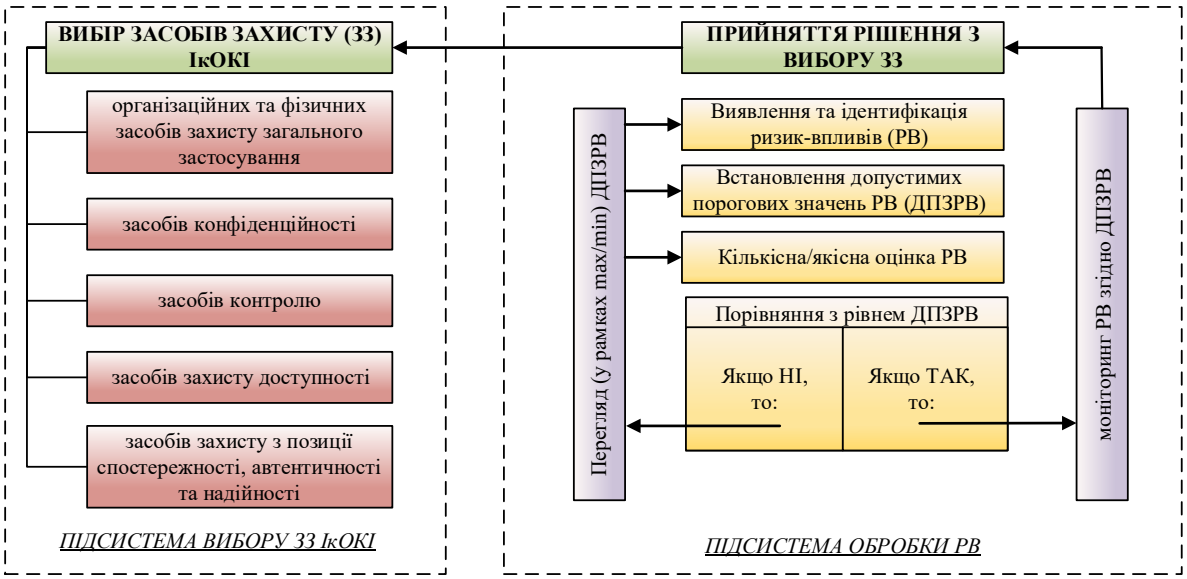


Рис.2. Представлення циклічності прийняття рішень з вибору ЗЗ

Із врахуванням вибору критеріїв ризику та «ступеню реалізації запланованих робіт і досягнення запланованих результатів» (тобто результативності [5, п.3.7.11]), як правило, и проводять оцінювання втрат безпеки згідно ДСТУ ISO/IEC 27000:2019 відносно конфіденційності, цілісності, доступності, спостережності, автентичності, надійності інформації [3]. При цьому рівень остаточного прийняття рішення за вибором ЗЗ забезпечується у процесі оптимізації управління ризиком шляхом багаторазової реалізації процедури обробки ризика, використовуючи, наприклад, метод послідовних наближень по зниженню ризику до прийнятного рівня (див.рис.2). У цьому випадку

гіпотетична структурно-блокова підситема обробки ризику (ПОР) повинна послідовно забезпечувати:

- виявлення і розпізнавання ризик-впливів на ІкОКІ;
- встановлення порогових значень ризику (ПЗР);
- кількісну (при бажанні, - і якісну) оцінку ризику;
- функціональне порівняння відфільтрованого сигналу з ПЗР.

Крім цього, до складу ПОР повинні входити:

- система моніторингу ризику, яка забезпечує фільтрацію (по max/min) ПЗР у вигляді відсічення (завершення) доступу до системи. Прийняття рішення по вибору ЗЗ, де рівень ПЗР встановлюється апріорі, наприклад, по аналогії з критерієм ідеального спостерігача або Неймана-Пірсона [6], що використовують не тільки у радіолокації;

- система переоцінки ПЗР, яка здатна варіювати допустимими значеннями ризиків, забезпечуючи таким чином багаторазову реалізацію процедури вибору ЗЗ, остаточне рішення по яким залишається за Особою, що приймає рішення.

Звичайно очевидно, що настільки коротке представлення ввідного лекційного матеріалу у майбутньому потребує більш детального викладення (опису) існуючих технологій і інструментальних засобів виду Coras, Ebios, ISAMM, IRAM$_2$, PTA и т.д.. Але, знаходячись у межах освітньої сфери, потрібно мати на увазі, що найбільш досконалий процес управління ризиками не дозволяє звести їх до нуля. Таким чином, викладене вище формує загальне уявлення про ітераційно-циклічний процес управління ризиком по апостеріорно створеному списку потенційних ризиків (у нашому випадку – це ІкОКІ) із врахуванням ймовірності їх настання і можливих негативних наслідків для конкретного ОКІ. При цьому акцентується наступність із раніше викладеними спеціальними дисциплінами, неперервність пізнавального процесу з обраної спеціальності і доцільність викладення матеріалу з позицій методики пізнання предмету вивчення та його значимості на рівні викладення з використанням нормативних державних та міжнародних стандартів. Усе це без сумніву підвищує престижність лекцій та їх значимість для студентів, що у підсумку сприяє майбутнім особам, що приймають рішення, свідомо підвищувати свій професійний рівень.

1. ДСТУ ISO/IEC 27000:2019 (ISO/IEC 27000:2018, IDT) Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Огляд і словник термінів. Київ ДП «УкрНДНЦ». Наказ від 16.10.2019 № 312.

2. ISO/IEC 27001:2013 Информационные технологии — Методы обеспечения безопасности — Системы менеджмента информационной безопасности — Требования /Information technology — Security techniques — Information security management systems —Requirements/ Вторая редакція. 2013-10-01.

3. . ДСТУ ISO/IEC 27005:2019 Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки (ISO/IEC 27005:2018, IDT) Дата початку дії 01.11.2019. ДП «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» (ДП «УкрНДНЦ») Дата прийняття 16.10.2019. Мова документа Англійська. International standard ISO/IEC 27005:2019 Information technology – Security techniques – Information secure risk management. https://www.google.com/url

4. Yu.S. Tarasenko, V.Iu. Klym. Safety of critical infrastructure objects from the positions of risk effectiveness reduction. // System technologies. Pp. 158-168. Vol. 4 No. 141 (2022): Published: 2023-03-04. Дніпро, 2022. – 205с.

5. ДСТУ ISO 9000:2015 (ISO 9000:2015,IDT) Системи управління якістю. Основні положення та словник термінів. Київ ДП «УкрНДНЦ», 2016. 51 с.

6. Тарасенко, Ю.С. Фізичні основи радіолокації [Текст]: навч. посіб. / Ю.С.Тарасенко. – Д.: Вид–во «Пороги», 2011.– 487 с.

ТЕХНІКИ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКА

В.І.Бакало
Національний авіаційний університет

Інформація є важливим ресурсом держави, комерційних структур і приватних осіб. Тому її захист дуже важливий і актуальний під час воєнного стану.

Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України спільно з Національним банком України запустили проект з протидії кібершахрайству у фінансовому секторі. Його метою є захист громадян від крадіжок коштів через фішингові кампанії, що активізувалися в період воєнного стану.

Рис. 1 – Кіберінциденти

В Україні значно зросла кількість випадків кібершахрайства. З огляду на масштаби цієї загрози, національний телеком оператор Київстар здійснив інвестиції у розмірі 300 мільйонів гривень у проекти цифрового розвитку, кіберзахисту і кібербезпеки України.

Нестабільна емоційна поведінка людей у стресових ситуаціях стала сприятливим фоном для різного виду обману.

Масове розсилання різного виду інформації теж є загрозою, бо може містити не тільки комп'ютерні віруси, а повідомлення що поширюють фейки та негатив.

Після майже 36 років з моменту першої згадки про нього та майже 30 років з моменту появи перших примітивних форм атак у чатах фішинг все ще залишається однією з найбільших загроз в Інтернеті.

Як і будь-яка технологія фішинг розвивається, вдосконалюється від простої імітації надійного сервісу до атак на критичну інфраструктуру (Colonial Pipeline, США).

У 1990-х роках з’явився термін «фішинг» як позначення використання шахрайських електронних листів, щоб «виловлювати» інформацію від нічого не підозрюючих користувачів. AOL Inc. (американська медіакомпанія, постачальник онлайн сервісів та електронних дошок оголошень) була популярною системою контенту з доступом до Інтернету, зловмисники використовували фішинг і обмін миттєвими повідомленнями, щоб маскуватися під співробітників AOL, щоб обманом змусити користувачів розкрити свої облікові дані для викрадення облікових записів.

Фішингові електронні листи у 2000-х роках стали використовувалися, щоб обманом змусити користувачів розкрити облікові дані свого банківського рахунку. Електронні листи містили посилання на шкідливий сайт, який дублював офіційний банківський сайт, але домен був незначним варіантом офіційного доменного імені (наприклад, paypai.com замість paypal.com). Пізніше зловмисники переслідували інші облікові записи, такі як eBay і Google, щоб викрасти облікові дані, викрасти гроші, вчинити шахрайство або розсилати спам іншим користувачам.

Перший позов про фішинг був поданий у 2004 році проти каліфорнійського підлітка, який створив імітацію сайту «America Online». За допомогою цього підробленого веб-сайту він міг отримати конфіденційну інформацію від користувачів і отримати доступ до даних кредитної картки, щоб зняти гроші з їхніх рахунків.

Соціальна інженерія як метод маніпулювання людською психікою допомагає кібершахраям в їх незаконних діях. Фішингові листи – ефективний, дешевий, безкоштовний інструмент для швидкого отримання доступу до різного виду даних.

Підштовхуючи до спонтанних дій перед загрозою блокування облікового запису, втрати грошей чи клієнтів люди діють необдумано та не розпізнають необґрунтованих вимог, підозрілих запитів. Розпізнають обман лише після того, як перестануть хвилюватися, ретельно все зважать - бачать результат шахрайства.

Використовуючи, здавалося б, невинну електронну пошту, кіберзлочинці можуть отримати невелику точку опори та розвинути її.

Діючи за простою логікою шахраї отримують доступ до персональних даних. Використовуючи прості кроки, які показано у схемі вони отримують фінансові ресурси довірливого користувача.

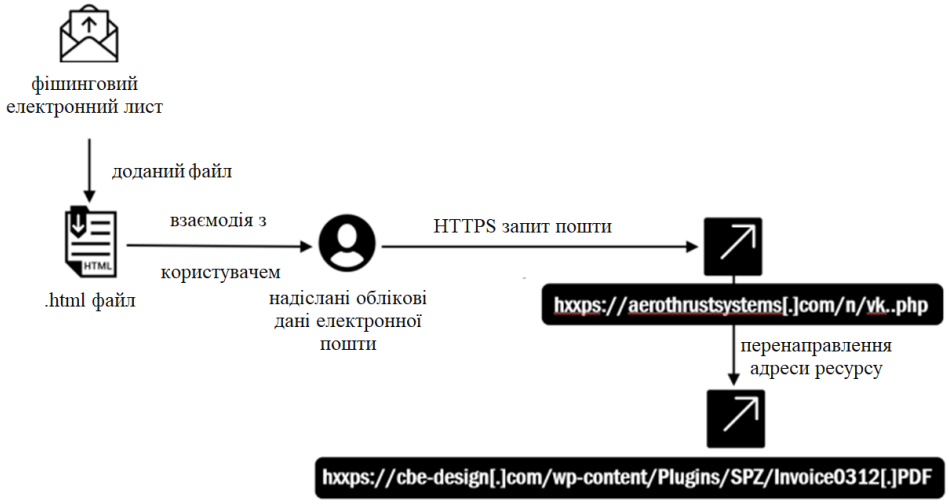


Рис. 2 – Узагальнена схема ланцюга атаки

Використовуючи людські слабкості фішинг розвивається, вдосконалюється і на сьогодні відомі такі його види:

- оманливий фішинг (посилання електронної пошти, які перенаправляють користувачів на помилкові веб-сайти збору даних, наприклад облікові дані для входу);
- підробка веб-сайтів (команди javascript використовуються для зміни URL-адреси, на яку вони ведуть. Це може статися, якщо відкрити фальшиву веб-адресу замість легальної);
- обхід фільтра (замість тексту використовуються зображення, тому антифішинговим фільтрам важко виявити їх);
- голосовий фішинг (дзвінки з банків з вимогою надати конфіденційні дані для крадіжки грошей, покупок);
- SMS-фішинг (повідомлення оманливого характеру: «ви виграли приз, натисніть ..., щоб подати заявку»);
- InSession Phishing (відкриває спливаюче вікно, яке вводить користувача в оману);
- мобільний фішинг (спонукання мобільних абонентів переказувати гроші зі свого рахунку на рахунок шахрая);
- спуфінг (тактика видавання себе за когось з метою отримання доступу до конфіденційних даних або банківських рахунків).

Фінансова вигода є основною метою більшості фішингових атак. Маючи на меті конкретні цілі, що містять дані кредитних карток, великі суми грошей їхні зусилля спрямовані на електронну комерцію, соціальні медіа, фінансові установи, платіжні системи, IT-компанії, телекомунікаційні компанії та компанії з доставки.

Фішинг постійно розвивається, щоб обійти засоби безпеки та виявлення людьми, тому потрібно постійно вчитися розпізнавати найновіші стратегії фішингу. Щоб спровокувати серйозне порушення даних, потрібно лише одній людині потрапити на фішинг. Ось чому це одна з найбільш критичних загроз, яку потрібно пом'якшити, і найскладніша, оскільки вона потребує людського захисту.

Жертвами кібершахрайства стають сотні тисяч українців, які втрачають десятки мільйонів гривень щодня. Українські банки блокують такі кошти на рахунках злочинців, і під час розслідування злочинів гроші повертаються. Проте не завжди можливо заблокувати викрадені кошти вчасно, бо вони перераховуються на території, не підконтрольні правоохоронним органам України.

Захист від фішингу є важливим компонентом безпечної роботи будь-якої структури та фінансової безпеки людини. Тому прості дії допоможуть вам уникнути неприємностей:

- використовуючи фільтри спаму ми захищаємось від нього. Фільтри аналізують походження повідомлення, програмне забезпечення, яке використовувалося для його надсилання, зовнішній вигляд для визначення чи воно є спамом. Але маємо враховувати що не завжди спам-фільтри діють на 100% точно (блокують електронні листи з законних джерел);

- зміна налаштувань браузера може запобігти відкриттю шахрайських веб-сайтів, оскільки вони зберігають список підроблених веб-сайтів, і при отриманні доступу до веб-сайту адреса блокується або з'являється повідомлення з попередженням. Такі налаштування допомагають відкривати лише надійні веб-сайти;

- банківські та фінансові установи для запобігання фішингу використовують моніторингові системи;

- слід пам'ятати, що захищені веб-сайти з дійсним сертифікатом Secure Socket Layer (SSL) починаються з «https».

Список літератури

1. Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. URL: https://scpc.gov.ua/api/docs/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7/4eeb6a10-b7aa-4396-8b04-e0e4b7fca1b7.pdf
2. Перелік категорій кіберінцидентів. URL: https://www.cip.gov.ua/ua/news/perelik-kategorii-kiberincidentiv.
3. О. Трофименко, Ю. Прокоп, Н. Логінова, О. Задерейко. Кібербезпека України: аналіз сучасного стану. Захист інформації. 2019. (том 21, № 3).
4. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. Київ: Видавничий дім «АртЕк», 2017.

МЕТОДОЛОГІЯ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ KANBAN: ПРИНЦИПИ ТА ПЕРЕВАГИ

О. Лебідь, Я. Лебідь
Університет митної справи та фінансів

У будь-якого програмного забезпечення є свій життєвий цикл – етапи, через які воно проходить з початку створення до кінця розробки. Найчастіше це підготовка, проєктування, створення та підтримка. Етапи можуть називатися по-різному і поділятися на більш дрібні стадії. Необхідність вибирати методології розробки програмного забезпечення обґрунтована якісним підходом. Оскільки без чіткого плану дій можна почати створення продукту, але так і не закінчити його. Існують різноманітні методології, що покращують роботу. Так, наприклад, каскадна модель, ітеративна та інкрементна моделі, V-модель, RAD та Agile моделі.

Одним із підходів Agile є так звана система постановки завдань та організації робочих процесів Канбан, вона направлена на ефективне досягнення поставленої мети. Головний принцип полягає в обговоренні продуктивності у режимі реального часу, наочності просування роботи. Учасники команди мають змогу бачити стан завдань у будь-який час, оскільки вони візуально представлені на спеціальній дошці.

Інструмент управління Agile-проєктами, Канбан-дошка, допомагає візуально подати завдання, визначити обсяг незавершеної роботи, підвищити її ефективність та швидкість. Метод заснований на управлінні виконанням завдань за допомогою карток, що сигналізують про настання та завершення певних етапів. Така система дозволяє делегувати завдання, керувати реалізацією проєкту будь-якої складності, швидко виявляти слабкі місця. Учасникам команди простіше виконувати завдання, оформлені візуально, зростає ефективність роботи при одночасному зниженні навантаження, до того ж вирішується проблема зірваних дедлайнів та завдань, що забули виконати. Також дошка не тільки допомагає виявити недоліки, така візуалізація процесу показує внесок та цінність кожного співробітника, що є джерелом мотивації для людей. Почати побудову своєї системи Канбан можна з простої дошки з трьома основними колонками: Зробити (To do), У роботі (Doing), Готово (Done). Але у випадку з розробкою програмного забезпечення можуть містити такі розділи, як: обговорювані завдання; узгоджені завдання; написання коду; тестування; підтвердження; виконані завдання тощо.

Вперше концепцію Канбан-дошки розробила та впровадила на своїх заводах компанія Toyota. Візуальна система управління завданнями допомогла менеджерам швидко підвищити ефективність організації виробничого процесу та постачання. Його основною метою спочатку була мінімізація відходів без шкоди продуктивності. Головне завдання – створення більшої цінності для клієнта без збільшення витрат. Завдяки своїй ефективності Канбан залишив сферу автомобільної промисловості та був застосований в інших секторах: фінансах, маркетингу, IT-індустрії (розробка програмного забезпечення) та ін [3].

Важливо знати основні принципи, щоб користуватися даною методикою, оскільки однієї дошки недостатньо. Це скоріше побажання для успішної роботи, аніж жорсткі правила. У цій методиці змішалися принципи agile-методологій і lean-мислення. Отож, перший принцип – це візуалізація процесів. Варто забезпечити, щоб усі поставлені завдання було додано у план. Їхній статус варто оновлювати в міру завершення етапів, що вже пройшли. Таким чином можна стежити за прогресом та крок за кроком просуватися вперед і бачити завдання, для вирішення яких необхідно більше часу та допомоги. Друге – згрупування завдань. Найпростіше – розділити завдання на три колонки: «Треба виконати», «Виконується», «Виконано». Такий підхід передбачає візуалізацію робочого процесу та переміщення отриманого завдання з одного етапу на інший. По-третє, потрібно звертати особливу увагу до незавершених завдань. Якщо завдання затримуються на якомусь з етапів, варто розібратися в причинах, розподілити ресурси у разі потреби або надати потрібну підтримку для завершення роботи. Ще один важливий принцип – постійне вдосконалення та покращення [2]. Оскільки контроль за дотриманням термінів виконання завдань та їх переміщенням з одного рівня на інший у цій системі допомагає бачити слабкі місця в роботі. Таким чином, можна чітко визначити, де слід приділити більше часу роботі, а в яких ситуаціях потрібно змінити навантаження. Також дуже важливо підтримувати лідерство на всіх рівнях, так як лідерські дії на всіх рівнях – від окремих працівників і аж до старшого менеджменту – дуже хороша ознака [1] .

Порівняння Kanban і Scrum. Існує ще така система управління проєктами, яка на перший погляд схожа з Канбаном, що носить назву Скрам (англ. scrum), вона теж відображає процес вирішення завдань і допомагає досягати поставлених цілей. Однак між цими двома методами є суттєві відмінності. Варто виділити головні з них:

1. У Скрамі робота ділиться на фази, які називають спринтами. Кожен із них вирішує певне завдання — частину проекту. Після закінчення спринту є якийсь конкретний результат, який можна оцінити чи презентувати замовнику. У Канбані робота над завданням розділена на кілька етапів і вона вважається вирішеною тільки після того, як пройшла їх усі.

2. У Канбані можна розділити процес на будь-які відповідні етапи. У Скрамі є конкретна структура, що дозволяє сфокусуватись на результатах.

3. У Скрамі не можна вносити зміни в процесі роботи, щоб не переривати спринт. У Канбані навпаки – можна змінювати перебіг подій, якщо це знадобиться.

4. У Канбані немає вимог щодо проведення щоденних зустрічей для оцінки результатів виконаної роботи. У Скрамі це основа виконання проекту.

5. У системі Скрам є чітко визначені ролі: власник продукту або менеджер продукту, скрам-майстер та команда. У Канбані такого поділу немає, роботою керують усі учасники процесу.

Переваги та недоліки. У методології Канбан немає жорстких правил чи обмежень. Тому її використовують у найрізноманітніших сферах. Тож можна виділити основні переваги, якими вона наділена:

1. Наочність просування роботи та прозорість робочого процесу. Одна з головних переваг даної методології управління процесами. Легше виявляти та усувати проблеми, коли є доступ до поставлених завдань та результативності просування у всіх членів команди. Так кожен може швидко отримати інформацію про стан проєкту.

2. Гнучкість планування. Команда зосереджується лише на певному завданні, незважаючи на те, що їх може бути декілька. Також керівник проєкту може змінювати пріоритети виконання роботи, не торкаючись безпосередньо робочого процесу. Після завершення одного завдання команда одразу розпочинає наступне.

3. Швидкість виконання. З’являється безліч способів для менеджерів проєктів уважно стежити за розподілом роботи та робити обґрунтований аналіз.

4. Контролює терміни виконання. Така методологія забезпечує відстежування робочого процесу, дозволяє оптимізувати його тривалість і прогнозувати час, який буде потрібен для вирішення майбутніх задач.

5. Задоволеність клієнтів. Можливість скоротити втрати, концентруючи роботу лише над тими завданнями, які потрібні зараз.

Серед недоліків можна виділити те, що цей метод не підходить для довгострокового планування. Тобто він розрахований для досягнення швидких цілей, де робота вибудовується на вирішенні актуальних завдань, при цьому їх пріоритетність може змінюватися залежно від обставин. Також він не підходить для команд з великою кількістю учасників. Оскільки чим більше людей задіяно у робочому процесі, тим складніше контролювати виконання завдань. Тож краще було б, щоб в одній команді було не більш як десять осіб, а якщо виконання завдання вимагає багато людей, слід розбити їх на невеликі групи і створити для кожної окрему систему Канбан.

Зважаючи на вищезазначені переваги та недоліки, все частіше віддають первагу саме цій методології, оскільки вона може полегшити роботу в багатьох інших сферах, відмінних від IT-індустрії. Візьмемо, наприклад, промислове виробництво – різні ділянки виробництва мають власні плани, які враховують реальну обстановку. У результаті одні деталі виробляються надміру, інші опиняються в дефіциті – звідси перебої у роботі та невиконання плану. Методологія Канбан пропонує такий тип виробництва, при якому робота у такому разі ведеться точно і у поставлений термін. Замовлення виконуються після надходження, а замість плану – попит споживачів. Кожна наступна ділянка виробництва замовляє попереднім ті деталі, які потрібні у необхідній кількості. Деталі подаються одночасно у потрібні точки, готова продукція відправляється споживачеві. Як наслідок, зменшення ризиків, грамотне регулювання складських запасів.

Дана система допоможе також при збільшенні продажів – оскільки одним із найважливіших напрямків у B2B-бізнесі є робота з клієнтами, вона ідеально підходить для прискорення воронки продажів. Так менеджер вибирає свої угоди та визначає статус клієнта. Щоб пересунути картку на дошці вперед, потрібно підштовхнути клієнта до покупки. Далі треба продати товар клієнту, з яким уже ведеться робота і тільки тоді можна братися до наступної справи. На кожному етапі в свою чергу має бути список умов подальшого просування угоди. Таким чином аналіз роботи етапів даної угоди сприяє оптимізації процесу. А щоб створити досконалу систему роботи з клієнтами, слід відстежувати статуси, які накопичуються на етапах воронки продажів, проводити аналіз ситуації, що складається, вживати відповідних заходів, тим самим змінюючи систему в потрібну сторону.

На думку авторів така система може бути дуже корисною і в особистому плануванні. Вона, безумовно, ефективніша за щоденники та списки, а дошка, завдяки своїй наочності, допомагає упорядковувати домашні та особисті справи. Таким чином, можна спланувати свій місяць чи тиждень, визначивши для себе першочергові задачі та ставити цілі, які крок за кроком будуть досягнуті.

Можна підвести підсумок, що Канбан – досить ефективна методологія, яку можна використовувати у різних сферах. Проте залежно від завдань, які вирішує команда, керівник проєкту може вибрати будь-яку іншу систему організації спільної роботи та управління. Кожна з яких має свої сильні та слабкі сторони. Не можна однозначно сказати, який із методів кращий, тому потрібно вибирати той підхід, який найбільш зручний для команди і найбільше підходить для вирішення певних завдань.

1. What is Kanban? – Basics. Get to know the advantages, disadvantages, and principles of Kanban. – URL: https://sendpulse.com/support/glossary/kanban

2. Методологія Kanban: можливості та принципи роботи. – URL: https://para.school/blog/management/metodologija-kanban-vozmozhnosti-i-printsipu-rabotu

3. Kanban (development). – URL: https://en.wikipedia.org/wiki/Kanban_(development)

ШЛЯХИ ВДОСКОНАЛЕННЯ ДИСТАНЦІЙНОГО ВИКЛАДАННЯ МАТЕМАТИЧНИХ ДИСЦИПЛІН В УКРАЇНСЬКИХ НАВЧАЛЬНИХ ЗАКЛАДАХ ЗА УМОВ ВОЄННОГО СТАНУ

М. Ф. Мормуль, Д. М. Щитов, О. М. Щитов, Є. С. Курбацька
Університет митної справи та фінансів

Дистанційне навчання набуло в Україні стрімкого розвитку з 2019 року, під час епідемії коронавірусу COVID-19, а з 2022 року стало невід'ємною формою навчання у школах, спеціальних середніх і вищих навчальних закладах тих населених пунктів, де: 1) існує реальна загроза бомбування чи потрапляння ракет; 2) часто звучать сирени, за яких слід негайно переривати заняття та йти в укриття; 3) які безпосередньо знаходяться на лінії вогню; 4) або у тимчасовій окупації.

При дистанційному навчанні (або навчанні онлайн) вся чи більша частина курсу викладається слухачам за допомогою сучасних технологій та в інтерактивному режимі, при цьому викладачі та слухачі можуть знаходитись в різних країнах та навіть на різних континентах. Щоправда, таке навчання підходить не для всіх дисциплін. Слід зазначити, що деякі студенти продовжують навчання в такий спосіб, навіть перебуваючи на фронті, в перервах між бойовими діями. Зокрема, є такі студенти-

фронтовики серед студентів Університету митної справи та фінансів. До переваг цього виду навчання відносяться:

- економія часу – не треба витрачати дорогоцінні години, простоюючи у заторах чи приїжджаючи з далека. Люди, які не живуть у містах, економлять також і значні кошти, які мали б витратити на проїзд;
- охоплення більшого числа слухачів, оскільки можливість навчатися мають мешканці не тільки великих міст, але й найвіддаленіших містечок і сіл, і навіть країн. А це вкрай важливо, оскільки, як ми знаємо, велика кількість мешканців з дітьми та студентів (в основному, дівчат) внаслідок російської агресії виїхали за кордон;
- зручність викладання, оскільки усі потрібні матеріали для занять завжди є під рукою (і у викладача, і у слухача);
- можливість контролювати увагу кожного слухача, що важко робити у реальному часі;
- збереження у файлах переписки зі слухачами, їх відповідей та всього заняття, що дає змогу в будь-який момент повернутися до пройденого матеріалу;
- зручність такого формату для людей з обмеженими фізичними можливостями;
- активне використання зображень, тексту, звуку та відеоряду, що суттєво підвищує якість засвоєння нової інформації.

Дослідники зазначають й інші переваги [1, с. 8-9], [2, с. 28].

До вад дистанційного викладання можна віднести наступні:

- не завжди гарний Інтернет чи добра якість зв'язку;
- вимушене припинення уроку через вимкнення електропостачання (планового чи аварійного, від чого останні місяці потерпає Україна);
- недостатність спілкування з викладачами у режимі реального часу, бо Інтернет все ж таки не замінить дискусію з викладачем віч-на-віч на тему, що вас хвилює;
- відсутність повноцінного педагогічного контролю з боку викладача, що є стимулюючим чинником для ефективного навчання;
- ресурсовитратність і трудомісткість з боку закладa вищої освіти (ЗВО) та викладача. Окрім необхідного технічного оснащення закладу освіти, від викладача вимагається створення дистанційного курсу [2, с. 29];
- велика кількість відомостей за досить короткий час тощо.

Дуже важливо для проведення дистанційного навчання з конкретного курсу обрати платформу, найбільш зручну для даного випадку та даного предмету. Розроблених платформ для дистанційного навчання існує досить багато. В українських навчальних закладах в основному користуються платформами Zoom на базі Google.classroom, Skype, Moodle, Googgle Meet. При цьому існують декілька видів (форм) дистанційного навчання, які зазвичай використовуються сумісно:

1) кореспондентське, коли студенти отримують навчальні матеріали, тести чи екзаменаційні питання електронною поштою або через посилення на файл у Google Class і працюють, отримуючи певну допомогу викладача через пошту, телефон або чат;

2) електронне навчання через комп'ютер, Google Диск, компакт-диски або DVD-диски, певні комп'ютерні програми;

3) онлайн-навчання у форматі діалогу – це власне інтерактивне навчання.

Дистанційне навчання саме математичним дисциплінам має свої особливості та труднощі, оскільки доводиться не лише проголошувати текст, а й писати формули, креслити графіки. Це можна робити одним із трьох способів: 1) за допомогою планшета або онлайн дошки (online whiteboard) з мишею, але це часом досить складно, якщо формул та графіків забагато; 2) направити веб-камеру не на викладача, а на його стіл, щоб слухачі бачили те, що він пише на аркушах паперу; 3) поступово в ході заняття викладати заздалегідь підготовлені матеріали презентації: текст, формули, графіки та

рисунки. Але це є статичною інформацією, і втрачається «живе» інтерактивне спілкування з аудиторією, динаміка показу матеріалу, відповідей на питання.

Виходячи з власного досвіду, хочемо висунути пропозиції щодо вдосконалення вже існуючих платформ з метою пристосування їх для більш зручного викладання математичних дисциплін та суміжних з ними. Зокрема, платформа google.classroom, за допомогою якої проводяться тестування та іспити, потребує таких доробок.

1. Форми google.classroom призначені більш для гуманітарних наук. Однак ними доводиться користуватись і викладачам точних наук: математичні дисципліни, фізика, хімія, економіка і т. ін. У тестах та завданнях з цих предметів треба вводити багато формул та графіків, але у «формах» google.classroom немає можливості вводити їх безпосередньо. Треба спочатку переводити їх у формат рисунка з розширенням jpg або jpeg, а потім заводити у форму через файл, що дуже незручно та довго. До того ж, як у текст завдання, так і у варіанти відповідей можна вставити тільки один рисунок чи формулу, (переведених у рисунки), а якщо їх кілька, то доводиться весь текст завдання переводити у формат рисунка jpg або jpeg. Отже, було б доцільно уникнути цей недолік і надати викладачам можливість просто вставляти формулу у рядки «Варіант» чи «Текст завдання», а не як рисунок, розташований нижче цих рядків.

2. Також доцільно зробити можливим введення надрядкових та підрядкових індексів, чого поки що немає. Щоб передати такі індекси, доводиться також переводити їх у формат рисунка. Також бажано мати можливість безпосередньо вводити у рядки «Варіант» чи «Текст завдання» й інші символи та літери.

3. Те ж саме стосується рисунків – зручніше вводити їх безпосередньо у тексті завдання, а не вставкою через файл з розширенням jpg або jpeg, що займає зайвий час.

1. Андрусенко Н. В. Дистанційне навчання в Україні // Дистанційне навчання як сучасна освітня технологія: матеріали міжвузівського вебінару 31 березня 2017 року. – Вінниця: ВТЕІ КНТЕУ, 2017. – С. 7-9.

2. Дистанційне навчання в глобалізованому світі: Міжвуз. науково-методичний семінар. Тези доповідей. – К.: Київський нац. торг.-екон. ун-т, 2021. – 101 с.

ОСОБЛИВОСТІ ВИКЛАДАННЯ ФАХОВИХ ДИСЦИПЛІН АНГЛІЙСЬКОЮ МОВОЮ

Г.В. Щолокова
Університет митної справи та фінансів

У сучасному глобалізованому світі володіння англійською мовою є важливим чинником конкурентоспроможності фахівця. Англійську мову називають глобальною мовою, адже саме нею насамперед користуються на міжнародному рівні у таких сферах, як бізнес, політика, туризм тощо. Зважаючи на перспективи набуття в Україні англійською мовою статусу мови міжнародного спілкування, особливої актуальності набуває необхідність запровадження / розширення практики викладання фахових дисциплін англійською мовою здобувачам, які навчаються у вітчизняних закладах вищої освіти.

Отже, йдеться насамперед про формування у здобувачів вищої освіти здатності ефективно здійснювати професійну комунікацію англійською мовою. Очевидно, що змістовна специфіка професійної комунікації може значним чином варіюватися, зважаючи на спеціальність (освітню програму).

Наприклад, якщо говорити про підготовку фахівців сфери обслуговування, то йдеться про те, що вони повинні вміти здійснювати комунікацію з іноземцями фактично на щоденній основі. При цьому вагомого значення набуває саме

міжкультурний контекст комунікації [2]. Водночас слід зазначити, що викладання фахових дисциплін англійською мовою (як один із складників процесу формування у студентів здатності ефективно здійснювати професійну комунікацію) видається таким, що має універсальний характер.

У західному науковому дискурсі існує спеціальний вислів, який характеризує ту ситуацію, коли англійську використовують як мову викладання, – "English as a Medium of Instruction (EMI)". Можливо говорити про цілий ряд аргументів на користь такого підходу: власне покращення здатності до комунікації, що у т.ч. збільшує шанси успішної професійної самореалізації майбутніх фахівців; можливість долучитися до глобального (який здебільшого є англомовним) освітньо-наукового дискурсу шляхом ознайомлення із науковою літературою мовою оригіналу та участі у міжнародних проєктах та заходах, наприклад у міжнародних конференціях тощо [1].

На нашу думку, в якості окремої значимої переваги, яку отримує здобувач вищої освіти, який мав можливість вивчати ряд фахових дисциплін англійською мовою, є подолання мовного бар'єра під час здійснення професійної комунікації. Очевидно, що для особи, яка не є носієм англійської мови, не є легким завданням, навіть за умов наявності відповідних знань, вільно комунікувати за допомогою англійської мови, оперуючи фаховою термінологією. Для здобувачів можливість на постійній основі слухати лекції англійською мовою; долучатися до обговорень як із викладачем, так і з іншими студентами; ознайомлюватися з англомовною літературою під час підготовки до занять; готувати та презентувати усні доповіді та виконувати письмові роботи англійською мовою сприяє органічному та комплексному залученню до усіх видів усної та письмової професійної комунікації в умовах саме навчання, а не вже безпосередньо професійної діяльності. Це дозволяє студенту адаптуватися до комунікації англійською мовою у комфортних умовах навчання, що у майбутньому дозволить легко реалізовувати сформовані навички у сфері практичної діяльності за фахом.

При цьому існують і проблемні аспекти, на які необхідно зважати, впроваджуючи концепцію викладання фахових дисциплін англійською мовою. Йдеться насамперед про належний рівень підготовки студентів. Існує така світова практика, як підготовчий рік (після закінчення школи та до вступу до закладу вищої освіти), протягом якого може відбуватися інтенсивна мовна підготовка. В якості ще одного важливого підготовчого інструмента може виступати запровадження спеціалізованої мовної обов'язкової дисципліни, в рамках якої буде відбуватися зокрема засвоєння базової професійної термінології, формування навичок перекладу фахової літератури з української мови на англійську та у зворотний бік. Окремо слід наголосити на тому, що мотивація здобувачів вищої освіти є визначально важливим чинником успішності опанування ними англомовних фахових дисциплін. Важлива роль у підвищенні мотивації студентів належить викладачеві. Відповідно, доцільним є й надання консультативної та методичної допомоги викладачам, які розпочинають викладати професійні дисципліни англійською мовою [1].

Отже, підводячи підсумки, слід зазначити наступне. Викладання фахових дисциплін англійською мовою має подвійний позитивний ефект. З одного боку, йдеться про формування у студентів власне іншомовної мовленнєвої компетентності. З іншого боку, йдеться про можливість розширення обсягу безпосередньо фахових знань. При цьому необхідно наголосити на тому, що досягнення вказаних позитивних результатів багато в чому обумовлюється ефективністю заходів, проведених на підготовчому етапі.

1. Бурмакіна Н. Проблеми імплементації фахових дисциплін з англійською мовою викладання у програму підготовки здобувачів вищої освіти. *Актуальні питання гуманітарних наук.* 2023. Вип. 59, том 1. С. 239–243. URL: http://www.aphn-journal.in.ua/archive/59_2023/part_1/37.pdf .

2. Шестель О., Старинець О., Заїка О. Засоби формування іншомовної комунікативної компетентності фахівців сфери обслуговування. *Актуальні питання гуманітарних наук.* 2019. Вип. 26, том 2. С. 179–183. URL: https://er.chdtu.edu.ua/bitstream/ChSTU/2979/1/%D0%A1%D1%82%D0%B0%D1%82%D1%82%D1%8F%2029.pdf .

USING THE LINUX CLASS IN CYBERSECURITY

D.I. Prokopovych-Tkachenko, Iu. Savchenko, N.O. Sugak
University of Customs and Finance

With the development of technology and the computerization of society, the need to study computer science and information technology is growing. Today, these fields have already become an integral part of many other industries, such as medicine, science, business, law and politics. In a world where almost all processes are being transferred to electronic form, it is necessary to have a deep understanding of the technologies underlying these processes.

In such a world, it is especially important to ensure cybersecurity, as technology can be used by malicious actors for crime and espionage. This can lead to catastrophic consequences, including the loss of confidential information, disruption of critical infrastructure, and threats to human life. Therefore, in addition to studying computer science and information technology, it is also necessary to focus on the development and application of effective cybersecurity measures.

All this has made the study of computer science and information technology an important task today.

Running and maintaining computer systems, including servers, are also key aspects of creating an efficient and secure infrastructure. Servers provide storage and access to large amounts of data and applications, and are used in a variety of industries, from web hosting and data storage to scientific research and financial transactions. Ensuring the security of servers is an important task, as they can be attacked by intruders trying to gain unauthorized access to data or compromise the system.

Thus, the study of computer science and information technology is becoming increasingly important in a world where more and more processes depend on technology. Cybersecurity and server support are key components of these fields, making them particularly interesting to learn and use. In this article, we'll look at creating a Linux classroom to show how computer science helps create the powerful and secure infrastructure needed for the modern world.

Software packages are an important part of an operating system and provide functionality for various tasks.

The main software packages in the operating system include the following:

- Package Management System - this package allows users to install, update and uninstall applications from the operating system.
- Text Processing System - this package allows users to edit and process text files, including text editors, word processing applications, and others.
- Network Protocol System - this package provides the ability for the operating system to interact with network devices and resources, including network drivers, protocol stacks, and others.
- Graphics System - this package allows users to work with graphics, including graphical user interfaces, graphics device drivers, and others.
- Audio System - This package allows users to work with audio, including audio device drivers and applications for recording and playing audio.

- Database System - this package allows users to create and manage databases.
- Security System - this package protects the operating system and user data from unauthorized access.
- Development Tool System - this package contains tools for software development, such as compilers and more.

A graphical user interface (GUI) is a set of tools that allow a user to interact with an operating system and software using graphical elements such as buttons, menus, and windows.

GNOME is a graphical user interface based on the GTK+ library developed for the Linux operating system. GNOME offers a graphical user interface with a simplified and clear design that makes it easy to navigate and use the system.

KDE is another popular graphical user interface that runs on the Linux operating system and uses the Qt library. KDE offers more advanced features to the user, such as customization of the desktop and taskbar.

XFCE is another graphical shell for Linux that has low system resource requirements and is very fast and efficient. XFCE offers the user the ability to customize the desktop and window manager, and allows the use of various themes and taskbars.

Linux has a number of technical advantages over other operating systems. One of the main arguments in favor of Linux is its open-source code, which allows users to modify and customize the system to their needs. In addition, Linux is highly stable and secure, thanks to its system of user rights and the use of protection against viruses and other threats. Linux is also known for its efficiency and speed, which is especially important for server applications. It has built-in support for network devices and development and programming tools, making it popular with software developers. All of these advantages make Linux a viable choice for many users and businesses.

Linux is an efficient operating environment due to its special architecture that allows it to run on simple hardware. This means that Linux does not require such high system characteristics as well-known operating systems such as Windows or MacOS. As a result, Linux can be installed and used on low-cost, low-specification hardware, which significantly reduces the cost of ownership and management.

In addition, Linux is more stable and efficient because it uses optimized data and memory algorithms to deliver high performance on low-powered machines. This makes it possible to use Linux on servers that operate in continuous operation and ensure stable systems for many years.

Compared to its direct competitors, namely Window and MacOS, Linux has the aforementioned open-source advantage, which allows it not only to be customized for specific tasks, but also to track any processes, which other solutions cannot, making it more secure. Linux has a lot of free and freeware software, which allows users to install the applications they need for free and without restrictions.

Linux uses the ext4 file system, which is faster and more reliable than Microsoft and Apple file systems.

The main feature of ext4 is its support for large files and high performance. It uses a number of new technologies that make it more reliable and efficient than older file systems.

One of the key features of ext4 is the dynamic indexing of file blocks, which reduces the time it takes to access data. In addition, ext4 supports block allocation in large chunks, which allows for more efficient use of disk space.

Another important feature of ext4 is metadata logging, which provides a higher level of data security in the event of a system crash or other unforeseen events.

In addition, ext4 supports interval file defragmentation, which reduces disk fragmentation and improves performance.

Linux is known for its high resistance to cyber-attacks, which makes it particularly attractive for use in this area. Linux is used in many areas of cybersecurity, including both

national and corporate security. Linux also has a built-in network security system that allows you to set up firewalls and deny access to certain resources. Open interfaces provide the ability to change settings. Let's take a look at how Linux can be used in information security systems.

Linux has a built-in security mechanism that makes it more resistant to malware than other operating systems.

One of the key elements of protection against malware is a permission system that allows you to restrict user access to certain files and resources. In addition, Linux allows you to set access rights to files and directories based on their owner, user group, and other parameters.

Another important element of security is the use of package managers to install programs. Package managers provide digital signature verification of programs, which allows you to make sure that programs are installed from official sources and avoid installing malware.

Another security tool is the use of network filters. For example, iptables allows you to configure filtering rules for network traffic passing through the system. This can help protect the system from attacks from the network.

Linux also has a built-in SELinux (Security - Enhanced Linux) mechanism that allows you to protect the system from vulnerabilities that can be used to perform malicious actions. SELinux includes a number of modules that allow you to control access to files, network resources, system services and other elements of the operating system.

Another security feature in Linux is the use of virtualization. Virtualization allows you to run separate, isolated instances of the operating system on a single physical server, which reduces the risk of unauthorized access to the system.

Linux also has a built-in software packaging system, Package Kit, which provides updates and installation of malware-protected software. To scan files for viruses, antivirus programs such as Clam AV are used, which are included in various Linux distributions.

Linux has a lot of system monitoring tools, but they all have a common goal - to prevent system hacking. This is the first principle of their work.

The second principle is notification of detected problems. Security monitoring tools allow you to set up a notification system for operators, administrators, and other responsible persons to detect potential threats and vulnerabilities.

The third principle is responding to detected problems. Security monitoring tools help to provide an automatic or manual response to detected threats. This can include blocking access to resources, disabling potentially harmful services, and more.

Such tools can be used to monitor both individual computers and the network as a whole. They allow for continuous security monitoring, which helps to detect and neutralize threats at an early stage.

In Linux, it is possible to encrypt disc space using various tools, such as dm-crypt, LUKS, VeraCrypt and others. Disk space encryption means that the data on the disc is encrypted and becomes unreadable without the correct key. This ensures a high level of data protection in case of loss, theft, or stealing of a computer.

Disk space encryption is used in a variety of areas where sensitive data is stored, such as financial documents, medical records, personal customer data, commercial information, and more. This is especially important for organizations that process sensitive information or are subject to personal data protection legislation.

For example, in the finance and banking industry, where a lot of customer financial data is stored, disk space encryption is used to protect against unauthorized access to this data. Disk space encryption can also be used in government agencies, such as military organizations, to protect against disclosure and unwanted access to classified information.

CONCLUSIONS

As Linux is freely distributed and open-source software, it has found its way into many

areas, including cybersecurity. Linux has numerous technical advantages over other operating systems, such as high stability, low vulnerability, and a large number of security monitoring tools. A feature of Linux is also the ability to encrypt disc space, which allows you to keep your data safe. The use of Linux in cybersecurity helps protect information from unauthorized access, prevent external attacks and ensure network security.

Thus, the use of Linux in cybersecurity can be an important component of protecting data and networks from malware and external attacks. To do this, it is worth paying attention to the technical advantages of Linux, using security monitoring tools, and using the disk space encryption capabilities to keep important data safe.

ECONOMIC SECURITY AS AN ELEMENT OF NATIONAL SECURITY

Iu. Savchenko, D.I. Prokopovych-Tkachenko, I.I. Zhulkovska
University of Customs and Finance

For the current state of Ukraine's economy as an independent state and its establishment as a member of the global community, the most pressing issues are ensuring sustainable socioeconomic development, forming a mechanism to counter internal and external threats, and developing a system of international economic interdependence. The totality of these problems and the sequence of their solution are closely related to the category of "security", and thus to the national security of the state as a whole.

Investment interest in cryptocurrencies is not yet high enough to have a significant impact on the global economy, but the situation may change in the future, and crypto economics will contribute to the development of the global economy. Blockchain technology can play an important role in making the global financial system and the economy as a whole more open and efficient.

Cryptocurrency is a type of digital currency, the issue and accounting of which is based on asymmetric encryption and the use of various cryptographic security methods, such as Proof- of-work and/or Proof-of-stake. The system operates in a decentralized manner in a distributed computer network.

Today, cryptocurrencies are not only an objective reality, but also a significant economic factor. As already mentioned, there is no consensus in the scientific community or at the level of governments of different countries on which category cryptocurrencies should be classified.

Cryptocurrencies, as the latest electronic means of payment, currently have no legal basis in Ukraine, and therefore no regulatory definition. There is a general understanding that cryptocurrencies are units of value that are stored on electronic devices, used as means of payment, and transactions are carried out using cryptography.

To date, modern scholars have researched and introduced the concept of "national security of Ukraine - protection of state sovereignty, territorial integrity, democratic constitutional order and other national interests of Ukraine from real and potential threats" [3].

Ukrainian legislation considers national security to be the protection of vital interests of a person and a citizen, society and the state, which ensures sustainable development of society, timely detection, prevention and neutralization of real and potential threats to national interests in the areas of law enforcement, anti-corruption, border management and defense, migration policy, healthcare, education and science, scientific, technical and innovation policy, cultural development of the population, ensuring freedom of speech and expression, and ensuring the protection of the rights of the people to freedom of association.

Constant changes in internal and external factors of the national economy development make it important to study the issue of ensuring the economic security of the State.

In the national security system, economic security performs certain functions, i.e.,

carries a significant functional burden. Its essence lies in the fact that it is the material basis of national sovereignty, which formulates real opportunities for ensuring other types of security. In other words, economic security is the basis for the functioning of all its other elements that make up this system [1].

In foreign and domestic literature, there are many approaches to the interpretation of the concept of economic security of the state using the following characteristics [4, p. 40 - 41]:

- Stability and sustainability, counteraction to internal and external threats, which means the strength and reliability of links between all elements of the economic system, stability of economic development of the state, resistance to deterrence and neutralization of destabilizing factors;
- economic independence, which primarily characterizes the ability of any economic security entity to independently make and implement strategic economic and political decisions for development, and the ability to use national competitive advantages to ensure stability and development;
- self-reproduction and self-development. This characteristic implies the creation of the necessary conditions for an effective economic policy and expanded self-reproduction, ensuring the competitiveness of the national economy on the world stage;
- national interests. This characteristic determines the ability of the national economy to protect national economic interests.

National economic interests form the basis of the economic policy pursued by the state, an important part of which is ensuring economic security, one of the most important functions of the state. This is a guarantee of the country's independence, a condition for the stability and effective functioning of society.

Therefore, taking into account the research of scholars, it can be concluded that national security will be incomplete without a comprehensive assessment of the economy, its strength and reliability, taking into account the presence of real and potential external and internal threats. Consequently, the economy is one of the vital activities of an individual, society and the state, and ensuring economic security is among the most important national priorities in the fight against crime.

There is a fairly wide range of interpretations of the concept of "cryptocurrency" by official bodies of different countries. There is a certain regularity in this diversity: in one form or another, cryptocurrencies are nevertheless recognized as means of exchange, and in some cases, even as means of payment.

The emergence of cryptocurrencies was made possible by cryptography and the principle of cryptocurrency circulation is based on blockchain technology, but these aspects are the technical side of the issue. Cryptography is only a mechanism, not the essence; a mechanism that has nothing to do with the legal nature or legal status of cryptocurrencies. Cryptography has long been used to encrypt information, and cryptocurrencies are just a by-product of this. The same blockchain technology is used in many other areas, for example, in state registries, such as the State Land Cadaster of Ukraine. Moreover, the NBU has announced the possibility of issuing an e-hryvnia based on blockchain technology, and it is clear that under the terminology of both of the above draft laws, the e-hryvnia will not fall under the definition of a cryptocurrency, even if cryptography and blockchain technology were used in its creation, as one of the main features of cryptocurrencies such as Bitcoin is decentralization and the absence of a single issuer.

1. Law of Ukraine "On National Security of Ukraine" No. 2469-VIII of 21.06.2018.
2. Malyshko V.M. Actual problems of economic security in the system of national security of Ukraine. Legal Bulletin. Air and Space Law. 2015. № 4. c. 129 - 133.
3. On the Fundamentals of National Security Law of Ukraine - access mode: http:// zakon2.rada.gov.ua/l aws/ show/96415.
4. Skoruk O.V. Economic security of the state: essence, components and problems of

ensuring. Scientific Bulletin of Uzhhorod National University: Ser: International economic relations and world economy. Uzhhorod. 2016. Issue 6. Part 3. pp. 39 - 42.

ПРОГНОЗ РІВНЯ ЗАРОБІТНОЇ ПЛАТИ В ГАЛУЗІ ОСВІТИ УКРАЇНИ В СУЧАСНИХ УМОВАХ ГОСПОДАРЮВАННЯ

Н.В. Майбородіна, В.П. Герасименко
ВП НУБіП України "Ніжинський агротехнічний інститут"

Заробітна плата – це винагорода, обчислена, як правило, у грошовому виразі, яку за трудовим договором роботодавець виплачує працівникові за виконану ним роботу.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства [1].

Заробітна плата є основним показником, який визначає рівень матеріального добробуту освітян. Належна оплата праці є не лише запорукою матеріального добробуту освітян, а й впливає безпосередньо на якість освіти в Україні.

Метою даного дослідження є прогноз заробітної плати освітян на перший квартал 2023 року. З цією метою було використано дані за чотири квартали 2022 року з офіційного сайту Державної служби статистики України [2]. Дані наведено в таблиці 1.

Таблиця 1. Середньомісячна заробітна плата за видами економічної діяльності за квартал у 2022 році
(у розрахунку на одного штатного працівника)

Вид діяльності	I квартал, грн	II квартал, грн	III квартал, грн	IV квартал, грн
Освіта	11431	11907	11258	13429

Для побудови моделі був обраний табличний процесор Excel, в якому вже є вбудовані функції та інструменти аналізу статистичних даних.

У багатьох практичних випадках моделювання економічних явищ і процесів лінійними моделями дає цілком задовільний результат і може використовуватися для аналізу і прогнозування. Однак внаслідок різноманіття і складності економічних явищ та процесів обмежитися застосуванням тільки лінійних моделей неможливо. Багато економічних залежностей, як свідчить економічна теорія, не є лінійними по суті, і тому їх моделювання лінійними залежностями, безумовно, не дасть позитивний результат. У цьому випадку необхідно використовувати нелінійні моделі [3, с.73].

Під час дослідження був проведений аналіз з вибору лінії тренду, яка відповідає найбільшому значенню величини достовірності апроксимації R^2. Результатом дослідження є вибір поліноміальної функції третього степеня, для якої значення величини достовірності апроксимації $R^2 = 1$ (рис. 1).

Емпірична модель заробітної плати освітян має вигляд

$$y = 657{,}21x^3 - 4505{,}2x^2 + 9390{,}6x + 5888{,}4. \quad (1)$$

Теоретична модель заробітної плати освітян має вигляд

$$y = 657{,}21x^3 - 4505{,}2x^2 + 9390{,}6x + 5888{,}4 + u, \quad (2)$$

де u – випадкова (стохастична) складова моделі.

Використовуючи знайдену модель заробітної плати (1) освітян можна одержати прогноз на перший квартал 2023 в розмірі 22362 грн.

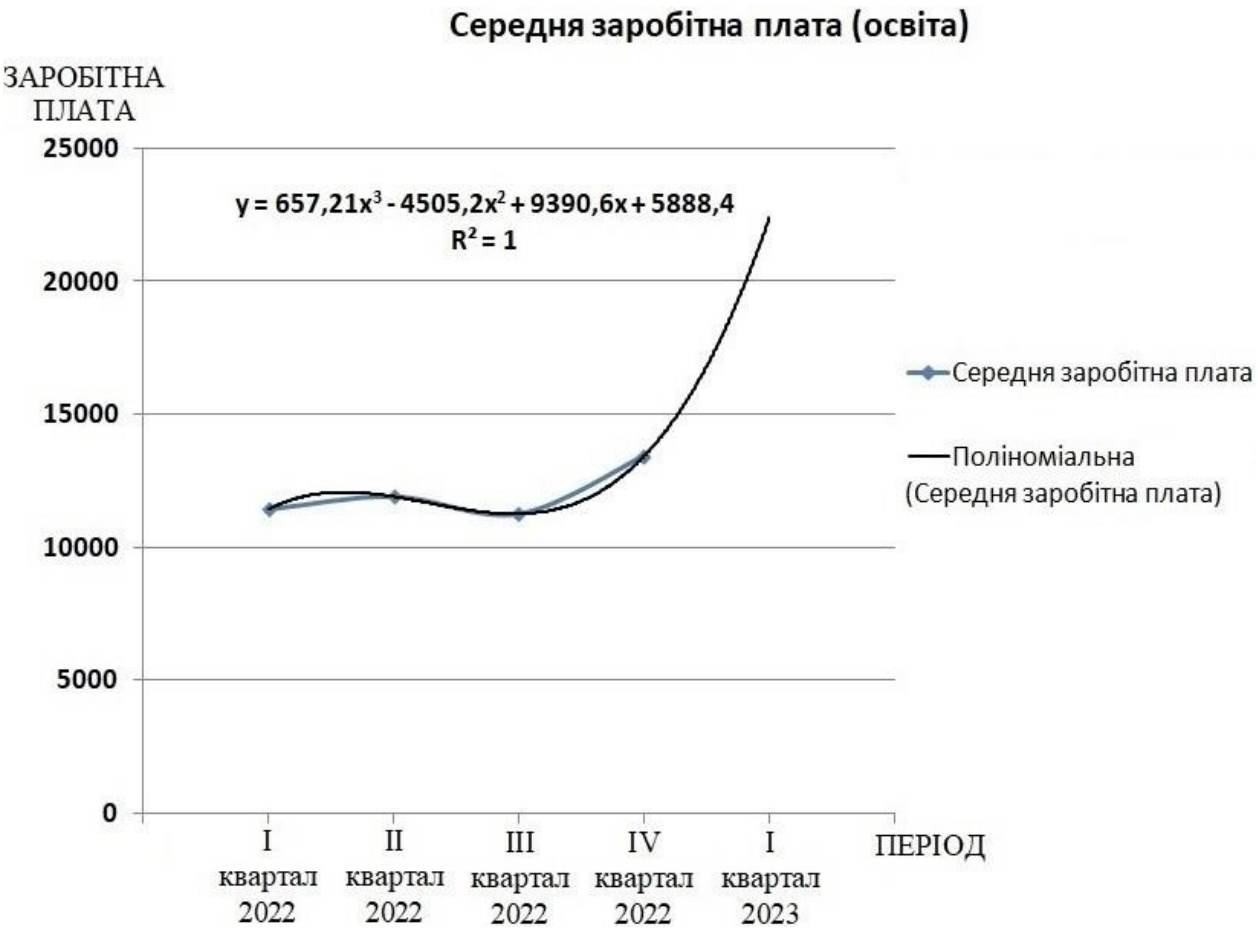


Рис. 1 Модель середньої заробітної плати освітян

Але на початку листопада 2022 року Верховна Рада України прийняла закон «Про Державний бюджет на 2023 рік», у якому основні видатки передбачено на обороноздатність України та соцзабезпечення [4].

«В умовах воєнного стану не може бути по-іншому. Та навіть попри складні часи, Уряд знайшов можливість збільшити видатки державного бюджету МОН на 2023 рік до другого читання на 555 млн грн.», –прокоментував Міністр освіти і науки України Сергій Шкарлет. Дані про бюджет для розвитку освіти і науки України зображені на рис 2.

БЮДЖЕТ РОЗВИТКУ ОСВІТИ І НАУКИ	*** у гривнях**			
ЗАГАЛЬНИЙ ОБСЯГ ВИДАТКІВ МОН	**139,3 МЛРД 2021**	**153,7 МЛРД 2022**	**131,0 МЛРД 2022 (після секвестру)**	**122,1 МЛРД 2023**
СУБВЕНЦІЇ	**103,7 МЛРД**	**112,9 МЛРД**	**97,7 МЛРД**	**90,3 МЛРД**
Освітня	**99,6**	**108,0**	**97,2**	**87,5**

для підтримки осіб з ООП	**млрд 0,50 млрд**	**млрд 0,50 млрд**	**млрд 0,45 млрд**	**млрд 0,30 млрд**
забезпечення пожежної безпеки в школах		**1,50 млрд**		
облаштування безпечних умов у ЗЗСО				**1,5 млрд**
придбання шкільних автобусів				**1,0 млрд**
ДЕРЖАВНІ ВИДАТКИ	**35,5 МЛРД**	**40,9 МЛРД**	**33,3 МЛРД**	**31,8 МЛРД**
підготовка кадрів закладами вищої та фахової передвищої освіти	**25,6 млрд**	**27,8 млрд**	**25 млрд**	**22,5 млрд**
виплати академічних стипендій	**3,94 млрд**	**5,14 млрд**	**4,6 млрд**	**4,2 млрд**
забезпечення діяльності НФД, грантової підтримки наукових досліджень і науково-технічних (експериментальних) досліджень	**2,2 млрд**	**2,5 млрд**	**1,5 млрд**	**2,0 млрд**

Уряд збільшив видатки до II читання на 555 млн грн
50 млн – забезпечення здобуття професійної освіти
20 млн – продовження навчання молоді
30 млн – проведення Всеукраїнських заходів із позашкільної освіти
215 млн – здійснення зовнішнього оцінювання та моніторинг якості освіти
150 млн – організація здобуття освіти за дистанційною формою
90 млн – для Національного фонду досліджень

Рис. 2 Бюджет для розвитку освіти і науки України

На основі одержаних дані проведених досліджень можна зробити наступні висновок, що заробітна плата освітян у першому кварталі 2023 року має підвищитися. Але враховуючи введення воєнного стану в Україні і необхідності збільшення витрат на обороноздатність України, можливо, що заробітна плата залишиться на рівні четвертого кварталу 2022 року з незначним підвищенням.

1. Закон України "Про оплату праці" (Відомості Верховної ради України (ВВР), 1995, №17, ст. 121 [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/108/95-%D0%B2%D1%80#Text.
2. Офіційний сайт Державної служби статистики України [Електронний ресурс] – Режим доступу: http://www.ukrstat.gov.ua.
3. Майбородіна Н.В. Економетрика: навчальний посібник / Майбородіна Н.В. – Ніжин: ПП Лисенко М.М., 2021. 280 с.
4. Офіційний сайт Міністерства освіти і науки України [Електронний ресурс] – Режим доступу: https://mon.gov.ua/ua/news/derzhbyudzhet-na-2023-rik-vidatki-na-osvitu-ta-nauku.

ЗМІСТ