ІНСТИТУТ
СХІДНОЇ ЄВРОПИ

THE EASTERN-EUROPEAN
INSTITUTE

м. Львів, 79008, вул. Тесленка, д.2; тел. 097-496-22-40
www. easterneurope.nethouse.ua; E-mail: ukrainoznavezz@ukr.net

Науково-технічний Відділ Інституту Східної Європи.

Завідувач, Ігор Васильович Огірко - доктор фізико-математичних наук, професор, заступник директора з науково-технічних проблем Інституту Східної Європи.

APPLIED MATHEMATICS FOR MATHEMATICS

Ihor Ohirko–doctor of sciences, professor, Kazimierz Pułaski University of Technology and Humanities in Radom

Ігор Огірко – доктор фізико-математичних нау, професор, заступник директора з науково-технічних прблем Інституту Східної Європи.

Reviewer Volodymyr Yuzevych - doctor of sciences, professor, Kujawsko-Pomorska Szkola Wyzsza (Bydgoszcz, Poland)

Numerical methods [1] consist in solving mathematical problems by means of operations on numbers. The results obtained in this way are generally approximate, however, the accuracy of calculations can be predetermined and selected depending on the needs.Numerical methods are used when the problem in question does not have a general analytical solution, or the use of such solutions is cumbersome due to their complexity.A very important problem in the numerical calculations is the occurrence of numerical errors. In general, errors can be presented in two forms: as absolute errors and relative errors. There are three groups of errors associated with the solution of a numeric task: input errors, truncation errors and rounding errors.When implementing the algorithm, one should ask the basic question whether our algorithm is numerically correct and whether the task is well conditioned. The algorithm is numerically stable when increasing the accuracy of calculations, we can designate any existing solution to the task. The error in the numerically stable algorithm is at the level of the inevitable error of the solution resulting from the approximate representation. Numerical stability[1-3] is the basic, minimal property that should be required of the algorithm.However, the essential requirement that we will require from the algorithm is numerical correctness. A numerically correct algorithm is one for which the calculated solution is an exact solution for tasks with slightly disturbed data. Slightly disturbed data means data with a disorder at the level of representation errors. This is in turn the property that characterizes the best algorithms. The correct numeric algorithms are a subset of a set of stable numeric algorithms.The conditioning of the task is the sensitivity of the result of the task to the small relative disturbances of the initial task data. The task is well conditioned if small relative changes in data give small relative changes in results. In turn, if the introduction of small relative changes in the task data causes large relative changes in the solution, this task is called badly conditioned.Task conditioning can be measured by means of determinants of the task. The high value of the conditioning factor indicates the poor conditioning of the task. The method of calculating the conditioning factors depends on the type of the numerical task.Interpolation – a numerical method involving the determination in the given range of the so-called an interpolation function that assumes predetermined values in it at set points called nodes. It is often used in experimental sciences, where there is usually a finite number of data to determine the relationship between quantities and to simplify complex functions, eg during numerical integration. Interpolation is a special case of numerical methods of approximation.Approximation– the process of determining approximate solutions based on known solutions that are close to solutions accurate in a strictly defined sense. Typically, beings complicated by simpler entities are approximated. Often used when looking for solutions for data obtained by empirical methods, which may be burdened with errors.System of linear equations – conjunction of a certain number of linear equations, i.e. first order equations.The theory of systems of linear equations is a branch of linear algebra which underlies modern mathematics. The computational algorithms are dealt with by the department called numerical linear algebra, while the methods themselves play an important role in engineering, physics, chemistry, computer science and economics. It often approximates more complicated systems of nonlinear equations with much simpler systems of linear equations.Systems of linear equations are usually considered over bodies; although this makes sense already in the case of rings, then solving such systems is much more difficult. It is further assumed that all factors belong to a fixed body.Numerical integration [3-6] – a numerical method involving the approximate calculation of definite integrals. The term numerical quadrature, often simply quadrature, is a synonym for numerical integration, in particular with regard to one-dimensional integrals. The two- and higher-dimensional integrals are sometimes called volumes, although the word squared also has the meaning for integration in higher dimensions.Simple numerical integration methods rely on the approximation of the integral by means of the appropriate sum of the weighted value of the integral function in several points. To get a more accurate approximation, the integration interval is divided into small fragments. The final result is the sum of the integral estimations in the individual sub-ranges. Most often, the interval is divided into equal subintervals, but more sophisticated algorithms are able to adjust the step to the speed of function variation.Ordinary differential equation – an equation in which there are constant, unknown functions and derivatives of unknown functions. In ordinary differential equations, unknown functions depend on one independent variable.

References:

[1] Fronczak P. „ Prezentacja z wykładu Metody numeryczne" Zakład Fizyki i Układów Złożonych Politechniki Warszawskiej

[2] https://pl.wikipedia.org/wiki/Interpolacja_(matematyka)

[3] https://pl.wikipedia.org/wiki/Aproksymacja

[4] https://pl.wikipedia.org/wiki/Uk%C5%82ad_r%C3%B3wna%C5%84_liniowych

[5] https://pl.wikipedia.org/wiki/Ca%C5%82kowanie_numeryczne

[6]https://pl.wikipedia.org/wiki/R%C3%B3wnanie_r%C3%B3%C5%BCniczkowe_zwyczajne

MATERIALS AND NUMERICAL METHODS

Numerical methods are the way to solve complex mathematical problems using computational tools provided by popular programming languages. Numerical methods are one of those areas of applied mathematics, whose practical application is widespread. They are used when the problem is not an analytical solution at all, or the use of such solutions is cumbersome because of their complexity or for other reasons (eg the use of Gaussian elimination instead of calculating solutions of the system of equations by the determinants is applied accordingly. that it is better conditioned numerically, and not because there is no pattern. The results obtained are generally approximate, but the accuracy of the calculations may be predetermined and adjusted according to needs.Numerical modeling is today one of the most promising and developing the fields of engineering. Its main advantage is the possibility of obtaining a solution of the given a problem that would otherwise be solved by experimental methods. In recent years, the rapid development of nanotechnology has been observed. Nanotechnology is a field of study dealing with materials and systems whose structures and elements exhibit peculiar characteristics well developed physically, chemically and biologically,Their processes are caused by their nanoparticles. The goal of nanotechnology is to use these properties by achieving control on the atomic and molecular levels of molecules and developing effective their production and use. The behavior of the particles in the "nanoscale" is unpredictable compared to that observed in larger molecules. Ability to reduce particle size to nanoscale leads to exceptional properties. Designing such However, devices and materials require the development of adequate computing tools.

Numerical integration is a numerical method that approximates the integral calculations. The term quadratic, often simply quadrature, is synonymous with numerical integration, in particular with respect to one-dimensional integers. Two- and higher-dimensional integrals are sometimes called cubes, although the word quadrature also has significance for integration in higher dimensions.Simple methods of numerical integration consist in approximating the integral by the sum of the weighted values of the integrated function at several points. For a more accurate approximation, the integration interval for small fragments is divided. The final result is the sum of the estimates of the integrals in the individual subdivisions. The compartment is usually divided into equal subtracts, but more sophisticated algorithms can adapt the step to the rate of variability of the function. The methods of numerical integration include: Method of rectangles, Trapezoid method, Parabolic Method, Random methods.

In rectangular integration, we use the definition of the integral of Riemann, where the value of the integral is interpreted as the sum of the fields of the areas under the curve in the given integration interval <x_p, x_k>. We sum this sum with the sum of the fields of appropriately selected rectangles. The procedure is as follows:

The integral of x <x, x_k> is divided into n equally distant points x_1, x_2, ..., x_n. These points are determined simply by the formula:

for: i = 1,2,...,n

$$x_i = x_p + \frac{i}{n}(x_k - x_p)$$

We calculate the distance between two adjacent points - this will be the basis of each rectangle:

$$dx = \frac{x_k - x_p}{n}$$

For each point determined in this way we calculate the value of the function f (x) at this point:

$$f_i = f(x_i), \qquad for\ i = 1,2,\dots,n$$

We calculate the sum of the product of the determined function values by the distance dx between two adjacent points - this is the sum of the fields of the individual rectangles bounded by the function graph:

$$S = f_i dx + f_2 dx + \cdots + f_n dx$$

and after bringing out the common factor before the bracket:

$S = dx(f_1 + f_2 + \cdots f_n)$

The sum obtained is the approximate value of the integral of the denoted function f (x) in the interval <x_p, x_k>.

$$\int_{x_p}^{x_k} f(x)dx \approx \frac{x_k - x_p}{n} \sum_{i=1}^{n} f\left(x_p + i\frac{x_k - x_p}{n}\right)$$

The rectangle method described in the previous chapter is not very accurate because the fields used in the rectangles misrepresent the area under the curve. A much better solution is to use trapezoids instead of them with dx heights and bases equal to the value of the function at the endpoints respectively. The same principle does not change.

The integral of x <x, x_k> divides n + 1 equally at distant points x_0, x_1, x_2, ..., xn. These points are determined simply by the formula:

for: $i = 0,1,2,...,n$

$$x_i = x_p + \frac{i}{n}(x_k - x_p).$$

We calculate the distance between two adjacent points - it will be the height of each trapeze:

$dx = \frac{x_k - x_p}{n}.$

For each point determined in this way we calculate the value of the function f (x) at this point:

$$f_i = f_{(x_i)},\ for: i = 1,2,\dots,n.$$

The area under the function graph is approximate n trapezoid fields. The i-th trapezoid is calculated according to the formula:

for: i=1,2,...,n

$$f_i = f(x_i),\ for: i = 1,2,\dots,n.$$

The approximate value of the integral is the sum of the fields of all the trapezoids thus obtained:

$$S = P_1 + P_2 + \cdots + P_n$$

Derived at the end of the formula is the basis for the approximate calculation of the integral in the trapezoid method.

$$\int_{x_p}^{x_k} f(x)dx \approx \frac{x_k - x_p}{n}\left(\sum_{i=1}^{n-1} f(x_p + i\frac{x_k - x_p}{n} + \frac{f(x_p + f(x_k))}{2}\right)$$

Literature

1. Weisstein, Eric W. "Cubature". MathWorld.
2. Jump up^ http://jeff560.tripod.com/q.html

3. Jump up^ Mathieu Ossendrijver (Jan 29, 2016). "Ancient Babylonian astronomers calculated Jupiter's position from the area under a time-velocity graph". Science. 351: 482–484. doi:10.1126/science.aad8085. PMID 26823423.
4. Jump up^ Leader, Jeffery J. (2004). Numerical Analysis and Scientific Computation. Addison Wesley. ISBN 0-201-73499-0.
5. Jump up^ Briol, François-Xavier; Oates, Chris J.; Girolami, Mark; Osborne, Michael A. (2015-06-08). "Frank-Wolfe Bayesian Quadrature: Probabilistic Integration with Theoretical Guarantees". arXiv:1506.02681.
6. Philip J. Davis and Philip Rabinowitz, Methods of Numerical Integration.
7. George E. Forsythe, Michael A. Malcolm, and Cleve B. Moler, Computer Methods for Mathematical Computations. Englewood Cliffs, NJ: Prentice-Hall, 1977. (See Chapter 5.)
8. Press, W.H.; Teukolsky, S.A.; Vetterling, W.T.; Flannery, B.P. (2007), "Chapter 4. Integration of Functions", Numerical Recipes: The Art of Scientific Computing (3rd ed.), New York: Cambridge University Press, ISBN 978-0-521-88068-8
9. Josef Stoer and Roland Bulirsch, Introduction to Numerical Analysis. New York: Springer-Verlag, 1980. (See Chapter 3.)
10. Boyer, C. B., A History of Mathematics, 2nd ed. rev. by Uta C. Merzbach, New York: Wiley, 1989 ISBN 0-471-09763-2(1991 pbk ed. ISBN 0-471-54397-7).
11. Eves, Howard, An Introduction to the History of Mathematics, Saunders, 1990, ISBN 0-03-029558-0,

METHODS OF ELEMENTS COMPLETED

The Finite Element Method is on today's one of the basic methods of computer assisted computing engineering . FEM is an advanced method of solving systems of differential equations, based on the division of the domain into finite elements, for which the solution is approximated by specific functions, and performing actual calculations only for nodes of this division.

Finite Element Method is one of the methods of discretization of systems geometric continuous, i.e., dividing the continuum into a finite number of subareas. To above, the idea of the method assumes modeling even very complex constructions (parts and bands) through their representation using geometrically simple elements components, even considering material discontinuities and multiphases. The main assumption of MES is the division of a continuous geometric model (Fig. 1) into finite elements combining in the so-called nodes, resulting in the creation of the model geometric discrete. Once again, it should be emphasized that the effect of discretization is transformation of a system with an infinite number of degrees of freedom (the ability to change values specified coordinate) to the form of a system with a finite number of degrees of freedom (SSW).

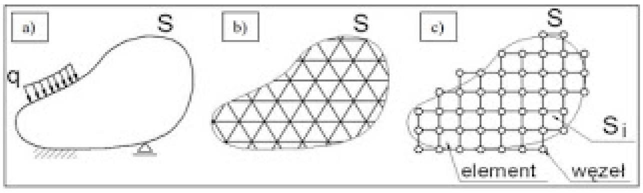


Fig. 1. Discretization of the continuous model - transformation into a set (grid) of elements finite: a) continuous geometric model, b) ideal discrete model, c) model discrete calculation

Any other calculation is also discredited with MES calculation physical quantities, represented in the system by means of continuous functions. When discretizing a particular size physical effort to maximize its discrete and continuous form using approximate methods. To solve a particular problem of mechanics pay attention to the physical environment of the system, i.e. in the case of a system shown in Fig. 1a: extortion and restraint.

Modern CAE engineering applications in which MES is applied consist of three mutually cooperating modules, which are: a) preprocessor ,b) solver,c) postprocessor.

From a practical point of view, before discretising the CAD model, it should be subjected appropriate simplification, during which points irrelevant to point view of the analyzed phenomenon, eg radii, phases, openings, tilt, etc.The geometry of the analyzed systems can be significantly different from each other. They can be 1-dimensional, 2-dimensional and 3-dimensional objects dimensional. In view of the above, during the preparation of FEM analysis available there are many types of finite elements, and the criteria for their division are included you can:the number of dimensions that an element can be described (Figure 4),geometric shape,type and degree of polynomial of the assumed shape function of a finite element, number of nodes in the element,types of general constraints imposed on a finite element.

Discretization of the mesh may be useful when discretizing the model elements, in areas particularly exposed to boundary conditions. However, it should be remember that the so-called "Densifying the grid indefinitely", i.e. bringing it to generate very small finite elements in the given regions may even imply a distortion of the value of the unknowns sought.

It should also be mentioned that the division of the geometric continuum into finite elements it can be done in a manual or semi-automatic manner.

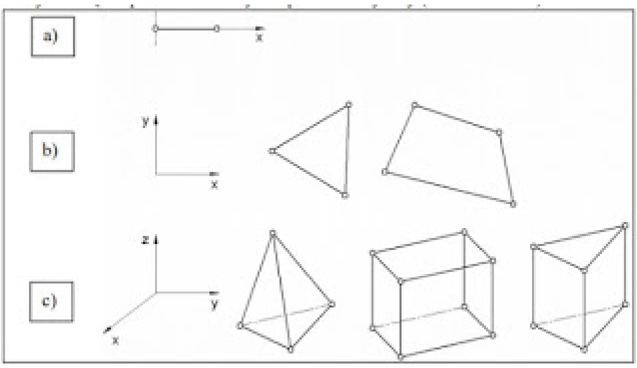


Fig. 4. Schematic diagrams of selected finite elements: a) 1D, b) 2D, c) 3D.

Literature

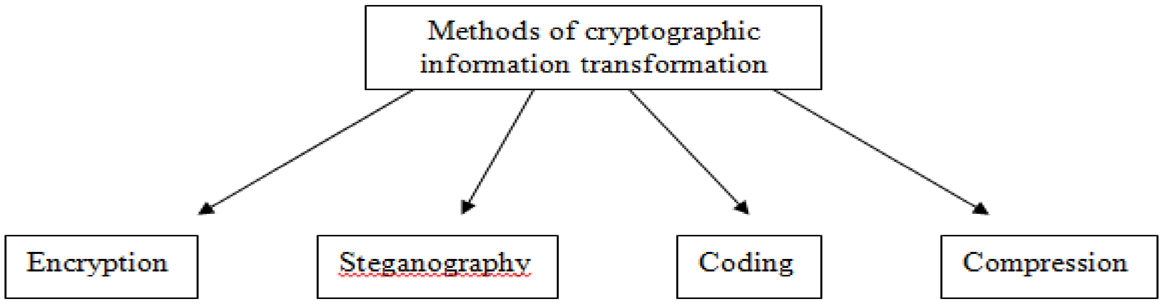
1. Dacko M, Borkowski W., Dobrociński S, Niezgoda T., Wieczorek M.: Metoda Elementów Skończonych w mechanice konstrukcji, Arkady, Warszawa 1994

2. Rakowski G., Kacprzyk Z.: MES w mechanice konstrukcji, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa 2005

3. Rusiński E., Czmochowski J., Smolnicki T.: Zaawansowana metoda elementów skończonych w konstrukcjach nośnych, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2000

Methods and means of information protection

The recent progressive impact of information technology on virtually all spheres of human activity causes a gradual growth of requirements for telecommunications systems and telecommunications devices. This is due to the fact that these systems are still the main means of information exchange, and the quality of their work is a determining factor in the effectiveness of most information technologies. The most important component of the quality of functioning of telecommunication systems is the quality of information security. The provision of this component currently faces a number of challenges, chief among them the contradiction between the potential of existing approaches and the ever-growing demands for data protection. The potential failure of these approaches to meet changing requirements explains the relevance of the direction of research searching for fundamentally new approaches that allow solving these problems.Cryptographic methods of information protection are a powerful weapon in the struggle for information security.Cryptography is a set of data transformation methods designed to make data useless to an attacker. The problems of protecting the confidentiality and integrity of information are closely related, so the methods of solving one of them are often applicable to other solutions.There are various approaches to the classification of methods for converting cryptographic information. Turning to the initial information on the exposure, the methods for converting cryptographic information can be divided into four groups.The process of encryption consists in carrying out reversible mathematical, logical, combinatorial and other transformations of the initial information, as a result of which the encrypted information is a chaotic set of letters, digits and other symbols and binary codes. For the encryption algorithm information is used, As a rule, the encryption algorithm for a particular method does not change. The initial data for the encryption algorithm is the information to be encrypted and encrypted. The key contains control information that determines the selection of the conversion at certain stages of the algorithm and the size of the operands used in the implementation of the encryption algorithm. Operand - constant, variable, function, expression and other programming languages of objects on which operations are performed. Unlike other methods of cryptographic transformation of information, steganography methods can hide not only the value of stored or transmitted data, but also the fact of storing or transferring sensitive information. The basis of all steganography methods is the masking of sensitive information among open files, ie, hiding secret data, so these are realistic figures that can not be distinguished from the real thing. The processing of multimedia files in information systems has opened almost unlimited possibilities for steganography. Graphical and sound information is presented in digital form. Thus, the graphic objects in the smallest element of the image can be encoded in one byte. The lower level of certain bytes of the image in accordance with the cryptographic transformation algorithm places the bit of the hidden file. If you choose the right image transformation algorithm and against which the hidden file is placed, the human eye is almost impossible to distinguish from the original image. Using steganography tools can be masked by text, image, voice, digital signature, encrypted message.



Classification of cryptographic information conversion methods

A hidden file can also be encrypted. If someone accidentally discovers a hidden file, the encrypted information is perceived as a system crash. The integrated use of steganography and encryption significantly increases the complexity of solving the problem of detection and disclosure of confidential information.The content of the information encoding process consists in replacing the initial value of the message codes. Codes can be used as a combination of letters, numbers, punctuation marks, special tables or dictionaries used for encoding and reverse conversion. Coding of information networks of source software and hardware used to improve the reliability of transmitted information.Often encoding and encryption are mistaken for the same thing, forgetting that to recover an encoded message it is sufficient to know the replacement rule, and to decrypt the message's encryption, in addition to knowledge of the rules, a key to the cipher is required.Compression of data can be attributed to methods of cryptographic transformation of information with certain reservations. The purpose of compression is to reduce the amount of information. At the same time, compressed data can not be read or used without inversion. Given the availability of compression and inversion tools, these methods can not be considered a reliable means of converting cryptographic information. Even if they contain secret algorithms, they can be easily opened by statistical processing methods. Therefore compressed files of confidential information are subject to subsequent encryption. To reduce the time of data transfer, it is advisable to combine information about the process of compression and encryption.The program methods are zahistu - su sukupnist algorithmov i programm, yaki zabezpechuyte rozmuzhuvannya access and exclusion of unsanctioned information and information. Factors threats to save information in information systems.Overseers of deliberate information preservation in SODs share threats from users of computers and non-users. Unauthorized access to information may include unauthorized use of system information and active infiltration. Unauthorized use of information is identified with the situation where an unauthorized user receives an opportunity to view information stored in the system and use it for their own purposes.Under active infiltration of information, such actions as viewing files of others through remote terminals, masking for a particular user, physical collection and analysis of files on maps, magnetic tapes and disks, etc. are understood.Intentional penetration attempts in SOD can be classified as passive and active.Passive penetration is the connection to the communication lines or the collection of electromagnetic radiation of these lines at any point in the system by a person who is not a user of the computer.Active penetration into the system is a direct use of information from files stored in the SOD. This penetration is realized by the usual access procedures: using a known method of access to the system or a part thereof for the purpose of the task of prohibited questions, access to files containing information of interest; cloaking to a genuine user after receiving the characteristics of access; using the official position, that is, the unplanned review of the file information by the staff of the computer system.Active penetration into the SOD can be carried out secretly, that is, the use of control programs to ensure the security of information.The most typical penetration techniques are: the use of entry points installed in the system by programmers, service personnel, or points detected when checking the circuit of system control; connecting to the network of a special terminal providing access to the system by intersection of the legitimate user's communication with the computer with the subsequent restoration of the connection by the type of erroneous message, as well as at the moment when the legitimate user does not show activity, but continues to occupy communication channel; cancellation of the user's signal about the termination of the system and the further continuation of work on his behalf.With these techniques, the offender, replacing for the time of his lawful user, can only use files available to that user; unauthorized modification - an unauthorized user makes changes to the information stored in the system. as a result, the user to whom this information belongs, can not access it.The term "unauthorized" means that the listed actions are performed contrary to the instructions of the user responsible for storing the information, or even bypassing the restrictions imposed on the access regime in this system. Similar attempts to penetration can be caused not only by the simple satisfaction of the curiosity of a competent programmer, but also by the deliberate receipt of information of limited use.There are other types of violations that lead to the loss or leakage of information. Thus, electromagnetic radiation during the operation of the computer and other technical means of SOD can be intercepted, decoded and presented in the form of bits constituting the flow of information.Requirements for the protection of information systems.One of the essential requirements for a secure information system is the separate identification of individual users, terminals, individual programs by name and function, as well as, if necessary, the data to the record level or element. Restrict access to information allows a set of the following methods: - hierarchical classification of access; - Classification of information on the importance and place of its occurrence; - Specifying specific restrictions and their application to specific objects, for example, the user can only read the file without the right to write to it; - content of data or separate data groups; - procedures presented only to specific users. Program users should be limited to one or all of the privileges: reading, writing, deleting information.When implementation of the record it is envisaged its modification, build and input. The system of ensuring the security of information must ensure that any data movement is identified, authorized, detected and documented. Organizational requirements for the system of protection are implemented by a combination of administrative and procedural measures. Conservation requirements must be met primarily at the administrative level. For this purpose: - limited unconnected access to the computer system; - control over the change in the software system; - testing and verification of changes in the software system and security programs are performed; - mutual control over the implementation of data storage rules is organized and maintained; - the privileges of personnel servicing the SOD are limited; - record of the access protocol to the system; - the competence of the service personnel is guaranteed. Organizational measures undertaken to improve the security of information security may include the following: - Developing a consistent approach to ensuring the security of information for the entire organization; - organization of clear work of service of tape and disk libraries; - staffing of the main personnel on the basis of integral assessments and solid knowledge; - organization of the system of training and professional development of service personnel.From the point of view of providing access to SOD, it is necessary to perform the following procedural steps: - to develop and approve written instructions for starting and stopping the system: - to control the use of magnetic tapes, disks, cards, lists, the order of software changes and bringing these changes to the user. - Develop a procedure for restoring the system in case of collision; - to establish a policy of restrictions on authorized visits to the computer center and to determine the amount of information to be issued; - to develop a computer logging system, data input and output; - to ensure the periodic cleaning of archives and repositories of tapes, disks, maps for the exclusion and elimination of unused; - maintain documentation of the computing center in accordance with the established standards.Classification of schemes of protection of information systems. Saving information can be broken in two main cases: when receiving unauthorized access to information and violation of the functioning of the computer. The system of protection against these threats includes the following main elements: protection of the SOD and its equipment, organizational measures for ensuring the preservation of information, protection of the operating system, files, terminals and communication channels.It should be borne in mind that all types of protection are interconnected and in the performance of their functions, at least one of them deceives the efforts of others. The proposed and implemented data protection schemes in the SOD are very diverse, which is caused mainly by the choice of the most convenient and easy to implement method of access control, that is, changing the functional properties of the system. As a classification feature for the protection schemes you can select their functional properties. Some systems lack the mechanism that prevents the user from accessing any information stored on the system. Characteristically, most of the most common and widely used abroad SOD with batch processing do not have a protection mechanism. However, such systems usually include a well-developed detection and prevention device that ensures the elimination of the failure of the operating mode. In systems with full protection, the mutual isolation of users is provided, which is violated only for general information. In some systems, tools for working with public libraries allow users to include information about them, which also becomes a common asset. For systems with a single protection scheme, a list of authorized users is created for each file. In addition, each file specifies how to use it: read, write, or execute if this file is an application. The basic concepts of protection here are quite simple, but their implementation is quite complicated. In systems with a programmable protection scheme, a data protection mechanism is envisaged, taking into account specific user requirements, for example, limiting the system time, accessing only the average values of the data file, local protection of individual elements of the data array, etc. In such systems, the user should be able to select protected objects and subsystems.The protected subsystem is a collection of programs and data, the right of access to which is endowed only by the inputs in the subsystem programs. Obrazhanie to these programs, in turn, can only be in predefined points. Thus, the subsystems control access to secure objects. A similar mechanism of protection with various modifications is implemented only in the most advanced SOD.In systems with classification, not the issue of limiting the access of programs to information, but the control over the further use of the information received. For example, in the system of use of stamps secrecy on documents stamp serves as a message of control. In the SOD, this protection circuit is rarely used.Distinctive feature of the considered schemes of protection - their dynamism, that is, the possibility of entering and changing the rules of access to data in the process of the system. However, ensuring the dynamism of protection schemes greatly complicates their implementation. Questions about the organization of information protection should be solved already at the pre-project stage of development of SOD.It should be borne in mind that infiltration in the system will increase with the increasing value of access to restricted information. At this stage, it is necessary to clearly identify the potential of the perpetrator in order not to overly "heavier" the system. The experience of designing security systems is still insufficient.However, some generalizations can already be made. Security mistakes can be greatly reduced if the following basic principles of building a protection system are taken into account when designing.This principle is well-known, but not always deeply understood. Indeed, some errors not found during the design and implementation, allow you to find unapproved access paths. Therefore, it is necessary to carefully test the software or circuit protection device, but in practice such verification is possible only for simple and compact schemes. 2. In the protection mechanism, permissions must prevail over prohibitions. This means that, under normal conditions, access should be absent, and for the operation of the protection scheme necessary conditions under which access becomes possible. In addition, it is believed that the prohibition of access in the absence of special instructions provides a high degree of reliability of the mechanism of protection. Error in the protection scheme based on the use of permits, leads to the extension of the scope of the prohibitions. This error is easier to detect and it will not violate the general protection status. The control should be comprehensive. This principle requires the need to verify the authority of any appeal to any object and is the basis of the system of protection. The task of access control, taking into account this principle, should be solved on a system-wide level and for such modes of operation as start-up, recovery after failure, exclusion and preventive maintenance. It is necessary to ensure a reliable determination of the source of any access to data.4. The mechanism of protection may not be classified, that is, it makes no sense to declassify the details of the implementation of a system of protection intended for widespread use. The effectiveness of security should not depend on how experienced the potential offenders are, because it is much easier to secure the password list. The absence of the same link between the mechanism of protection and passwords allows you to make the scheme of protection, if necessary, a subject of wide discussion among specialists without affecting the interests of users.In the SDS, the availability of several security keys is convenient in cases where the right to access is determined by the fulfillment of a number of conditions. For any program and any user, the minimum range of powers required to complete the assigned work must be determined. Thanks to these actions, the damage caused by crashes and accidental violations is greatly reduced. In addition, reducing the number of exchanges of data between privileged programs to the required minimum reduces the likelihood of unintentional, undesirable or false use of authority. Thus, if the protection scheme allows to set "barriers" in the system, then the principle of minimum powers ensures the most rational location of these "barriers". Maximum isolation of the mechanism of protection. In order to exclude exchanges of information between users in designing a protection scheme, it is recommended to minimize the number of parameters common to several users and the characteristics of the protection mechanism. Despite the fact that the operating system's access control functions overlap, the permission system should be constructed as an isolated software module, that is, protection should be separated from data management functions. Implementing this principle allows you to program the system of permission access as a stand-alone package of programs with subsequent independent debugging and verification. The software package must be located in a secure memory field to ensure the system localization of external access attempts. Even attempts to penetrate the operating system applications should be automatically captured, documented and rejected if the call is not executed correctly. Naturally, as a result of the implementation of a separate mechanism of protection, the scope of the program and the timing for its development may increase, there will be duplication of managers and support programs, as well as the need to develop independent calling functions. Analysis of the storage of information systems. Analysis of the preservation of information systems is based on the continuous study of protocols, checking alarm systems and other devices. An important factor is the fact that such an overview maintains interest in security issues.A security officer is responsible for conducting the analysis. Alarm devices should be checked frequently, but at random moments of time. These include fire and smoke detectors, humidity and temperature sensors, signaling equipment when attempting to penetrate the premises, physical access control devices, door signaling and other similar devices. Also, checking the state of fire equipment, access to emergency exits and systems for switching off the electricity, water and heat supply is also carried out. Every week the serviceability of devices and communication lines is checked. It also looks at the space under the technological floor and other cavities in which waste that creates the danger of self-ignition, or water at its sources can accumulate. From the performed work, a checking protocol is conducted, each record of which is accompanied by observations on the rejection. Foreign experts believe that this work should be given about one hour per week. Another important and regular work is the study of manual and machine protocol records. the results of regular checking of protocols should be drawn up in a certain way in order not to miss any type of inspection. It is recommended to thoroughly investigate any suspicious tendencies and deviations from the accepted standards in the work.Moreover, the described operations in and of themselves are the object, the preservation of which must be ensured, therefore, a special room with a terminal should be allocated, in which only work on maintenance of safety is carried out. The by-product of the safety analysis can be a statistical evaluation of the effectiveness of the use of equipment of the organization and evaluation of the effectiveness of users. On the basis of the results of the inspection, weekly meetings of the leaders of the organization are held, at which a message is heard by the employee responsible for ensuring security. Such meetings allow for the assessment of protection efforts and the development of additional recommendations for the improvement of accepted security methods. It is necessary to analyze all the possibilities of breaking the preservation and to find ways to combat them. If standard procedures are not performed, then the instruction is repeated to carry out these procedures. In addition to the usual regular inspections described above, the employee responsible for ensuring security is required to perform test control of hardware and software inspection. Test results are recorded in a special journal. It requires some manual labor and machine time. In SODs in which the level of security is high, testing should be carried out more often and as far as possible automatically. The test results are also analyzed by the employee responsible for ensuring security. Comprehensive protection of information in personal computers.According to statistics, more than 80% of companies and agencies suffer financial losses due to data security breaches.Many companies are now developing various antivirus programs, systems for differentiating data access, copy protection, etc. This is explained by the comparative simplicity of the development of similar methods and at the same time, their high efficiency. Consider the main mechanisms for the implementation of specific software information protection. Application IDs are used to control the logon on the computer, authenticate the user to enter the password and delimit the access to computer resources. The user identification refers to the process of recognizing a particular subject of a system, usually using a predefined identifier; each subject of the system must be uniquely identified. And authentication means verification of user authentication, as well as checking the integrity of the data when they are stored or transmitted to prevent unauthorized modification.When booting from a hard disk drive, the BIOS system reads the 1st sector of the 0th cylinder of the 0th track. This sector is called "Master Boot Record" - Master boot record / MVR /. Usually, the program written in the MVR downloads the BOOT RECORD / BR / active section record. However, you can use the MVR to organize the control of logging into the PC. Since the size of the MVK program is small, then it can put very limited functions. For example, you can try to "put" it together with the main function and password validation program.However, it is more efficient to use the MVR to download another, larger program volume. When using a standard partition of HDD for partitions using the FDISK program, the sector with a number greater than or equal to the 3rd, 0th cylinder 0th track is not used, so they can be used to store a larger volume of program that performs control functions. In addition, the record of the MVR stores the original table of descriptors logical disks. Changing this table prevents access to the logical disk at the DOS level when booting from a floppy disk. The first sector of the active partition contains a bootable VC record that loads the operating system. At the beginning of this record contains a table of parameters of the logical disk. BR can be used to download a non-operating system, and some other application that implements access delimitation. In turn, this program should download the operating system at the end of its work. The volume of VR is sufficient for placing an application that implements the download of an arbitrary file from the root directory of the logical disk. Modification of the table of parameters of some logical disk can also be used to prevent access to this logical disk when booting EOB from a floppy disk.   An example of such programs is the SHIELD system, which consists of 2 files: sset.com and sswith.com When you first install the system, the sset.com file copies the original MVR to the 2nd sector of the 0th track of the zero cylinder, and in the first sector leaves a modified version of the MVR, which, before loading DOS, asks for a password. If the password is incorrect then the hard drive is not available. To remove protection, the sswitch.com file is used, which returns the original sector of the MVR. It is advisable to use programs of this kind to protect a computer without HMDD, as during boot from a floppy disk, you can freely read and copy data from an HDD.In addition, for a professional, such protection does not present serious difficulties. In the standard DOS environment, COMMAND.COM is used as the command processor. However, the system allows the installation of another shell command on the SHELL command in the file COMG10.BUB. With the new command processor, you can only allow the launch of certain programs and prevent the launch of others. An example of a command processor is the PWLOAD.COM file, developed by 2B P rogrammers Groups. This program asks for a password, and if it is typed incorrectly, then the computer is blocked.Access separation functions can also be implemented using the device driver specified in the CONFIG.SYS file. This driver can control access to files, directories, and non-standard logical drives. For this purpose, interception of the interrupt of DOS INT 2lh and other interruptions of the operating system is usually carried out, sectoral protection against reading / writing is organized, protection against renaming and moving. This is due to some difficulties, since it is important to store large volumes describing the access authority to each sector, and FAT and DIR shadow tables to verify that they are overwritten. In general, this problem seems to be difficult due to the large amount of data to be stored and processed in the access differentiation system. You can also enter the password for logging in to the driver on the driver. There are drivers for organizing the mode of transparent encryption of data on disks. This driver intercepts the interrupt of the BIOS INT 13h, thus controlling all operations on the disk. In this case, the data on the protected disk are encrypted, and the keys can be stored on a non-standard formatted key floppy disk for better data security. This protection measure is convenient to prevent reading from HDD data when booting from a floppy disk.But here there are a number of significant disadvantages. First, the encryption keys are stored in the RAM, and therefore can be numbered by malicious people. Secondly, you can always get the open file content by rewriting it to some file, which is not in the group of transparently encrypted files.Example driver - DISKREET system from the package NORTON UTILITES: includes the files DISKREET.SYS and DISKREET.EXE. DISKREET.SYS is a driver loaded from CONFIG.SYS and allows you to create non-standard logical drives that are password protected, which are also encrypted using the original algorithm.The DISKREET.EHE program allows you to encrypt and decrypt any files and directories on disks. Programs resident in memory can perform the same functions as drivers. There is only a difference when loading: the driver is loaded from the CONFIG.SYS with the DEVICE command, and the resident programs are from the AUTOEXEC.VAT file.In addition, such programs are often used to control and prevent the infection of the computer by viruses. Encryption programs perform only one function - data encryption: files, directories, and disk drives by the user key. Various encryption algorithms are applied: from cryptographically stable DES and FEAL to trivial bitwise algorithms with key. There are quite a lot of examples of such programs. The advantages of software protection can be attributed to their low cost, ease of development. The disadvantage of such systems is the low level of information security. To enhance security, you can propose the use of multiple software at a time. For example, use the password at the entrance, the access differentiation system, and the transparent encryption mode. In this case, there will be some inconvenience in the work, but at the same time, reliability will increase. Let's consider the main types of software - hardware protection of information. They are characterized by higher resistance and, consequently, a higher cost. But with the application of hardware and software complexes at enterprises with increased risk of emerging threats, the costs of installing such protection are fully paid off. Many companies - computer manufacturers provide protection against unauthorized access at the chip level of the ROM from the BIOS. So, when you boot your computer when you turn on the power while still in the POST procedure, you must specify the correct password so that the machine continues to work. Sometimes the ability to set the password is implemented in the BIOS, but not described in the documentation. Some viruses can write random information in the password field, and once the user finds out that his machine is well protected from it. The password itself is stored in the CMOS area and may be erased if desired. Firm Compaq went further and included in the BIOS programs that support the following areas of sharing access: the ability to quickly shut down the computer, protecting the hard disk, the floppy disk, serial and parallel ports. The startup of protection programs from the BIOS is controlled by the switches on the computer board. It should be noted that the effectiveness of such protection is achieved only in conjunction with the organizational protection measures, as if the free access to the "inside" of the computer malicious person will not be too difficult to replace the chip from the BIOS or to disassemble the battery, thus neutralizing the above protective measures . The encryption board is inserted into the expansion slot on the motherboard of the computer and serves as an encryption function. On the board there is a pseudorandom number sensor for generating keys and encryption nodes, hardware implemented in specialized single-chip microcomputers. Encryption keys are stored on a specially designed diskette for this purpose. The software part of the complex contains a driver for the interaction of user programs with the board of encryption. As an example, consider the product of the firm "ANKAD" - software and hardware complex "Krypton". This device provides high cryptographic stability, encryption is carried out according to the algorithm GOST 28174 - 89. The open interface allows the development of additional software special purpose. The key length is 256 bits. Encryption speed - up to 200 Kbytes / sec. Hardware Requirements: IBM PC CT / AT, MS-DOS 3.0 and above. Software support allows you to: encrypt files, partitions, disks; separation and control of access to the computer; electronic signature of legal and financial documents; transparent encryption of hard and floppy disks. Encryption boards have a high degree of protection of information, but their application makes certain inconveniences to the operation of the PC, above all, a significant reduction in the speed of data processing, as well as the need to initialize the card each time the computer is turned on.Recently widespread electronic keys have been acquired. This device connects to the computer via the LPT port. In this case, the electronic key does not interfere with the normal operation of the parallel port and is completely "transparent" for the printer and other devices. The keys can be connected cascading, usually up to 8 pieces in a row. At the same time in the chain can work absolutely different types of keys, issued by different firms.Electronic keys can perform various functions. Electronic keys allow you to protect not only the COM and EXE applications, but also work with non-performing applications, for example: AUTOCAD LISP, LOTUS type spreadsheet macros, RUNTIME modules, interpreters, databases, encoded graphics files, etc. In addition to the main protective functions of the keys of many companies are able to detect the fact of infection of the protected program by various types of file viruses. Very effective is the use of electronic keys for storing and transmitting encryption keys when using different encryption methods, since key storage and transmission are the weakest place in most of the existing algorithms. And when using electronic keys to generate encryption keys, there is no need to memorize or record them, and then enter from the keyboard. The key does not have built-in power supplies and stores the information stored on it when disconnected from the computer. In our country, the most common keys of the American firm "Software Security Inc.". This company produces keys for DOS, WINDOWS, UNIX, OS / 2, Macintosh. Keys can be both single-entry and reprogramming; may or may not contain non-volatile memory. Electronic keys are one of the most effective and convenient copying protection. Plastic Identification Cards (ICs) are being implemented in many areas of our lives. The small size of the card, the convenience of storage, a fairly high amount of memory make the IR irreplaceable in many areas of human activity.There are many examples of the use of IR in the GIS, for example, to implement protection of PC from unauthorized access. Such a hardware-software complex consists of a hardware part: a special board, which is inserted into the expansion slot of the PC, devices for reading information from the IR and the IR themselves; There is also a program part: a driver for controlling the board and a reader with an IR. The software part of the complex may also include software for organizing the separation of access to parts and partitions of the hard disk. In addition, the security system asks for a password. Thus, the logon is stuck on the card.An example of a hardware-software complex of protection is the development of the Datamedia firm. A series of its Netmate computers is equipped with a special device Securecard reader - a security card reader. Security Cards in execution - an option for credit cards; on their magnetic media with the help of special equipment, which is only at the disposal of the administrator, a record of the user is made: his name, password and describes all the powers that he receives when logging in. In particular, the card records how many times a user can try to enter the password when logged in. Thus, accidental loss of a security card or its theft does not allow an attacker to access the computer: if the user name can still be found without attention, then the password is unknown to him. Only a conscious transfer of security cards to someone at the same time as the password is disclosed may open access to the computer to a third party.The system administrator creates a security card for legitimate users. On this map, in addition to the information already listed, the profile of the user is described. It includes, for example: access to the program SETUP, that is, the following characteristics of the computer are recorded, such as the screen, the number and types of disks; It also determines which of the local devices are available to that user from which local or network devices it can boot. Passwords are provided for translation: the password assigned to the user is usually easy to remember, but not the one with which the system works. When you try to simply pull off the security card from the reader, access to the computer is tightly blocked until the same security card is inserted into the reader. If the wrong passwords - the machine is blocked, and only the administrator can "revive" it, that is, it is stimulated by the need to inform the administration of all cases of violation of the privacy regime.From the point of view of virus protection, the listed systems are also important because they, in addition to identifying the user, somehow organize their work on the computer, forbidding certain dangerous actions such as the launch of programs from a floppy disk, boot from a floppy disk. Restrictions on the use of certain system resources such as network cards, serial ports are also useful in terms of protection against viruses, because they limit the ability or even cut off some ways of spreading or getting infected, Finally, the increased level of anxiety, which is typical for this system is very useful and with an antivirus point view: any malfunctions and miracles in the work of computers should immediately become the property of the administration and also be immediately brought to the attention of specialists, which dramatically reduces the size of damage from penetration usiv.IRs can be used to store encryption keys in cryptographic protection systems. The disadvantage of such a system is the low security of the IR with the magnetic stripe. As experience shows, the information from them can be unhindered. And the use of IC with an integrated chip due to the high cost of such IC leads to a significant increase in the cost of installing a system of protection, In addition, expensive and equipment to read information from the IR. But, despite the high cost, IR-based security systems are widely used where high reliability is needed, for example, in commercial structures.Currently, the family of Touch Memory devices (TM), manufactured by Dallas Semiconductods, has become very popular.This choice was determined primarily by high reliability, since it is difficult to remove the touch-memory from the system. One of the main differences between Touch Memory devices and other compact media is the design of the case. In addition to protecting the steel case also plays the role of electrical contacts. Acceptable and mass-dimensional characteristics - a tablet with a diameter of two-ply coin and a thickness of 5 mm is very suitable for such applications. Each device of the family is unique because it has its own serial number, which is recorded in the device with a laser installation during its manufacture and can not be changed during the entire life of the device. In the process of recording and testing at the factory, it is guaranteed that no two devices with the same serial numbers will be manufactured. Thus, the possibility of tampering of devices is excluded. It is quite acceptable when using Touch-memory there is a price: it is more than 4 times lower than when using plastic cards. The Toich Memory devices represent a non-volatile, non-volatile, static memory with multiple recording / reading located inside the metal case. Unlike conventional memory with a parallel port / data port, Toich Mempry has a serial interface. Data is recorded / read in memory by one two-way signal line. From this line commands and data are transmitted to the device, data is read out. This uses the pulse-width encoding method. Logic signals "1" and "0" with a level from +5 V to VV are transmitted by pulses of different durations. This digital interface allows you to connect Touch Memory devices directly to a personal computer or through a microprocessor controller.An important feature of the devices is the low power consumption, which allows the use of a miniature lithium battery built into the cabinet for storing information in memory for 10 years.There are specific development of hardware-software complexes for the protection of information on the basis of TM. As an example, consider the QPDOS system, developed by specialists from JSC "RNT". QPDOS is a functional extension of MS-DOS and is intended for use as part of a PC based on IBM PC / AT. QPDOS fully monitors and controls the access of all users to PC resources and data. As QPDOS functional parts, the following subsystems can be included: logging and accounting, which is used for logging of events occurring in the system, monitoring possible NDS attempts, recording user sessions and generating reports; operational control that allows you to quickly monitor PC system administrators by events and actions of users that occur on any PC within the network; integrity control and copy protection software; Prohibition of initial boot from HMD, preventing the possibility of bypassing the breach protection system by downloading a PC from its system floppy disk; cryptographic, which is an MS-DOS driver, encrypts and decrypts information on individual logical drives of the PC in a transparent application mode. In addition, the subsystem includes tools for generating encryption keys and re-encryption of information on a new key, and the introduction of key encryption into the system of electronic keys Touch Memory. The system of cryptographic protection can be used both in purely software version and with hardware support in the form of kriptoplata "Krypton - 3", which increases the system performance.It should be noted that computer security measures are not limited only to security devices located in the computer itself - inside the computer, or as external devices. All of the above software and hardware and software information protection are only effective when strictly adhering to a range of administrative and organizational measures.Before building a system of protection, it is necessary to estimate the costs of its creation and the possible costs of eliminating the consequences in case of loss of protected data. Protection will be economically feasible only if the costs of its creation will be less than possible losses. Problems of providing security are significantly complicated in the organization of machine processing information in the conditions of collective use, which focuses, processed and accumulates information for different purposes and belongings.There is no reason why data processing systems based on modern computer facilities would not be able to provide a greater degree of data storage than conventional systems for collecting, storing and processing information. The system should protect its users from each other from both accidental and targeted threats of violation of the security of information. In addition, the accepted security mechanisms must provide the user with means to protect his programs and data from

him/her.Improving the technology of information processing has led to the creation of information databases that contain large volumes of various information, which also requires additional requirements to ensure the security of information.In systems of collective use, which have a developed network of terminals, the basic complexity of security is that the potential violator is a full subscriber of the system.Therefore, the term "protection" refers to a method of ensuring safety in SOD. The protection of information is usually reduced to the choice of means of control over the execution of programs that have access to information stored in the data processing system (SOD).

List of references:

1. Gaikovich B, Pershin O. Security of electronic banking systems. - M., 1999.
2. Gruzdev S. "16 variants of Russian protection" / ComputerPress № 392
3. Gruzdev S. Electronic keys. - M. 1993.
4. Karasik I. Software and hardware protection of information for personal computers / / ComputerPress № 3, 1995
5. Maftik S. Mechanisms of protection in networks of computers. / Per. from english M .: SVIT, 1993.
6. Petrov VA, Piskarev S.A., Shein A.V. Informational security. Protection of information from unauthorized access in automated systems. - M., 1998.
7. Spesivtsev A.V. etc. Protection of information in personal computers. - Moscow: Radio and Communications, 1993.

SECURITY

People's trust builds the state and interstate education. People's trust in state and international institutions gives governments and international organizations the money and legitimacy to act. Without trust, the meaning of the deal is lost, alliances are devalued, blank guarantees. The credibility of the modern security model of the world is undermining the legitimacy of the modern security model. So the question of time is coming to replace the current models of international security that should protect people from the ghosts of the world war. And the strength or fragility of this model will depend directly on how much people believe in it, which is now in a state of uncertainty and fear. The Bespoke Forum is a discussion platform for finding the answer to the question of what should be the new security order in the world.The work syllabus contains the following sections: Purpose and tasks of the discipline. The tasks of the discipline "Fundamentals of National Security of Ukraine": from the standpoint of synergetic, systemic, and managerial approaches give students theoretical and practical knowledge that will allow them to be professionally oriented in various situations related to the preparation and implementation of management decisions in various areas of national security.Know:conceptual foundations of Ukraine's national security;Components of the national security system of Ukraine;criteria for the formation of vital life spheres; main objects and subjects of national security; basic concepts of national security; basic approaches to the definition of key concepts; stages of the formation of threats and dangers;The main geopolitical doctrines of our time; algorithm for modeling a security system; basic approaches to ensuring national security; the place and role of the non-state security system in ensuring the national security of Ukraine; the role of benchmarking in ensuring national security; The legal and regulatory framework governing public security relations.

TENSOR

Tensors are a generalization of the notion of scalar and vector. They are used, for example, to describe deformations and stresses. In a simplified way, the Tensor T can be imagined as a rope operator acting on vector a and producing from it a new vector v with a different return, direction and value:

$$V=T\ a$$

The number of all components of the tensor is calculated according to the 3 n reality, where n is the tensor order:

— the scalar size is the zero order tensor, e.g. mass,

— the vector is the first order tensor, e.g. force,

— 2nd order tensor has the form of a 3 × 3 matrix, e.g. stress tensor. The 2nd order Tensor is the size specified in point P, which assigns the vector t to any direction μ, i.e. it is a linear operator that maps the vector into a vector according to the relation:

$$t_{\mu} = T \times \mu$$

The nine components of the T tensor can be written in matrix form:

$$\begin{bmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & t_{22} & t_{23} \\ t_{31} & t_{32} & t_{33} \end{bmatrix}$$

which is a representation of the Tensor T.
Coordinate transformation of the second order Tensor can be written as follows:

$$t'_{i\,j} = \sum_{k\,l} t_{k\,l}\, q_{i'\,k}\, q_{j'\,l} = t_{k\,l}\, q_{i'\,k}\, q_{j'\,l}, \quad k,l = 1,2,3;\ i',j' = 1,2,3.$$

For example, for example, the t'$_{13}$ component is transformed according to the formula:

$$\begin{aligned} t'_{13} = t_{kl}\, q_{1'k}\, q_{3'l} = & t_{11}\, q_{1'1}\, q_{3'1} + t_{12}\, q_{1'1}\, q_{3'2} + t_{13}\, q_{1'1}\, q_{3'3} + \\ & t_{21}\, q_{1'2}\, q_{3'1} + t_{22}\, q_{1'2}\, q_{3'2} + t_{23}\, q_{1'2}\, q_{3'3} + \\ & t_{31}\, q_{1'3}\, q_{3'1} + t_{32}\, q_{1'3}\, q_{3'2} + t_{33}\, q_{1'3}\, q_{3'3}. \end{aligned}$$

Tensor T is transformed according to the matrix record:

$$T' = Q \times T \times Q^{T}$$

and the inverse transfomation is recorded as the product of:

$$T = Q^{T} \times T' \times Q.$$

Operations on tensors— Adding tensors:

$$t_{ij} + p_{ij} = s_{ij}$$

odczas tej operacji dodaje się odpowiednie składowe, podobnie jak przy dodawaniu macierzy.

— Mnożenie tensora przez skalar:

$$at_{ij} = t_{ij}a \;\; i \;\; a(t_{ij} + s_{ij}) = at_{ij} + as_{ij}$$

— Iloczyn zewnętrzny dwóch tensorów:

$$a_i b_j = c_{ij}\,, \quad a_{ij} b_{km} = c_{ijkm}$$

Rząd powstałego tensora jest równy sumie rzędów mnożnej i mnożnika.

— Iloczyn wewnętrzny (zwężenie, kontrakcja) dwóch tensorów. Mnożąc dwa tensory ich wskaźniki się powtarzają, otrzymamy tzw. iloczyn wewnętrzny (kontrakcję):

$$t_{ijk}\, p_{km} = s_{ijm}$$

gdzie rząd powstałego tensora jest mniejszy od sumy rzędów mnożnej i mnożnika o wielokrotność 2 powtarzających się indeksów. W powyższym przykładzie
$3 + 2 - 2 \cdot 1 = 3$.

Reference

- L. Górniewicz, R. S. Ingarden: Analiza matematyczna dla fizyków. Wydawnictwo naukowe Uniwersytetu Mikołaja Kopernika, 2012.
- J. Musielak, L. Skrzypczak: Analiza matematyczna. T. III. Cz. 2. Wydawnictwo Naukowe UAM, 2006.
- P. K. Raszewski: Geometria Riemanna i analiza tensorowa. Warszawa: Państwowe Wydawnictwo Naukowe, 1958.
- W. Thirring: Fizyka matematyczna. T. 1: Klasyczne układy dynamiczne. Państwowe Wydawnictwo Naukowe, 1985.
- W. Thirring: Fizyka matematyczna. T. 2: Klasyczna teoria pola. Państwowe Wydawnictwo Naukowe, 1985.

TIME-BASED OPTICAL MODELING METHODS

The finite-difference time-domain (FDTD) numerical modeling method is considered to be one of the most accurate and simple rigorous methods to model anti-reflective properties of sub-wavelength structures. Though it is computationally intensive, the FDTD method handles any arbitrarily shaped structure naturally using an explicit numerical solution to Maxwell’s curl equations.The FDTD method was first introduced in 1966 by Yee and was furthered by Taflove [3,4]. Yee developed the mathematical approach to spatially discretize the computational space into what is now known as a Yee cube (see figure 1). The Yee cube is the unit cell of the equally offset electric and magnetic field computation points. The FDTD method, described thoroughly in Taflove’s book “Computational Electrodynamics: the finite-difference time-domain method” [5] was first developed to model electromagnetic (EM) radio waves. However, due to the simple and versatile approach, it is able to naturally handle any EM modeling situation given sufficient computing resources.

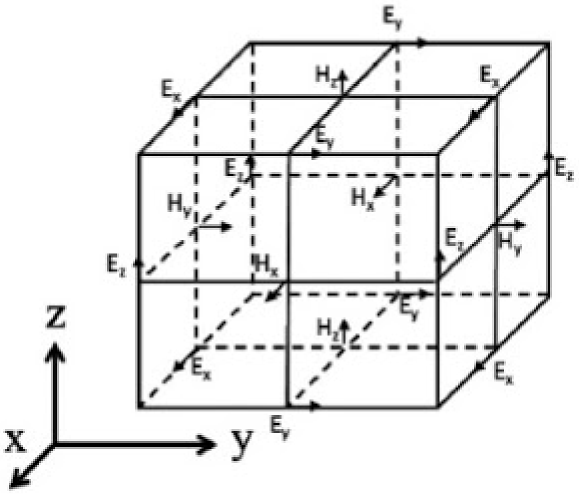


Figure 1. Yee cell. Arrows indicate the direction of the *E* or *H* field that is calculated at each point.

Prior to the turn of the millennium, lack of computing resources was a limiting factor to analyzing ARSWS using the FDTD method. Yamauchi *et al*. [6, 7] paved the way with their 1993 and 1996 publications that modeled simple 2D thin film ARCs. In 2004, Yang *et al*. [8] first used the FDTD method to model a 3D nanoporous structure. The introduction of exponentially increasing computing resources in the 2000's enabled the EM modeling community to utilize FDTD to its greatest advantage; researchers were finally able to model the behavior of light at an interface of any texture, size, or shape, regardless of its regularity, with only the knowledge of bulk material properties. Calculations in the time domain avoid the problem of the single wavelength restriction of other methods. Given sufficient computing power FDTD is also capable of accurately modeling structures of any size to wavelength ratio, whereas EMT requires wavelengths much longer than the interface texture and geometric optical approaches require wavelengths much shorter than interface structures. However, FDTD is highly demanding of computer processing, memory, and storage abilities compared to frequency-based or non-spatially discretized methods.

The FDTD method is derived from Faraday's and Ampere's laws as well as the relationships between the electric field (*E*), the electric displacement field (*D*), the magnetic field (*B*), and the auxiliary magnetic field (*H*). These four equations are used to derive Maxwell's curl equations:

$$(1)\ \partial B/\partial t = -\Delta\cdot E - M$$

$$(2)\ \partial D/\partial t = \Delta\cdot H - J$$

$$(3)\ D = \mathcal{E}r\mathcal{E}0E$$

$$(4)\ B = \mu r\mu 0H$$

$$(5)\ \partial H/\partial t = -1/\mu\Delta\cdot E - 1/\mu\ (Msource + \sigma H)$$

$$(6)\ \partial E/\partial t = 1/\mathcal{E}\ \Delta\cdot H - 1/\mathcal{E}\ (Jsource + \sigma E)$$

where ε is the permittivity, μ the permeability of the medium, and σ is the conductivity. When conductivity is zero the Maxwell’s equations can be rewritten as

$$\partial Hx/\partial t = 1/\mu\ [(\partial Ey/\partial z) - (\partial Ez/\partial y)]$$

(7)

$$\partial Hy/\partial t = 1/\mu\ [(\partial Ez/\partial x) - (\partial Ex/\partial z)]$$

(8)

$$\partial Hz/\partial t = 1/\mu\ [(\partial Ex/\partial y) - (\partial Ey/\partial x)]$$

(9)

$$\partial Ex/\partial t = 1/\ [(\partial Hz/\partial y) - (\partial Hy/\partial z)]$$

(10)

$$\partial Ey/\partial t = 1/\ [(\partial Hx/\partial z) - (\partial Hz/\partial x)]$$

(11)

$$\partial Ez/\partial t = 1/\ [(\partial Hy/\partial x) - (\partial Hx/\partial y)]$$

(12)

Equations (17)–(22) can be discretized using the central difference approximation to produce six algebraic equations that describe the behavior of EM waves in three dimensions. These equations are solvable for the electric and magnetic fields in each dimension: E_x, E_y, E_z, H_x, H_y, and H_z. To carry out the FDTD calculations, permittivity and permeability properties are assigned to each point in the computational grid and boundary and initial conditions are set (described by Taflove [5]). The discretized *E* and *H* equations are then solved alternately at each half time step, with the current E values depending on previous and adjacent *H* values and *vice versa*. Using this scheme, one can timestep through an entire simulation, resulting in electric and magnetic field values at each point for each timestep. For ARSWS analysis, these time-based data points are discrete Fourier-transformed (DFT) to the frequency scale [9]. The power of the EM waves is then calculated by squaring the absolute value of the DFT result and is multiplied by the index of refraction to account for the change in velocity in a non-vacuum medium if applicable. Reflectance and transmittance are found by normalizing the power against the input EM power.

Appropriate boundary conditions must be applied to the computational boundaries to avoid artificial reflections within the domain. Implementing boundary conditions in FDTD for ARSWS analysis is normally done one of two ways: an absorbing boundary condition or a periodic boundary condition. Periodic boundary conditions are simple and allow for modeling of an infinitely large array of ARSWS features. Absorbing boundary conditions (ABCs), which are necessary for all non-periodic boundaries, function to attenuate the EM signals at the interface. The most commonly used ABC is the perfectly matched layer (PML), which was introduced by Berenger in 1994 [10]. The PML functions to anisotropically attenuate all EM intensity that is traveling in the direction toward the boundary, effectively eliminating any artificial reflections from that surface.

Introducing a plane wave into an FDTD simulation is done by setting the *E* and *H* values in one plane to appropriate non-zero values for a period of time, either a short pulse or a continuous source. All values in the plane must be the same at any given time point to ensure plane wave functionality. The signs of *E* and *H* must be chosen to propagate the EM wave in the desired direction following the right hand rule. Plane waves can be introduced as monochromatic waves (with the *E* and *H*fields oscillating in time at the appropriate rate) or as a distribution of wavelengths. An example of introducing a Gaussian distribution of wavelengths into one simulation can be seen in figure 2.

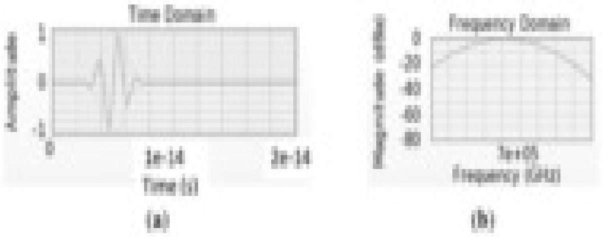


Figure 2. Time-based *E*-fields introduced as a plane wave (a) to simulate a range of frequencies (b).

In FDTD materials are defined only by their permittivity and permeability properties. Most ARSWS FDTD studies are based on dielectric materials, thus, the relative permeability is one and absorptive losses can be ignored. This is especially true when analyzing dielectric materials that are optically thin. Most studies also ignore dispersion, or the effect of wavelength on the permittivity, as permittivity of the commonly studied materials is relatively constant over the AM1.5 range. FDTD does not handle dispersion naturally, as multiple wavelengths are input simultaneously, but modern computing programs have been improved to include dispersion.

Programming FDTD simulations manually is feasible and is fully supported by Taflove's text on the subject [5]. However, there are several commercially-available or free software products that make FDTD simulations significantly easier to use, including XF by Remcom, FDTD Solutions by Lumerical, MEEP (open source), OptiFDTD, EM Explorer, FullWave by RSoft Design Group, and Electromagnetic Template Library. Commercial software often includes a user-friendly GUI and CAD modeling tools for drawing 2D or 3D materials.

Whether using in-house or commercial software, several guidelines must be taken into account when setting up an FDTD simulation. To be accurate, the software requires at least ten computational cells per wavelength. The time step is usually chosen so that there are at least 20 timepoints per wavelength. There must also be at least three calculation points across any feature that one is expecting to model; failure to comply with this requirement often results in the improper modeling of the tips of pointy nanostructures [32]. This pixilation effect would produce an artificially abrupt change in the effective refractive index at the pointiest parts of the ARSWS. Deinega *et al*. [22] reported a subgrid smoothing method to account for this effect, which improved the modeling of fine features. Even with this drawback, several authors reported the choice of FDTD over the rigorous coupled wave analysis (RCWA) method due to RCWA being oversimplified for some 3D models [19,23,24].

Several groups have used the FDTD method as an accurate method to fine-tune the designs of ideal anti-reflective interfaces. FDTD has been used in conjunction with the transfer matrix method (TMM); Feng *et al*. [25] developed a space mapping technique that applied both TMM and FDTD to converge on an optimal design for the thicknesses of a multiple thin film layered ARC. Feng *et al*. [25] compared the calculated reflectivity from FDTD, TMM, and experimental data to show that the FDTD method was more accurate than the TMM method for their multiple thin film simulations (see figure 3). Li *et al*. [26] and Zhou *et al*. [25] both also used TMM with FDTD to design antireflective and waveguide structures. The transfer matrix method is very efficient, but has limited accuracy due to its inherent approximations, while the FDTD method is versatile and accurate, but time consuming [26].

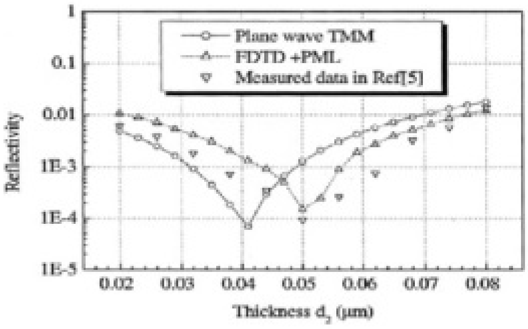


Figure 3. Reflectivity calculated from the finite-difference time-domain (FDTD) and transfer matrix method (TMM) methods compared to experimental data shows that the FDTD method is more accurate than the TMM method. Reprinted with permission from reference [15], Copyright 2003 IEEE.

Several groups used both FDTD and TMM, but refer to the TMM simulations as "effective medium theory" [8,32,39,40]. Effective medium theory takes subwavelength-textured structures and breaks them down into planes of effectively homogeneous "thin films". For example, Schmid *et al*. [29] sliced their nanotexture every 1 nm for their EMT models. The traditional thin film reflectivity equation (transfer matrix method) is used to calculate the reflectivity of the overall interface. This method works well for structures much smaller than the wavelength of EM radiation, but breaks down quickly as structures approach the wavelength size and if there are any non-zeroth order reflections or transmissions (due to a diffraction grating effect). Figure 4 shows the comparison of EMT results with FDTD results (including a subpixel smoothing method) for graded-index films with an integral RI profile ( ), square pyramids with linear and quantic RI profiles closely packed in a square lattice, and cones closely packed in a triangular lattice reported by Deinega *et al*. [11]. FDTD results are in good agreement with EMT over the wavelengths studied except for very short wavelengths where the assumptions of EMT break down. Separate results comparing FDTD, EMT, and experimental values for reflectivity *versus* GRIN height are shown in figure4.

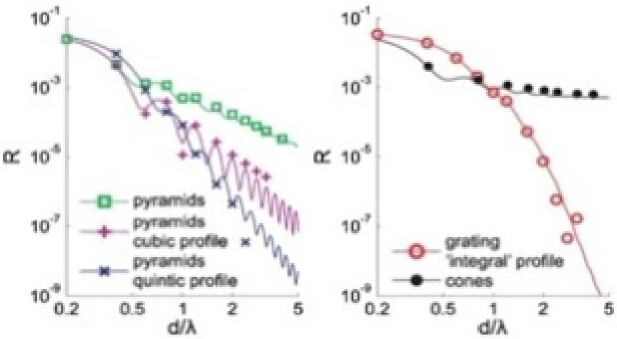


Figure 4. Reflectivity results from graded-index films with an integral RI profile, square pyramids with linear and quantic RI profiles closely packed in a square lattice, and cones closely packed in a triangular lattice from EMT (lines) and FDTD (points) calculations. Reprinted with permission from reference [11], Copyright 2011 Optical Society of America.

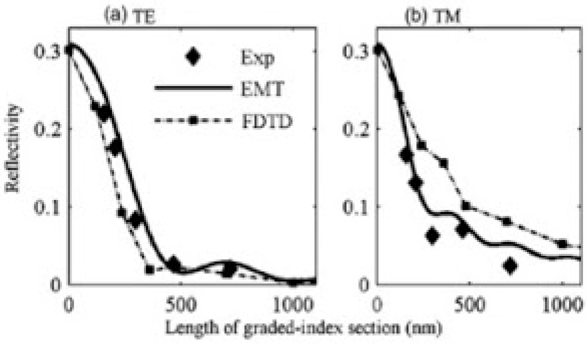


Figure 5. Comparisons between reflectivity calculated by EMT, FDTD, and experimental results for GRIN structures. Reprinted with permission from reference [29], Copyright 2007 Optical Society of America.

While effective medium theory requires features to be much smaller than the wavelengths of interest, geometrical optics or ray tracing is often used when feature sizes are much larger than the wavelengths [11,18,29]. Though specifically not useful for subwavelength structures, this method is often used to design anti-reflective gratings using light trapping. This method uses simple geometrical optics based on the index of refraction to calculate the behavior of light, assuming an abrupt change in index of refraction at the textured interface. Deinega *et al*. [11] report ray tracing models the short wavelength/large feature size extremes of anti-reflective designs and FDTD is still shown to have comparable, accurate results. However, due to the requirements of having many computational points per wavelength in space for this method it may not be ideal to model particularly large structures with FDTD due to processing power and data storage constraints.

Chen *et al*. [1,2] produced two studies that analyzed cones and pyramids using both RCWA (discussed in a later section) and FDTD. Ichikawa used both FDTD and the Fourier modal method (FMM/RCWA) to design two dimensional regular and random triangular gratings as early as 2002 [21]. The Fourier modal method was used to simulate the triangular gratings as a stack of twenty slabs and was used to verify the FDTD results. The author found that, while randomizing the triangular gratings in shape-, space-, or depth- modulated structures did not increase the AR properties of the SWS, the randomization did relax some of the subwavelength requirement for the ARC, which relaxes some of the fabrication constraints. They also determined that FDTD predicts higher reflectance than does zeroth order FMM, likely due to the neglect of higher order reflections in the FMM model. RCWA is a rigorous simulation method, but some authors have felt that it is too oversimplified to accurately model some 3D structures [19,14,15], especially those that are aperiodic.

As technology improvements have made 3D FDTD modeling faster and easier, more authors are performing several FDTD simulations to sweep across a range of feature properties in an attempt to design an optimal AR structure. Over primarily the last decade researchers have used FDTD to model thin films [6,36], nanoporous materials [8], regular and random 2D triangular gratings [21], cones [2,11,12,14,18,22,23], pyramids with a variety of base shapes [9], semi-spheres [9,13], rounded cones [11,24], nanoholes [25], and nanorods/nanowires [26,27]. As is reviewed in Chattopadhyay *et al*. [6], gradient index materials, or tapered nanostructures, generally perform the best as broadband anti-reflective interfaces. Thus, most of the FDTD simulation sweeps in the last decade have focused on sizes and shapes of pyramid, cone, or other nipple-like arrays of nanostructures. The ARSWS with the best broadband AR properties for wavelengths between 400 and 800 nm were found to be closely packed tapered nanostructures, cones or pyramids, with periods around 300 nm and lengths between 300 and 600 nm at about 0.3% reflectivity [13].

The FDTD method has been verified by experimental results by several authors. Deinega *et al*. [11] found the results of the FDTD simulations to be highly comparable to experimental results (Figure 15). Other authors have compared modeling and experimental results for pyramids [1], cones [24,26,29], hexaganol nanorods [26], round nanowires [27], tapered nanorods [26], and v-shaped nanoholes [25]. Although closely packed pyramids with high aspect ratios are known to have a smoother RI profile at the interface with the bulk material than cones due to their smooth fill percent profile, and hence theoretically lower reflection given the correct RI profile, they can be difficult to fabricate. Chen *et al*. [1] were able to fabricate what was effectively an array of hexagonal pyramids using a polystyrene nanosphere colloidal lithography technique. Their simulations predicted that the nanotexture would reduce the reflectance of the silicon to less than 1% and they were able to synthesize pyramidal structures with a reflectance of less than 1.5%.

FDTD has been used in literature to obtain reflectivity information about ARSWSs at non-zero angles of incidence. Deniz *et al*. [26] studied the effects of angle of incidence and plane wave polarization. They modeled hydrogen silsesquioxane nanorods that exhibited less than 2% average reflection over 400 to 800 nm wavelengths for between 0 and 60 degrees of incidence from normal in TM polarization (see figure 7). Some authors used FDTD to model embedded nanoparticles in silicon to enhance light scattering. Mokkapati *et al*. [29,31] modeled EM fields around metallic nanoparticles to increase light scattering for light adsorption in solar cells, though they reported E-field intensity, not reflectivity. Nagel and Scarpulla [31] modeled the light-trapping effects of embedding silica nanospheres in thin film silicon solar cells. Two groups also used the FDTD method to model the laser ablation process to produce AR nanomaterials [22,23].

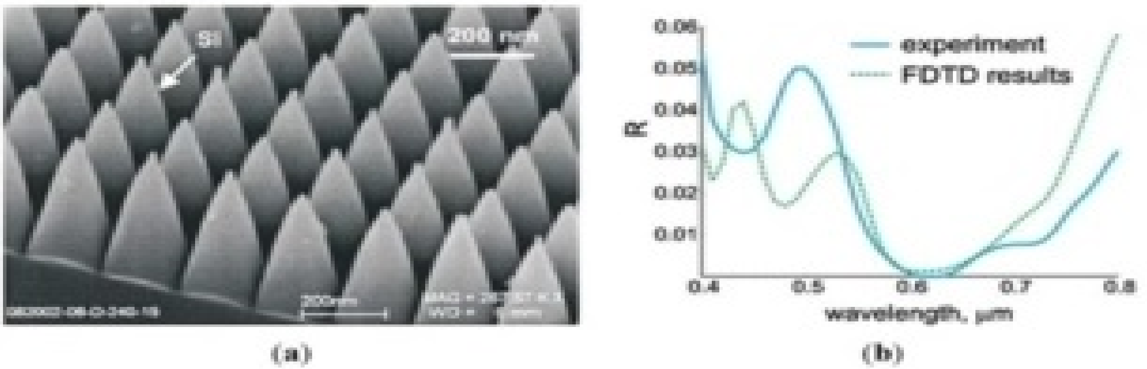


Figure 6. SEM image of square packed silicon cones (a) and (b) comparison of FDTD (dotted) and experimental results (solid). Reprinted with permission from reference [11], Copyright 2009 Optical Society of America.

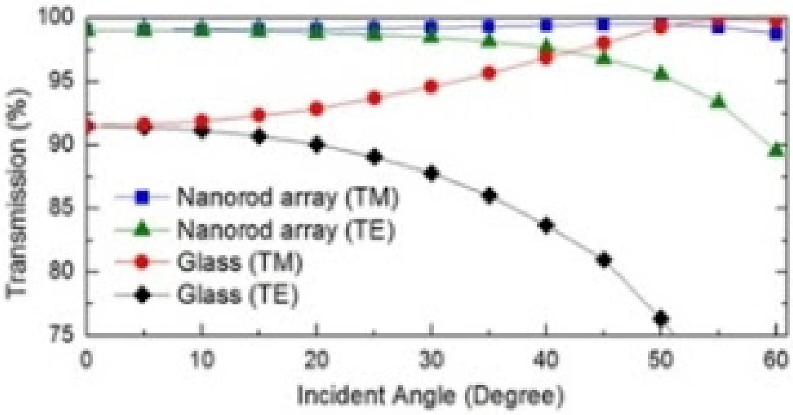


Figure 7. Angle of incidence FDTD simulations for nanorod arrays in TE and TM polarization [26]. Reprinted with permission from reference [26], Copyright 2011 AIP Publishing.

The FDTD method has been shown repeatedly to be a versatile, simple, and accurate modeling method for 2-D and 3-D modeling of anti-reflective subwavelength structures. This method can be accurate over any wavelength and feature size combination and can be used with any structure, regular or irregular. The FDTD method does not naturally handle dispersion, though refractive indexes in the visible wavelengths are relatively constant, and thus the modeling results from FDTD have been shown to match experimental results satisfactorily well. This can be overcome by inputting one wavelength per simulation and assigning the appropriate wavelength-dependent optical properties to the material. Computational resources have, in the past, limited the utility of FDTD modeling, though with the introduction of newer computing technologies these limitations are becoming fewer.

FDTD has been found to have convergence problems when attempting to calculate dispersion, with some metal components [31], or when modeling some features whose sizes approach the wavelength of EM radiation. These disadvantages have primarily been overcome by implementation of new algorithms in commercial software to reduce divergence and with faster hardware to handle longer simulation times. Also, for analysis of reflectance of ARSWS, FDTD requires post processing of time-based *E*-field data to obtain values for reflectance. This can either be a part of the modeling software or separate post-processing software.

Reference

1. Chen, H.L.; Chuang, S.Y.; Lin, C.H.; Lin, Y.H. Using colloidal lithography to fabricate and optimize sub-wavelength pyramidal and honeycomb structures in solar cells. Opt. Express 2007, 15, 14793–14803.

2. Chuang, S.Y.; Chen, H.L.; Shieh, J.; Lin, C.H.; Cheng, C.C.; Liu, H.W.; Yu, C.C. Nanoscale of biomimetic moth eye structures exhibiting inverse polarization phenomena at the brewster angle. Nanoscale 2010, 2, 799–805.

3. Yee, K.S. Numerical solution of initial boundary value problems involving maxwell’s equations in isotropic media. IEEE Trans. Antennas Propag. 1966, 14, 302–307.

4. Taflove, A.; Brodwin, M.E. Numerical-solution of steady-state electromagnetic scattering problems using time-dependent maxwells equations. IEEE Trans. Microw. Theory Tech. 1975, 23, 623–630.

5. Taflove, A.; Hagness, S.C. Computational Electrodynamics: The Finite-Difference Time-Domain Method, 3rd ed.; Artech House, Inc.: Norwood, MA, USA, 2005.

6. Yamauchi, J.; Mita, M.; Aoki, S.; Nakano, H. Analysis of antireflection coatings using the FD-TD method with the PML absorbing boundary condition. IEEE Photonics Technol. Lett. 1996, 8, 239–241.

7. Yamauchi, J.; Ando, T.; Nakano, H. Analysis of dielectric hollow slab wave-guides using the finite-difference beam-propagation method. IEICE Trans. Electron. 1993, E76C, 1695–1697.

8. Yang, Z.Y.; Zhu, D.Q.; Zhao, M.; Cao, M.C. The study of a nano-porous optical film with the finite difference time domain method. J. Opt. A Pure Appl. Opt. 2004, 6, 564–568.

9. Tsai, H.Y. Finite difference time domain analysis of three-dimensional sub-wavelength structured arrays. Jpn. J. Appl. Phys. 2008, 47, 5007–5009.

10. Berenger, J.P. A perfectly matched layer for the absorption of electromagnetic-waves. J. Comput. Phys. 1994, 114, 185–200.

11. Deinega, A.; Valuev, I.; Potapkin, B.; Lozovik, Y. Minimizing light reflection from dielectric textured surfaces. J. Opt. Soc. Am. A 2011, 28, 770–777.

12. Deinega, A.V.; Konistyapina, I.V.; Bogdanova, M.V.; Valuev, I.A.; Lozovik, Y.E.; Potapkin, B.V. Optimization of an anti-reflective layer of solar panels based on ab initio calculations. Russ. Phys. J. 2009, 52, 1128–1134.

13. Ting, C.J.; Chen, C.F.; Chou, C.P. Antireflection subwavelength structures analyzed by using the finite difference time domain method. Optik 2009, 120, 814–817.

14. Chou, T.H.; Cheng, K.Y.; Chang, T.L.; Ting, C.J.; Hsu, H.C.; Wu, C.J.; Tsai, J.H.; Huang, T.Y. Fabrication of antireflection structures on tco film for reflective liquid crystal display. Microelectron. Eng. 2009, 86, 628–631.

15. Feng, N.N.; Zhou, G.R.; Huang, W.P. Space mapping technique for design optimization of antireflection coatings in photonic devices. J. Lightwave Technol. 2003, 21, 281–285.

16. Li, Z.F.; Ozbay, E.; Chen, H.B.; Chen, J.J.; Yang, F.H.; Zheng, H.Z. Resonant cavity based compact efficient antireflection structures for photonic crystals. J. Phys. D 2007, 40, 5873–5877.

17. Zhou, G.R.; Li, X.; Feng, N.N. Design of deeply etched antireflective waveguide terminators. IEEE J. Quantum Electron. 2003, 39, 384–391.

18. Deinega, A.; Valuev, I.; Potapkin, B.; Lozovik, Y. Antireflective properties of pyramidally textured surfaces. Opt. Lett.2010, 35, 106–108.

19. Schmid, J.H.; Cheben, P.; Janz, S.; Lapointe, J.; Post, E.; Xu, D.X. Gradient-index antireflective subwavelength structures for planar waveguide facets. Opt. Lett. 2007, 32, 1794–1796.

20. Catchpole, K.R.; Mokkapati, S.; Beck, F.; Wang, E.C.; McKinley, A.; Basch, A.; Lee, J. Plasmonics and nanophotonics for photovoltaics. MRS Bull. 2011, 36, 461–467.

21. Ichikawa, H. Subwavelength triangular random gratings. J. Mod. Opt. 2002, 49, 1893–1906.

22. Ting, C.J.; Chen, C.F.; Hsu, C.J. Subwavelength structured surfaces with a broadband antireflection function analyzed by using a finite difference time domain method. Optik 2010, 121, 1069–1074.

23. Park, H.; Shin, D.; Kang, G.; Baek, S.; Kim, K.; Padilla, W.J. Broadband optical antireflection enhancement by integrating antireflective nanoislands with silicon nanoconical-frustum arrays. Adv. Mater. 2011, 23, 5796–5800.

24. Ting, C.J.; Chen, C.F.; Chou, C.P. Subwavelength structures for broadband antireflection application. Opt. Commun.2009, 282, 434–438.

25. Son, J.; Verma, L.K.; Danner, A.J.; Bhatia, C.S.; Yang, H. Enhancement of optical transmission with random nanohole structures. Opt. Express 2011, 19, A35–A40.

26. Deniz, H.; Khudiyev, T.; Buyukserin, F.; Bayindir, M. Room temperature large-area nanoimprinting for broadband biomimetic antireflection surfaces. Appl. Phys. Lett. 2011, 99, 183107:1–183107:3.

27. Yi, J.; Lee, D.H.; Park, W.I. Site-specific design of cone-shaped Si nanowires by exploiting nanoscale surface diffusion for optimal photoabsorption. Chem. Mater. 2011, 23, 3902–3906.

28. Ting, C.J.; Chang, F.Y.; Chen, C.F.; Chou, C.P. Fabrication of an antireflective polymer optical film with subwavelength structures using a roll-to-roll micro-replication process. J. Micromech. Microeng. 2008, 18.

29. Mokkapati, S.; Beck, F.J.; Polman, A.; Catchpole, K.R. Designing periodic arrays of metal nanoparticles for light-trapping applications in solar cells. Appl. Phys. Lett. 2009, 95.

30. Mokkapati, S.; Beck, F.J.; de Waele, R.; Polman, A.; Catchpole, K.R. Resonant nano-antennas for light trapping in plasmonic solar cells. J. Phys. D 2011, 44

31. Nagel, J.R.; Scarpulla, M.A. Enhanced absorption in optically thin solar cells by scattering from embedded dielectric nanoparticles. Opt. Express 2010, 18, A139–A146.

THE APPLICATIONS OF THE SIMULATION COMPUTER IN NANOTECHNOLOGY

The article discusses the problem of calculation methods used in solving problems of nanotechnology - computer simulation methods. Also illustrated will be simulation results based on simulations computer. In the nano and micro scale the calculation methods differ from used in macros. One of them is the Molecular Dynamics (MD) method. which we present in the following paper as well as the results of simulations carried out by this method, concerning nano-flows of water. Numerical modeling is today one of the most promising and developing the fields of engineering. Its main advantage is the possibility of obtaining a solution of the given a problem that would otherwise be solved by experimental methods. In recent years, the rapid development of nanotechnology has been observed. nanotechnology is a field of study dealing with materials and systems whose structures and elements exhibit peculiar characteristics well developed physically, chemically and biologically, Their processes are caused by their nanoparticles. The goal of nanotechnology is to use these properties by achieving control on the atomic and molecular levels of molecules and developing effective their production and use. In nanotechnology issues, the model of a continuous medium cann’t be used as well as the calculation methods based on this model. Computer simulations have become an excellent tool for solving many problems related to static physics, material chemistry and biophysics. In addition, computer simulation is the only reasonable alternative to analyzing the phenomenon where the construction of a reliable analytical model and the execution of an experiment is impossible or very difficult [1].It is worth emphasizing that computer simulations require some parameters which characterize the modeled system and either come from theoretical or are experimental data [2].

The deterministic method is based on the internal dynamics of the model to move the system in phase space. To move the system through The equation of motion must be formulated and completed over time. In case of The collection of particles subject to the laws of classical mechanics leads to trajectories in the phase space at fixed initial positions and shoots [1]. In stochastic methods a slightly different approach is used. It is based on The fact that in fact it is necessary to designate only a configurable part issues. You can always cycle and turn off. Transition from one convention to the next, which in deterministic terms was determined by values in stochastic methods is realized as a result of probabilistic evolution through the Markov process. The advantage of this approach is the ability to carry out Simulations on models with no internal dynamics. Both methods are complementary in nature and lead to the same average size static provided the considered system is ergodic and is used the same statistical team [2].

Molecular dynamics is a method of numerical integration of equations of motion of multiparticulates [3]. Each particle forming the system is subject to the classical laws of motion, and the macroscopic parameters describing the state of the system are calculated as the mean after the trajectory in the phase space. Functional description MD:At each time step we calculate for each particle the force acting on it derived from other particles;We use calculated forces and know the position of the particles in the previous step we calculate new positions and shoots of each particle numerically solving equations Newtonian movement;After determining the microscopic parameters In several steps, we can calculate macroscopic quantities [4]. As we mentioned in the introduction, Molecular Dynamics requires description of molecules and forces interacting between them. Simulation of Molecular Dynamics is reduced to Linking equations of motion for systems composed of several hundred to several million molecules. In addition, several thousand time steps are required. Trajectories The molecules in the calculation represent the actual molecular trajectories. Molecular Dynamics is a computer simulation technique that describes the pace of evolution a set of interacting atoms. In MD we follow the laws of mechanics classica:

$$F_I\,(t) = m_i\;a_i\;(t)$$

Since every atom and system is made up of N atoms, I am mass atom,

$$a_i = \frac{d^2\,r_i}{dt^2}$$

It is acceleration, Fi is the force acting by interacting with other atoms.

If we express the force derived the α atom from the molecule and onto the β atom from the molecule j as fiαjβ then all the forces acting on the molecule are:

$$F_i = \sum_j \sum_\beta \sum_\alpha f_{i\alpha j\beta}$$

Torque is expressed as:

$$N_i = \sum_\alpha (r_{i\alpha} - R_i) \times f_{i\alpha}$$

where,

$$R_i = {}^{1}/_{M_i} \sum_\alpha m_{i\alpha}\, r_{i\alpha}$$

is the center of mass of the molecule and. Motion is defined by the Newton-Euler equations:

$$M_i \ddot{R}_1 = F_i$$

$$I_i \cdot \omega_i - \omega_i \times I_i \cdot \omega_i = N_i$$

where ω_i is the angular velocity of the molecule,

$$I_i = \sum_\alpha m_{i\alpha}\left(p_{i\alpha}^2 1 - p_{i\alpha} p_{i\alpha}\right)$$

is a tensor of inertia,

$p_{i\alpha} = r_{i\alpha} - R_i$

is the coordinate of the atom in relation to the center of mass.

The position of the molecules can be represented by the quaternions as they are present is widely used. Pearls are more preferred than Euler angles for two reasons. First, they lead to equations of motion, which is free, in particular, This means that no special coding case is required. This leads to improve the numerical stability of the simulation. Second, the combination of molecular symmetry and rotation is elegantly expressive. under the conditions of a simple algebra of quaternions [5].

Literature

1. Heermann W.D., Computer Simulation Method in Theoretical Physics, Springer Verlag, Berlin 1990.
2. Grotendorst J., Marx D., Muramatsu A., Quantum Simulations of Complex Many-Body Systems: From Theory to Algorithms, John von Neumann Institute for Computing, Jlich, NIC Series, Vol. 10, ISBN 3-00-009057-6, pp. 211-254, 2002
3. Allan M.P., Tildesley D.J., Computer simulations of Liquids, Oxford University Press, 1989.
4. Kucaba-Piętal A., Modelowanie mikroprzepływów na gruncie teorii płynów mikro polarnych, Oficyna Wydawnicza Politechniki Rzeszowskiej, 2004.
5. Refson K., Moldy User’s Manual.Chapter II, ftp://ftp.earth.ox.ac.uk/pub
6. **Ihor Ohirko. Olexandra Romaniuk. Deformation. Thermosoftening plastic. University "Lviv Stavropigion". Institute for Eastern Europe. Lviv. 2014. s.59 .ISBN 978-966-2037-17-4.**
7. **Ihor Ohirko , Sofia Kaschevska. Modelowanie matematyczne. Administracja publiczna. Informatyka medyczna. Institute for Eastern Europe.Університет Львівський Ставропігіон",Lviv 2014 . s.75 ISBN 978-966-2037-17-5.**
8. **Ohirko I. V. Ohirko O. I. Yasinska-Damri L. M. Yasinskyi M. F. Information technologies and models of corrosion measurement for surface layers of metals. Scientific Papers Ukrainian Academy of Printing. 2016 .№ 1 (52) S.69-77. ISSN 1998-6912**
9. **Kucherov D.P., Ohirko I.V., Ohirko O.I., Golenkovskaya T.I. Neural Network technologies for recognition characters. Electronics and control systems. "National Aviation University"– № 4 (46). – 2015. – P. 65-71.ISSN: 1990-5548.**
10. **Ihor Ohirko, Michaił Yasinsky, Ludmiła Yasinska-Damri, Olga Ohirko. Models of Geometrical Optics and Lenticular Printing: "Computer Technologies of Printing ".Volume: 2 .Ukrainian Academy of Printing . 2015. – P. 205-213.ISSN: 2411-9210.**

11. W. Wysoczansky, A. Oliejnik, I. Ohirko. MATHEMATICAL MODELLING OF DIFFUSION PROCESSES IN THE SHALE GAS PRODUCTION TECHNOLOGY. Instytut Budownictwa, PSW im. Papieża Jana-Pawła II. „TELECOTRON INTERNATIONAL".WARSZAWA .2016. Pg. 22.ISBN 978-83-932045-2-6-0.

12. D. P. Kucherov, I. V. Ogirko, O. I. Ogirko. Calculation of integrals by Monte Carlo in the illumination problem of synthesized objects. SCIENCE AND EDUCATION A NEW DIMENSION. Natural and Technical Sciences, IV (11), Issue: 96, BUDAPEST. 2016. 42-47 ISSN 2308-1996

13. Joanna Masiewicz, Ihor Ohirko. Matematyka stosowana w nanotechnologii. Uniwersytet Technologiczno-Humanistyczny im. K. Pułaskiego w Radomiu. Wydział Informatyki i Matematyki. Artykuł naukowy. Opublikowane e-publikácie.http://dr-joannamasiewicz.blog.pl/ 13 października 2017 .

14. M. Snopczyński, I. Ogirko. Technologia spiekania laserowego proszków metalowych DMLS. Uniwerystet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu. e-publikácie.http://dr-snopczynski-m.blog.pl/ 13 października 2017.

15. Urban Paulina, Ihor Ohirko .Time-Based Optical Modeling Methods.E-publication. Kazimierz Pułaski University of Technology and Humanities in Radom. Department of Computer Science and Mathematics. http://dr-urban.bloog.pl/id,363922086,title,Time-Based-Optical-Modeling-Methods,index.html .11.11.2017. 9 S.

16. Ohirko Ihor. Statistical methods for assessing the quality of electronic publications. / / Proceedings of the Conference UAH works..// В зб.: Матеріали науково-практичної конференції УАД. Львів. УАД. 2013. с.106.

17. OHIRKO Igor, ZANIEWSKI Igor, OGIRKO Olga. Modelowanie i symulacja w naukach ekonomicznych. Czasopisma Autobusy z artykułami z Konferencji LogiTrans 2016, Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu, Organizacja i zarządzanie. 6 / 2016 . S.1742-1747.ISSN 1509-5878

Інститут Східної Європи

Eastern-European Institute

www.easterneurope.nethouse.ua

E-mail:ukrainoznavezz@ukr.net

Ihor Ohirko. APPLIED MATHEMATICS FOR MATHEMATICS.
Physics and Mathematical Journal. №3.
Institute of Eastern Europe. - Lviv, 2018.

Видавництво Інституту Східної Європи

Львів 2018р.

ББК 82.3

Друкується за рішенням Вченої Ради Інституту Східної Європи

Протокол № 19, від 4 січня 2018 року.

Фізико-математичний вісник

Інституту Східної Європи

№3 - Львів, 2018р.

Фізико - математичний вісник Інституту Східної Європи .

Наукові праці вчених країн Східної Європи, рецензії та інформаційні статті.

E-mail: ukrainoznavezz@ukr.net **https://easterneurope.nethouse.ua**

«Connoisseur of Ukraine» ISBN 978 - 966 - 665 - 570 - 1 7