4 Реферати

УДК 004.684.3

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

Михайло Прокофьєв, Володимир Хорошко*
НДЦ «ТЕЗІС» НТУУ «КПІ»
**Національний авіаційний університет*

Стаття: ***6 стор., 5 джерел.***

На підставі системного і предметного аналізу змісту і раціональних шляхів здійснення функцій захисту інформації в Україні сформовані десять завдань щодо створення системно-повних механізмів захисту (функцій першого виду, які мають на меті створення механізмів захисту) і чотири класи завдань з забезпечення безперервного і оптимального управління механізмами захисту (функції другого виду, які мають на меті управління механізмами захисту). Для подальшого розвитку системи технічного захисту інформації (ТЗІ) слід постійно вирішувати задачі, що стосуються усього комплексу проблем у сфері ТЗІ. Виділяють умовно такі групи: правові, нормативно-методичні, технічні, організаційні та метрологічні.

За результатами аналізу законодавчої бази України в галузі інформаційних відносин виділені основні правові проблеми загальної системи захисту інформації. Серед них виділяють: відсутність чіткого визначення прав та обов'язків учасників інформаційних відносин, недостатньо чітка регламентація виникнення права власності на інформацію та визначення видів, типів, обсягів інформації з обмеженим доступом, що не становить державну таємницю, відсутність чіткої деталізації правових норм, що визначають право особистості розпоряджатися інформацією про себе.

Показано, що визначення конкретної моделі загроз інформації на об’єкті та її комплексування з загальною моделлю загроз, яка буде описувати у вигляді математичних моделей реальні технічні канали витоку інформації, технічні засоби захисту і процеси захисту інформації, дозволяє створити замкнену систему моделювання конфліктної боротьби – систем розвідки і захисту. Засоби ТЗІ повинні створюватися з урахуванням обставин, які визначають необхідність концентрації наукових та інженерних зусиль для вирішення проблем розвитку технічних розвідок в умовах певної невизначеності інформації про них, оцінювання інформативності можливих технічних каналів витоку інформації в умовах їх комплексування.

Для успішного вирішення організаційних проблем доцільно виділити з них одну, а саме створення системи підготовки, підвищення кваліфікації та перепідготовки фахівців з питань ТЗІ.

З позицій метрології зазначено, що в діючих на сьогодні нормативних документах у сфері ТЗІ не регламентується вживання уніфікованих показників точності результатів вимірювань (випробувань). Вони спираються на різні методи їх оцінювання, відображають різні підходи до вирішення вимірювальних завдань і тому погано узгоджуються один з одним. Недостатньо уваги приділено визначенню кваліфікації виконавців робіт у сфері ТЗІ. Все це не сприяє забезпеченню єдиного підходу до проведення випробувань (інструментального контролю та атестації) в системі ТЗІ, що може призвести до недостовірних результатів при проведенні вимірювань значень параметрів побічних випромінювань та наведень. Відсутність в документації на проведення випробувань умов і характеристик, при яких були визначені декларовані параметри, роблять неможливим коректний перерахунок відповідних величин.

В цілому всі названі і багато інших проблем можуть бути вирішені тільки в результаті створення нормально функціонуючої національної системи ТЗІ.

ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В УКРАИНЕ

Михаил Прокофьев, Владимир Хорошко*
НИЦ «ТЕЗИС» НТУУ «КПИ»
**Национальный авиационный университет*

На основании системного и предметного анализа содержания и рациональных путей осуществления функций защиты информации в Украине сформированы десять задач по созданию системно-полных механизмов защиты (функции первого вида, имеют целью создание механизмов защиты) и четыре класса задач по обеспечению непрерывного и оптимального управления механизмами защиты (функции второго вида,

имеют целью управления механизмами защиты). Для дальнейшего развития системы технической защиты информации (ТЗИ) следует постоянно решать задачи, касающиеся всего комплекса проблем в сфере ТЗИ. Выделяют условно следующие группы: правовые, нормативно методические, технические, организационные и метрологические.

По результатам анализа законодательной базы Украины в области информационных отношений выделены основные правовые проблемы общей системы защиты информации. Среди них выделяют: отсутствие четкого определения прав и обязанностей участников информационных отношений, недостаточно четкая регламентация возникновения права собственности на информацию и определение видов, тип, объемов информации с ограниченным доступом, не составляющей государственную тайну, отсутствие четкой детализации правовых норм, определяющих право личности распоряжаться информацией о себе.

Показано, что определение конкретной модели угроз информации на объекте и ее комплексирование с общей моделью угроз, которая будет описывать в виде математических моделей реальные технические каналы утечки информации, технические средства защиты и процессы защиты информации, позволяет создать замкнутую систему моделирования конфликтной борьбы – систем разведки и защиты. Средства ТЗИ должны создаваться с учетом обстоятельств, которые определяют необходимость концентрации научных и инженерных усилий для решения проблем, связанных с развитием технических разведок в условиях некоторой неопределенности информации о них, оценка информативности возможных технических каналов утечки информации в условиях их комплексирования.

Для успешного решения организационных проблем целесообразно выделить из них одну, а именно создание системы подготовки, повышения квалификации и переподготовки специалистов по вопросам ТЗИ.

С позиций метрологии указано, что в действующих на сегодня нормативных документах в сфере ТЗИ не регламентируется применение унифицированных показателей точности результатов измерений (испытаний). Они опираются на различные методы их оценки, отражающие различные подходы к решению измерительных задач и поэтому плохо согласуются друг с другом. Недостаточно внимания уделено определению квалификации исполнителей работ в сфере ТЗИ. Все это не способствует обеспечению единства испытаний (инструментального контроля и аттестации) в системе ТЗИ, что может привести к недостоверным результатам при проведении измерений значений параметров побочных излучений и наводок. Отсутствие в документации на проведение испытаний условий и характеристик, при которых были определены декларируемые параметры, делают невозможным корректный пересчет соответствующих величин.

В целом все названные и многие другие проблемы могут быть решены только в результате создания нормально функционирующей национальной системы ТЗИ.

PROBLEMS OF INFORMATION SECURITY IN UKRAINE

Mikhail Prokofiev, Vladimir Khoroshko*
NIC "THESIS" NTUU "KPI"
**National Aviation University*

Based on a systematic and objective analysis of the content and rational ways of the functions of information security in Ukraine were formed ten tasks on creating a systematic and comprehensive protection mechanisms (functions of the first kind, aimed to create mechanisms of protection) and four classes of tasks to ensure continuous and optimal control of protection mechanisms (functions of the second kind, which are designed to control the mechanisms of protection). For further development of technical protection of information (TPI) should permanently be solved the tasks concerning the entire complex of problems in TPI. There are roughly following groups: legal, regulatory and methodological, technical, organizational and metrology.

The analysis of the legal framework of Ukraine in the sphere of information relations identified the main legal problems of general information security system. Among them: are marked the lack of a clear definition of the rights and obligations of participants in information relationships, not precise regulation of property rights to information and determine the species, types and volumes of information with limited access, which is not a state secret, the lack of clear detail specifications of legal rules, defining the right of the individual to manage information about themselves.

It is shown that the definition of specific model of threats for information on the object and its integration with general model of threats that will describe as mathematical models real technical information leakage, hardware protection and information security processes allow to create a closed system simulation combat conflict - of intelligence and security. TPI tools should be established taking into account the circumstances that determine the need for concentration of scientific and engineering efforts to solve the problems of technical intelligence in some

circumstances of uncertainty information about them informative assessment of possible technical information leakage in terms of their combining.

To solve organizational problems it is advisable to select one of them, namely the creation of training system, training and retraining for specialists in TPI questions.

From the standpoint of metrology noted that existing regulations currently in TPI is not regulated the use of standardized indicators accuracy of measurement (tests). They rely on different methods of their assessment, reflecting different approaches to solve measurement tasks and therefore poorly compatible with each other. Insufficiently attention is given to the definition of qualification of executors in TPI sphere. All this do not contribute to unity tests (tool control and certification) in TPI system that can lead to unreliable results during parameters measurement of secondary emission and inducting. The lack of documentation on testing conditions and characteristics for which were determined declared parameters make it impossible the correct recalculation of relevant variables.

In general, all named and many other problems can be solved only by creating a well-functioning national system of TPI.

Spysok vykorystanoi literatury. ***1.*** *Lenkov S. V. Metodы y sredstva zashchytы ynformatsyy. V 2-kh tomakh /Lenkov S. V., Perehudov D. A., Khoroshko V. A.– K.: Aryi,2008.* ***2.*** *Emelianov S. L. Problemы zashchytы ynformatsyy ot utechky y puty ee reshenyia / Emelianov S. L.– Odessa: Feniks, 2011. – s. 624* ***3.*** *Artemov V. Yu. Normatyvno-pravovyi dovidnyk z okhorony informatsii v Ukraini. U 4-kh tomakh / Artemov V. Yu., Lienkov O. S., Pashkov A. S., Stadnik O. M., Khoroshko V. O. – K.: Vyd. DUIKT, 2010.* ***4.*** *Babak V. P. Teoretycheskye osnovы zashchytы ynformatsyy / Babak V. P., Kliuchnykov A. A. – NAN Ukraynы, Yn-t problem bezopasnosty AЭS.– Chernobыl (Kyev.obl.): Yn-t problem bezopasnosty AЭS, 2012.– s.776* ***5.*** *Khoroshko V. O. Metodychne zabezpechennia pidhotovky ta perepidhotovky spetsialistiv z informatsiinoi bezpeky / Khoroshko V. O., Oriekhova I. I. // Suchasna spetsialna tekhnika, #3, 2011. – S. 22-27.*

УДК 004.773

ІНФОРМАЦІЙНА БЕЗПЕКА В СОЦІАЛЬНИХ МЕРЕЖАХ. МЕТОДИ ПОШИРЕННЯ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

Дмитро Мехед
Чернігівський національний технологічний університет

Стаття: ***5 стор, 7 джерел.***

Розвиток електронних технологій дозволяє мільйонам людей вільно користуватись мережею, що дає змогу використовувати їх творчий потенціал для вирішення інтелектуальних, наукових, суспільно значимих питань. В силу причин, описаних у даній статті, можна зробити висновок, що тема захисту інформації користувачів в соціальних мережах залишатиметься актуальною як мінімум в найближчі роки. Проблеми захисту інформації в даній сфері досі остаточно не вирішені і можуть вирішитися тільки в результаті комплексного підходу, що включає в себе спільну роботу творців і розробників мережі, користувачів і держави. Особливого значення набуває питання захисту інформації на фоні формування горизонтальних, корпоративних зв'язків з використанням електронних технологій, зокрема у сфері освіти, а також серед наукової спільноти.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СОЦИАЛЬНЫХ СЕТЯХ. МЕТОДЫ РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ В СОЦИАЛЬНЫХ СЕТЯХ

Дмитрий Мехед
Черниговский национальный технологический университет

Развитие электронных технологий позволяет миллионам людей свободно пользоваться сетью, что позволяет использовать их творческий потенциал для решения интеллектуальных, научных, общественно-значимых вопросов. В силу причин, описанных в данной статье, можно сделать вывод, что тема защиты

информации пользователей в социальных сетях будет оставаться актуальной как минимум в ближайшие годы. Проблемы защиты информации в данной сфере до сих пор окончательно не решены и могут решиться только в результате комплексного подхода, включающего в себя совместную работу создателей и разработчиков сети, пользователей и государства. Особое значение приобретает вопрос защиты информации на фоне формирования горизонтальных, корпоративных сетей с использованием электронных технологий, в частности в сфере образования, а также среди научного сообщества.

INFORMATION SECURITY IN SOCIAL NETWORKS. METHODS FOR DISSEMINATION IN SOCIAL NETWORKS

Dmytro Mekhed
Chernihiv National University of Technology

The development of electronic technology allowing millions of people to use a network that allows you to use their creativity to solve intellectual, scientific, socially important issues. Due to reasons described in this article, one can conclude that the issue of protection of user information in social networks at least remain relevant in the coming years. The problems of data protection in this area is still not completely resolved and may decide only through a comprehensive approach that includes collaboration creators and developers of network users and the state. Of particular importance is the protection of information on the background of the formation of horizontal, Corporate Communications using electronic technologies, particularly in education, as well as among the scientific community.

Spysok vykorystanoi literatury. 1. Sotsialni merezhi yak chynnyk rozvytku hromadianskoho suspilstva : [monohrafiia] / [O. S. Onyshchenko, V. M. Horovyi, V. I. Popyk ta in.] ; NAN Ukrainy, Nats. b-ka Ukrainy im. V. I. Vernadskoho. – K., 2013. – 220 c. 2. Typove polozhennia pro sluzhbu zakhystu informatsii v avtomatyzovanii systemi. – Rezhym dostupu: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article? art_id=39738&cat_id=38. 3. Sotsialna merezha (Internet) . – Rezhym dostupu: https://uk.wikipedia.org/wiki /Sotsialna_merezha_(internet) 4. Balovsiak N. Sotsialni merezhi vbyvaiut pryvatnist / Tyzhden.ua., 2013/ - Rezhym dostupu: http://tyzhden.ua/Society/70950. 5. Barnes J. A. Class and Committees in a Norwegian Island Parish // Human Relations. 1954. #7. Pp. 39-58. 6. Cotsialni merezhi – realni zahrozy virtualnoho svitu. – Rezhym dostupu: http://ogo.ua/articles/view/2011-02-23/26490.html. 7. Kak sotsyalnыe sety razrushaiut brak. – Rezhym dostupu: http://letidor.ru/article/kak_sotsialnye_seti_razrushayu_138521/

УДК 004.621.5

ОПТИМІЗАЦІЯ АРХІТЕКТУРИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ СУПР

Володимир Бурячок, Андрій Орєхов, Володимир Хорошко
Національний Авіаційний Університет

Стаття: ***3 стор., 3 джерела***

Важливим є питання оптимізації та уніфікації підходів до реалізації заходів щодо забезпечення інформаційної безпеки. Особливу роль відіграє при цьому правильний вибір архітектури системи захисту. Метою захисту інформації в системі управління повітряним рухом (СУПР) є діяльність, спрямована на запобігання витоку її різними каналами. Основною стратегією захисту інформації є вибір основних важливих базових системно-концептуальних положень. При спробі подолати захист зловмисник спробує використати найбільш слабкий напрям або рубіж в цій системі. З цієї причини підсумкова міцність системи комплексного захисту інформації (СКЗІ) буде визначатися міцністю найбільш слабкого напрямку або рубежу в цій системі. Отже, якщо міцність слабкої ланки, рубежу або напрямку не задовольняє заданим і необхідним рівням, то ця ланка, рубіж або напрямок зміцнюється або замінюється на більш міцний.

Під завданням синтезу СКЗІ розуміється етап формування профіля захищеності інформаційного простору. У загальному вигляді задача синтезу зводиться до формування оптимального варіанта реалізації профілю захищеності, що забезпечує максимум запобігання шкоди від впливу загроз при допустимих витратах на створення СКЗІ інформаційного простору (ІП) СУПР.

При складанні моделі загроз враховується також оточення функціонування ІП СУПР. Формування моделі загроз можна здійснити із застосуванням автоматизованих діалогових засобів при одночасній участі

експертів. Для цього передбачається розробка спеціального запитальника з використанням декількох варіантів відповідей на кожне питання, який би враховував всі можливі загрози і всі випадки застосування того чи іншого критерію. На підставі експертної інформації, що визначає перевагу того чи іншого показника, та інформації про характеристики загроз проводиться визначення коефіцієнтів відносної важливості виконання j-ої вимоги для усунення і-ої загрози. З отриманих таким чином коефіцієнтів формується матриця лінгвістичних змінних, що містить формалізований опис вимог і середовища безпеки.

Застосовуючи до отриманої матриці нечіткі арифметичні операції визначаємо важливість вимог, що пред'являються до системи захисту інформації. Параметри (вимоги) визначаються виходячи із заданих цілей. Далі необхідно визначити ступінь взаємозв'язків і взаємовідносин між ними. Характер цієї взаємозалежності впливає на вибір методу.

При вирішенні практичних завдань обґрунтування вимог та оцінки СКЗІ виникає питання раціонального вибору методу визначення вагових коефіцієнтів з числа існуючих методів.

Вибір методу рішення багатокритеріальної задачі залежить від того, в якому вигляді представлена експертна інформація про перевагу показників, а також від ступеня їх важливості.

Застосування даної методики формування профілю захищеності дозволяє здійснювати вибір оптимального варіанта побудови СКЗІ на основі експертної оцінки вимог і безпекового середовища, а також сформувати адекватний загрозам безпеки профіль захищеності для подальшого його реалізації в системі безпеки. Одночасно з цим в силу своєї універсальності можливе застосування даного методу і для проведення оцінки вже створеної системи безпеки на предмет виконання заданих функцій.

ОПТИМИЗАЦИЯ АРХИТЕКТУРЫ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА СУВД

Владимир Бурячок, Андрей Орехов, Владимир Хорошко
Национальный Авиационный Университет

Важным является вопрос оптимизации и унификации подходов к реализации мероприятий по обеспечению информационной безопасности. Особую роль играет при этом правильный выбор архитектуры системы защиты. Целью защиты информации в системе управления воздушным движением (СУВД) является деятельность, направленная на предотвращение утечки ее по различным каналам. Основной стратегией защиты информации является выбор основных важных базовых системно-концептуальных положений. При попытке преодолеть защиту злоумышленник попытается использовать наиболее слабое направление или рубеж в этой системе. По этой причине итоговая прочность системы комплексной защиты информации (СКЗИ) будет определяться прочностью наиболее слабого направления или рубежа в этой системе. Следовательно, если прочность слабого звена, рубежа или направления не удовлетворяет заданным и требуемым уровням, то это звено, рубеж или направление укрепляется или заменяется на более прочный.

Под задачей синтеза СКЗИ понимается этап формирования профиля защищенности информационного пространства. В общем виде задача синтеза сводится к формированию оптимального варианта реализации профиля защищенности, обеспечивающего максимум предотвращенного ущерба от воздействия угроз при допустимых затратах на создание СКЗИ информационного пространства (ИП) СУВД.

При составлении модели угроз учитывается также окружение функционирования ИП СУВД. Формирование модели угроз можно осуществить с применением автоматизированных диалоговых средств при одновременном участии экспертов. Для этого предполагается разработка специального вопросника с использованием нескольких вариантов ответов на каждый вопрос, который бы учитывал все возможные угрозы и все случаи применения того или иного критерия. На основании экспертной информации, определяющей предпочтение того или иного показателя, и информации о характеристиках угроз производится определение коэффициентов относительной важности выполнения *j*-ого требования для устранения *i*-ой угрозы. Из полученных таким образом коэффициентов формируется матрица лингвистических переменных, содержащая формализованное описание требований и среды безопасности.

Применяя к полученной матрице нечеткие арифметические операции определяем важность требований, предъявляемых к системе защиты информации. Параметры (требования) определяются исходя из заданных целей. Далее необходимо определить степень взаимосвязей и взаимоотношений между ними. Характер этой взаимозависимости влияет на выбор метода.

При решении практических задач обоснования требований и оценки СКЗИ возникает вопрос рационального выбора методов определения весовых коэффициентов из числа существующих методов.

Выбор метода решения многокритериальной задачи зависит от того, в каком виде представлена экспертная информация о предпочтении показателей, а также от степени их важности.

Применение данной методики формирования профиля защищенности позволяет осуществлять выбор оптимального варианта построения СКЗИ на основе экспертной оценки требований и среды безопасности, а также сформировать адекватный угрозам безопасности профиль защищенности для последующей его реализации в системе безопасности. Одновременно с этим в силу своей универсальности возможно применение данного метода и для проведения оценки уже созданной системы безопасности на предмет выполнения заданных функций.

ARCHITECTURE OPTIMIZATION PROTECTION SYSTEMS INFORMATION SPACE ATCS

Vladimir Buryachok, Andrey Orekhov, Vladimir Khoroshko
National Aviation University

An important question is the optimization and harmonization of approaches to the implementation of measures to ensure information security. It plays a special role in this case the right choice of the system architecture of protection. The purpose of information security is ATCS activities aimed at preventing diversion of it through various channels and their blocking. The main strategy for the protection of information is a basic range of important basic concepts of the systemic. When you try to overcome the protection the attacker will try to use the weakest area or abroad in this system. For this reason, the total strength of a comprehensive information protection (SCIP) will be determined by the strength of the weakest areas or abroad in this system.

Since the final strength of the SCIP determined by the strength of the weakest link, the turn or direction in this system, it follows that if the strength of the weak link, the turn or direction and do not match the desired level, it is the link line or direction is strengthened or replaced by a more durable.

Under the task of synthesis of complex information security systems mean the step of forming the profile of the security of information space. In general, the synthesis problem is reduced to the formation of the optimal embodiment of the security profile that ensures maximum prevented damage from exposure to threats in the eligible costs for the establishment of SCIP information space ATCS.

In drawing up the threat model also takes into account the environment of functioning IP ATCS. Formation of the threat model can be carried out using automated means of dialog, while the participation of experts. For this is supposed to develop a special questionnaire with multiple response options for each question, which would consider all possible threats, and all instances of a particular criterion. On the basis of expert information, which determines the preference of an indicator and information on the characteristics of the threat is determined coefficients of the relative importance of implementation of the *j*-th requirements to remove the *i*-th threat. From the thus obtained coefficients form a matrix of linguistic variables containing formalized description of the requirements and the security environment.

Applying to the resulting matrix fuzzy arithmetic, we determine the importance of the requirements for information security systems. Parameters (requirements) are determined on the basis of defined targets. Next you need to determine the extent of the relationship and the relationship between them. The nature of this interdependence affects the choice of method.

When solving practical problems and assess the requirements of justification SCIP question of rational choice of methods for determining the weighting factors from the existing methods.

Selecting a method for solving multiobjective problem depends on the form in which the information is presented expert preference indicators, as well as to their importance.

Application of this method of forming the profile of security enables the selection of optimal variant of building SCIP based on peer review requirements and security environment, as well as an adequate form of security threats to the security profile for the subsequent implementation of its security system. At the same time due to its versatility is possible to use this method and to assess the already established safety system for performing the specified functions.

Spysok vykorystanoi literatury: 1. Lenkov S. V. Metodы y sredstva zashchytы ynformatsyy. V 2-kh tomakh / S. V. Lenkov, D. A. Perehudov, V. A. Khoroshko. – K.: Aryi, 2008. 2. Shtoier R. Mnohokryteryalnaia optymyzatsyia. Teoryia, vыchyslenyia y prylozhenyia / R. Shtoier. – M.: Radyo y sviaz, 1992. – 374 s. 3. InternationalStandartISO/IEC 15408-99.

УДК 551.463.2 + 004.386

НАДЗВИЧАЙНІ СИТУАЦІЇ, ЩО ЗУМОВЛЕНІ ІНФОРМАЦІЙНИМИ ПОТОКАМИ

Олена Азаренко, Юлія Гончаренко, Михайло Дівізінюк, Валерія Ковач
Державна установа «Інститут геохімії навколишнього середовища НАН України»

Стаття: ***5 стор., 8 джерел***

В Україні всі надзвичайні ситуації прийнято розділяти на надзвичайні ситуації техногенного, природного, соціального і військового характеру. Прийнято вважати, що характер надзвичайних ситуацій визначається причинами їх виникнення. Незалежно від виду надзвичайна ситуація, що порушує повсякденну життєдіяльність людей, впливає на техногенне, природне і соціальне середовище, причому просторово-часові масштаби цього впливу визначаються просторово-часовими масштабами надзвичайної ситуації.

Природна складова надзвичайної ситуації – це частина біосфери (навколишнього природного середовища), яка піддається змінам як внаслідок самої катастрофічної події, так і наслідків, викликаних його настанням. Соціальна складова надзвичайної ситуації – це частина соціуму, яка постраждала чи може постраждати від настання катастрофічної події або її наслідків. Техногенна складова надзвичайної ситуації – це частина техносфери, яка опинилася в зоні впливу катастрофічної події, а також технічні засоби і сили, які використовуються для запобігання катастрофічній події, зменшення її впливу в разі настання, локалізації та ліквідації наслідків настання катастрофічної події. Це можуть бути техногенні будови і гідротехнічні споруди, як атомні гідроелектричні станції, нафтохімічні і металургійні комбінати, які, в свою чергу, складаються з технічних засобів меншого масштабу і т. д.

За основним або функціональним призначенням всередині техногенного об'єкту техносферу поділяють на основні (виробничі або виконавчі) структури, керуючі структури і структури забезпечення.

У техносферу також входять засоби зв'язку: стаціонарні і мобільні телефони, телетайп і скайп, електронні засоби передачі інформації. Тут також необхідно використовувати сучасний термін апаратно-програмні засоби, бо жодний сучасний засіб комунікацій не працює без використання інформаційних технологій або більш спрощено – без відповідного програмного забезпечення.

Порушення інформаційних потоків викличе збій в роботі техногенного об'єкту, а надзвичайні ситуації викликані порушеннями інформаційних потоків, які супроводжують і забезпечують роботу підприємства, слід відносити до нового виду надзвичайних ситуацій, зумовлених інформаційними потоками або надзвичайних ситуацій інформаційного характеру.

ЧРЕЗВЫЧАЙНЫЕ СИТУАЦИИ, ОБУСЛОВЛЕННЫЕ ИНФОРМАЦИОННЫМИ ПОТОКАМИ

Елена Азаренко, Юлия Гончаренко, Михаил Дивизинюк, Валерия Ковач
Государственное учереждение «Институт геохимии окружающей среды НАН Украины»

В Украине все чрезвычайные ситуации принято разделять на чрезвычайные ситуации техногенного, природного, социального и военного характера. Принято считать, что характер чрезвычайные ситуации определяется причинами их возникновения. Независимо от вида, чрезвычайная ситуация, нарушающая повседневную жизнедеятельность людей, влияет на техногенную, природную и социальную среду, причем пространственно-временные масштабы этого влияния определяются пространственно-временными масштабами чрезвычайной ситуации.

Природная составляющая чрезвычайной ситуации – это часть биосферы (окружающей природной среды), которая подвергается изменениям, как вследствие самого катастрофического события, так и последствий, вызванных его наступлением. Социальная составляющая чрезвычайной ситуации – это часть социума, которая пострадала или может пострадать от наступления катастрофического события или его последствий. Техногенная составляющая чрезвычайной ситуации – это часть техносферы, которая оказалась в зоне влияния катастрофического события, а также технические средства и силы, используемые для предотвращения катастрофического события, уменьшения его воздействия в случае наступления, локализации и ликвидации последствий наступления катастрофического события. Это могут быть техногенные строения и гидротехнические сооружения, как атомные гидроэлектрические станции,

нефтехимические и металлургические комбинаты, которые, в свою очередь, состоят с технических средств меньшего масштаба и т. д.

По основному или функциональному назначению внутри техногенного объекта, техносферу разделяют на основные (производственные или исполнительные) структуры, управляющие структуры и структуры обеспечения.

В техносферу также входят средства связи: стационарные мобильные телефоны, телетайп и скайп, электронные средства передачи информации. Здесь также необходимо использовать современный термин – аппартно-программные средства, так как ни одно современное средство коммуникаций не работает без использования информационных технологий или более упрощено – без соответствующего программного обеспечения.

Нарушение информационных потоков вызовет сбой в работе техногенного объекта, а чрезвычайные ситуации вызванные нарушениями информационных потоков, сопровождающих и обеспечивающих роботу предприятия, следует относить к новому виду чрезвычайных ситуаций, обусловленных информационными потоками или чрезвычайным ситуациям информационного характера.

EMERGENCIES CAUSED BY INFORMATION FLOWS

Elena Azarenko Yuliia Goncharenko, Michail Divizinyuk, Valeriia Kovach

State Institution "Institute of Environmental Geochemistry NAS of Ukraine"

In Ukraine, all emergencies are divided into man-made emergencies, natural, social and military ones. It is considered that the nature of the emergency is determined by their causes. Regardless of the type of emergency, which affects the daily livelihood of people, affects the industrial, natural and social environment, and spatial and temporal scale of influence is defined by the spatial and temporal scale of the emergency.

A natural component of emergency is part of the biosphere (environment), which is subject to change as a result of the catastrophic events and by caused consequences. The social component of emergency is a part of society, affected or may be affected by the onset of a catastrophic event or its consequences. Technological component of emergency is part of the technosphere, which was in the zone of catastrophic events as well as hardware, used to prevent the catastrophic event, reduce the impact in case of occurrence, localization and liquidation of consequences of catastrophic events. It can be man-made structure and waterworks as Nuclear, Hydroelectric plant, petrochemical and metallurgical plants, which, in turn, consist of smaller technical facilities, etc.

For basic functionality technogenic objects can be divided into basic technosphere (industrial or administrative) structures, control structures and support structures.

In the technosphere are also included communication, fixed mobile telephones, teletypes and Skype, electronic data transmission. You also need to use a modern term equipment and software base, as any modern means of communication does not work without the use of information technology, or more simplified - without appropriate software.

Violation of information flow will cause failure of the technogenic objects, and emergencies caused by impaired information flow accompanying the work and providing the enterprises with readiness to a new kind of emergencies caused by information flows or informational emergencies.

Spysok vykorystanoi literatury: ***1.*** *Terakты: byrzhevoi tovar treteho тыsiacheletyia. – Dostup: http://zonakz.net:8444/articles/4103.* ***2.*** *Kodeks tsyvilnoho zakhystu Ukrainy. Vyd-vo PALYVODA A. V., Kyiv 2015, 132 s.* ***3.*** *Honcharenko Yu. Yu. Otsenka эffektyvnosty upravlenyia chrezvыchainoi sytuatsyei / Yu. Yu. Honcharenko, E. V. Azarenko, Yu. V. Braslavskyi y dr. // Cb. nauch. tr. SNUIaЭyP. – Vыp. 2 (38). – Sevastopol: SNUIaЭyP, 2011. – S. 239 – 245.* ***4.*** *Honcharenko Yu. Yu. Osnovnыe trebovanyia k systeme podderzhky pryniatyia reshenyi po predotvrashchenyiu chrezvыchainыkh sytuatsyi v prybrezhnыkh vodakh / Yu. Yu. Honcharenko, E. V. Azarenko, A. N. Fursenko y dr. // Cb. nauch. tr. SNUIaЭyP. – Vыp. 2 (34). – Sevastopol: SNUIaЭyP, 2010. – S. 216 – 220.* ***5.*** *Honcharenko Yu. Yu. Zashchyta ynformatsyy – kak odyn yz kliuchevыkh aspektov predotvrashchenyia chrezvыchainыkh sytuatsyi / Yu. Yu. Honcharenko, E. E. Sыchkov, V. V. Rыbko // Zbirnyk naukovykh prats SNUIaEtaP. – Sevastopol: SNUIaEtaP, 2012. – Vyp. 1 (41). – S. 207 – 211.* ***6.*** *Honcharenko Yu. Yu. Struktura kontura upravlenyia ynformatsyonnoi bezopasnostiu predpryiatyia / Yu. Yu. Honcharenko // Nauchno-praktycheskyi zhurnal «Эkonomyka y upravlenye». – #5. – Symferopol: NAPKS, 2012. – S. 97 – 101.* ***7.*** *Honcharenko Yu. Yu. Kanalы utechky эkonomycheskoi ynformatsyy predpryiatyia / Yu. Yu. Honcharenko // Nauchno-praktycheskyi zhurnal «Эkonomyka y upravlenye». – #2. – Symferopol: NAPKS, 2013. – S. 83 – 86.* ***8.*** *Honcharenko Yu. Yu. Matematycheskaia model opysanyia nekorrektno postavlennыkh zadach / Yu. Yu. Honcharenko // Naukovo-tekhnychnyi zhurnal «Reiestratsiia, zberihannia i obrobka danykh», Tom 16. – Kyiv: Instytut problem reiestratsii informatsii NANU, 2014. - #2 – S. 52 – 61.*

УДК 504.05 : 502.55

МАТЕМАТИЧНІ ПІДХОДИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ ТЕХНОГЕННОГО ХАРАКТЕРУ

Михайло Дівізінюк, Олександр Попов, Валерія Ковач, Олег Бляшенко, Олена Алєксєєва, Кирило Сметанін

Державна установа «Інститут геохімії навколишнього середовища НАН України»

Стаття: ***6 стор., 9 джерел***

Розглянуто питання використання математичних засобів для підтримки прийняття ефективних управлінських рішень в умовах надзвичайних ситуацій техногенного характеру. Відзначено, що однією з важливих задач при управлінні під час ліквідації наслідків надзвичайних ситуацій є визначення зон можливого ураження, що дасть можливість мінімізувати ризик для здоров'я населення, яке мешкає в цих зонах, шляхом його вчасної евакуації. Це можливо здійснити лише за допомогою використання сучасних математичних моделей, що дозволяють адекватно описати масоперенесення небезпечної речовини в різних середовищах під впливом багатьох чинників. Використання таких моделей разом із сучасними картографічними пакетами дозволяє в реальному масштабі часу бачити на карті розподіл техногенного ризику в зоні ураження та приймати ефективні управлінські рішення щодо його мінімізації. Виконано детальний аналіз вражаючих факторів, що завдають шкоди людським і матеріальним ресурсам внаслідок виникнення надзвичайних ситуацій техногенного характеру. В роботі показано, що розвиток надзвичайних ситуацій техногенного характеру здійснюється в чотири етапи. На першому етапі відбувається вивільнення накопиченої в людино-машинній системі енергії або запасів шкідливої речовини внаслідок аварії, що там виникла. На другому етапі відбувається неконтрольоване поширення їх потоків в нове для них середовище і переміщення в ньому. На третьому етапі відбувається їх подальше фізико-хімічне перетворення з додатковим енерговиділенням і переходом в новий агрегатний або фазовий стан. І на четвертому етапі здійснюється руйнівний вплив первинних потоків та/або наведених ними вражаючих факторів на незахищені від них об'єкти. Представлено детальний аналіз кожного етапу. В статті відзначається, що для ефективного управління екологічною безпекою потенційно небезпечних об'єктів під час їх штатного та аварійного режимів роботи, необхідно створювати сучасні інформаційно-вимірювальні та керуючі системи екологічного моніторингу. Дані системи мають здійснювати збір та обробку інформації та її подання персоналу в зручній формі, а також керуючі функції: автоматичне керування і регулювання, блокування, дистанційне управління у всіх режимах роботи техногенного об'єкта. Розглянуто умови та процедура прийняття рішень в умовах надзвичайних ситуацій техногенного характеру. Показано, що прийняття управлінського рішення передбачає: визначення мети управління, оцінку обстановки і вихідного стану, прогнозування розвитку ситуації, визначення та оцінку послідовності дій, прийняття найбільш раціональної послідовності дій як управлінського рішення. Описано алгоритм відбору комбінацій ліквідаційних заходів в результаті надзвичайних ситуацій. Відзначено заходи, які повинен здійснювати ситуаційний центр в нормальному режимі роботи потенційно небезпечного об'єкту для запобігання виникнення на ньому надзвичайної ситуації.

МАТЕМАТИЧЕСКИЕ ПОДХОДЫ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ ТЕХНОГЕННОГО ХАРАКТЕРА

Михаил Дивизинюк, Александр Попов, Валерия Ковач, Олег Бляшенко, Елена Алексеева, Кирилл Сметанин

Государственное учереждение «Институт геохимии окружающей среды НАН Украины»

Рассмотрен вопрос использования математических средств для поддержки принятия эффективных управленческих решений в условиях чрезвычайных ситуаций техногенного характера. Отмечено, что одной из важных задач при управлении во время ликвидации последствий чрезвычайных ситуаций является определение зон возможного поражения, что позволит минимизировать риск для здоровья населения,

проживающего в этих зонах, путем его своевременной эвакуации. Это возможно осуществить только с помощью использования современных математических моделей, позволяющих адекватно описать массоперенос опасного вещества в различных средах под воздействием многих факторов. Использование таких моделей вместе с современными картографическими пакетами позволяет в реальном масштабе времени видеть на карте распределение техногенного риска в зоне поражения и принимать эффективные управленческие решения по его минимизации. Выполнен детальный анализ поражающих факторов, наносящих ущерб человеческим и материальным ресурсам в результате возникновения чрезвычайных ситуаций техногенного характера. В работе показано, что развитие чрезвычайных ситуаций техногенного характера осуществляется в четыре этапа. На первом этапе происходит высвобождение накопленной в человеко-машинной системе энергии или запасов вредного вещества в результате возникшей там аварии. На втором этапе происходит неконтролируемое распространение их потоков в новую для них среду и перемещение в ней. На третьем этапе происходит их дальнейшее физико-химическое преобразование с дополнительным энерговыделением и переходом в новое агрегатное или фазовое состояние. И на четвертом этапе осуществляется разрушительное воздействие первичных потоков и/или приведенных ими поражающих факторов на незащищенные от них объекты. Представлен подробный анализ каждого этапа. В статье отмечается, что для эффективного управления экологической безопасностью потенциально опасных объектов при их штатном и аварийном режимах работы, необходимо создавать современные информационно-измерительные и управляющие системы экологического мониторинга. Данные системы должны осуществлять сбор и обработку информации и ее представление персоналу в удобной форме, а также управляющие функции: автоматическое управление и регулирование, блокировка, дистанционное управление во всех режимах работы техногенного объекта. Рассмотрены условия и процедура принятия решений в условиях чрезвычайных ситуаций техногенного характера. Показано, что принятие управленческого решения предусматривает: определение цели управления, оценку обстановки и исходного состояния, прогнозирование развития ситуации, определение и оценку последовательности действий, принятие наиболее рациональной последовательности действий как управленческого решения. Описан алгоритм отбора комбинаций ликвидационных мероприятий в результате чрезвычайных ситуаций. Отмечены меры, которые должен осуществлять ситуационный центр в нормальном режиме работы потенциально опасного объекта для предотвращения возникновения на нем чрезвычайной ситуации.

MATHEMATICAL APPROACHES TO DECISION SUPPORT UNDER EMERGENCY SITUATION

Mikhail Diviziniuk, Oleksandr Popov, Valeriia Kovach, Oleg Bliashenko, Olena Alekseyeva, Kyrylo Smetanin

State Institution "Institute of Environmental Geochemistry NAS of Ukraine"

In the paper was considered the use of mathematical tools to support effective management decision-making under emergency situation. It is noted that one of the important tasks of the management during emergencies is to determine areas of possible defeat, which will enable to minimize the risk to the health of the population living in these areas through its timely evacuation. This can be done only through the use of advanced mathematical models that can adequately describe the mass transfer of dangerous substances in various media influenced by many factors. Using such models, along with modern mapping package allows real-time view on the map the distribution of technological risk in the affected area and make effective management decisions for its minimization. Completed a detailed analysis of the damaging factors that are detrimental to human and material resources as a result of artificial disasters. It is shown that the development of emergency situation carried out in four stages. The first step is to release the accumulated human-machine systems or energy reserves harmful substances from the accident that occurred there. In the second stage, the uncontrolled spread of flows in new environment for them and move in it. The third stage is the subsequent physical-chemical conversion of additional energy release and the transition to a new phase or state of aggregation. And on the fourth stage the devastating impact of primary flow and / or given them damaging factors on them unprotected objects. A detailed analysis of each stage. The article noted that for effective management of ecological safety of potentially dangerous objects during their regular and emergency modes, you must create modern information-measuring and management systems for environmental monitoring. These systems should collect and process information and its presentation staff in a convenient form, and control functions: automatic control and adjustment, locking, remote control in all modes of potentially dangerous objects. The conditions and procedure of decision making under emergency situation was described. It is shown that a management decision involves: defining management objectives, assess the situation and the initial state, prediction

of the situation, identify and evaluate the action sequences, making the most efficient sequence of actions as a management decision. The algorithm selecting combinations of measures resulting from liquidation of emergency situations. Noted measures must perform the Situation Centre in the normal operation of potentially dangerous facility to prevent it during the emergency.

Spysok vykorystanoi literatury: 1. Korotynskyi P. A. Klasyfikatsiia nadzvychainykh sytuatsii tekhnohennoho ta pryrodnoho kharakteru / P. A. Korotynskyi // Nadzvychaina sytuatsiia. – 2004. – # 8. – S. 8-11. 2. Shobotov V. M. Tsyvilna oborona : navchalnyi posibnyk / V. M. Shobotov. vyd. 2-he, pererob. K. : Tsentr navchalnoi literatury, 2006. 438 s. 3. Popov O. O. Prohnozuvannia avariinoho ryzyku / O. O. Popov // Tekhnohenno-ekolohichna bezpeka ta tsyvilnyi zakhyst. – K., 2013. – # 6. – S. 28-33. 4. Serheev V. S. Zashchyta naselenyia y terrytoryi v chrezvыchaynыkh sytuatsyiakh : uchebnoe posobye dlia vuzov / V. S. Serheev. – M. : Akademycheskyi Proekt, 2004. – 429 s. 5. Akymov V. A. Pryrodnыe y tekhnohennыe chrezvыchaynыe sytuatsyy: opasnosty, uhrozы, rysky / V. A. Akymov, V. D. Novykov, N. N. Radaev. – M. : ZAO FYD, 2001. – 344 s. 6. Koff H. L. Otsenka posledstvyi chrezvыchaynыkh sytuatsyi / H. L. Koff, A. A. Husev, Yu. L. Vorobev. M. : RЭFYA, 1997. 364 s. 7. Mastriukov B. S. Bezopasnost v chrezvыchaynыkh sytuatsyiakh : uchebnoe posobye dlia vuzov / B. S. Mastriukov. – M. : Akademyia, 2003. – 331 s. 8. Reahuvannia na vynyknennia nadzvychainykh sytuatsii / pid red. S. O. Hurieva / IDUSTsZ NUTsZU; UNPTs EMD ta MK. – Vinnytsia, 2010. – 412 s. 9. Serdiutska L. F. Do ohliadu modelei rozpovsiudzhennia domishok v atmosferi mista / L. F. Serdiutska, O. O. Popov // Modeliuvannia ta informatsiini tekhnolohii. – K., 2008. – Vyp. 45. – S. 67-80.

УДК 004.056:061.68; 004.3.75:061.68

ЗАГАЛЬНІ ПРОБЛЕМИ ПРОГНОЗУВАННЯ НСД В ІНФОРМАЦІЙНИХ СИСТЕМАХ ДЕРЖАВИ

Іван Опірський
Національний університет «Львівська політехніка»

*Стаття**: 4 стор., 9 джерел***

Важлива роль прогнозу в проблемі прийняття рішення за результатами контролю приводить до необхідності більш детально розглянути як саму постановку задачі прогнозу, так і можливих методів її рішення. Така необхідність, крім того, викликається такою обставиною, що прогнози різного характеру використовують відносно різні інформаційні мережі держави. Бажано визначити місце задачі, що розглядається, в загальній проблемі передбачення і прогнозу НСД і оцінити існуючі методи вирішення з точки зору їх можливості використання в даному випадку.

Однією з характерних особливостей будь-якого прогнозу, а в особливості НСД на інформаційні системи держави, є використання минулого досвіду для отримання оцінок майбутнього. Інформація про інформаційні мережі держави, що мається до моменту прогнозу і, що використовується, при його здійсненні і називається апріорною. Відповідно оцінки, отримані в результаті прогнозу називаються апостеріорними. Виходячи з цього, прогноз можна визначити як отримання апостеріорної оцінки деякої якості явища НСД, що досліджується, на основі апріорних відомостей про його минуле і теперішнє. Очевидно, що об’єм і характер апріорної інформації, яка використовується при прогнозуванні, в істотній степені складаються на методах отримання потрібної апостеріорної оцінки і степені її достовірності. Зокрема, апріорна інформація є єдиною основою для визначення моделі явища НСД, що досліджується – детермінованої або стохастичною. Проте проблема прогнозування включає в себе ряд численних труднощів, одні з яких власне зв’язані з прогнозуванням, другі характерні для всіх напрямків автоматичного контролю, треті визначають загальні можливості прогнозування і його місце серед інших видів контролю.

Досліджено та приведено деякі загальні проблеми прогнозування несанкціонованого доступу в інформаційних системах,досліджено загальні методи прогнозування та представлено етапи вирішення задачі прогнозування в автоматизованих системах контролю.

ОБЩИЕ ПРОБЛЕМЫ ПРОГНОЗИРОВАНИЯ НСД В ИНФОРМАЦИОННОЙ СИСТЕМЕ ГОСУДАРСТВА

Иван Опирский
Национальный университет «Львовская политехника»

Важная роль прогноза в проблеме принятия решения по результатам контроля приводит к необходимости более подробно рассмотреть как саму постановку задачи прогноза, так и возможных методов ее решения. Такая необходимость, кроме того, вызывается таким обстоятельством, что прогнозы различного характера используют относительно различные информационные сети государства. Желательно определить задачи, рассматриваемой в общей проблеме предсказания и прогноза НСД и оценить существующие методы решения с точки зрения их возможности использования в данном случае.

Одной из характерных особенностей любого прогноза, а в особенности НСД на информационные системы государства, является использование прошлого опыта для получения оценок будущего. Информация об информационных сети государства, имеется к моменту прогноза и, используемого при его осуществлении и называется априорной. Согласно оценки, полученные в результате прогноза называются апостериорными. Исходя из этого, прогноз можно определить как получение апостериорной оценки некоторой качества явления НСД, что исследуется на основе априорных сведений о его прошлом и настоящем. Очевидно, что объем и характер априорной информации, используемой при прогнозировании, в существенной степени состоят на методах получения нужной апостериорной оценки и степени ее достоверности. В частности, априорная информация является единственной основой для определения модели явления НСД исследуемого - детерминированной или стохастической. Однако проблема прогнозирования включает в себя ряд многочисленных трудностей, одни из которых собственно связанные с прогнозированием, вторые характерны для всех направлений автоматического контроля, третьи определяют общие возможности прогнозирования и его место среди других видов контроля.

Исследованы и приведены некоторые общие проблемы прогнозирования несанкционированного доступа в информационных системах, исследованы общие методы прогнозирования и представлены этапы решения задачи прогнозирования в автоматизированных системах контроля.

COMMON PROBLEMS PREDICTION UA IN THE INFORMATION SYSTEM OF THE STATE

Ivan Opirsky
National University "Lviv Polytechnic"

Weather important role in the issue of the decision on the results of control leads to the need to examine in more detail how the very formulation of the problem prognosis, and possible methods of solution. This need, in addition, called this the fact that forecasts of different nature using various information regarding the network state. It is advisable to determine the location of the problem under consideration in the general problem of prediction and forecast unauthorized access and evaluate existing methods of solution from the point of view of their possible use in this case.

One of the characteristics of any forecast, and in particular the unauthorized access to state information systems is the use of past experience for future assessments. Information about the network state information that refers to the moment and the forecast used when its implementation is called a priori. Accordingly estimates derived from the forecast called posterior. Therefore, the weather can be defined as getting some quality posteriori evaluation unauthorized access (UA) phenomenon under study, based on a priori information about his past and present. Obviously, the volume and nature of prior information used in forecasting, to a considerable degree on the methods consisting of obtaining the desired posteriori evaluation and degree of reliability. In particular, a priori information is the sole basis for modeling phenomena UA, investigated - deterministic or stochastic. But the problem of forecasting involves a series of numerous difficulties, some of which are actually connected to the prediction, others common to all areas of automatic control, others define the general predictability and its place among other controls.

The article explored and brought some common problems forecasting unauthorized access to information systems, studied general methods of forecasting and presents steps for solving the problem of forecasting in automated control systems.

Spysok vykorystanoi literatury: 1. Sylyn V. B., Zakovriashyn A. Y. Avtomatycheskoe prohnozyrovanye sostoianyia apparaturы upravlenyia y nabliudenyia. Moskva. Эnerhyia 1973h. – 336 s. 2. Putintsev N. D. Aparatnyi

kontrol tsyfrovykh obchysliuvalnykh mashyn. – M. Sov. radyo, 1966. – 236 s. 3. Smyrnov N. V., Dunyn-Barkovskyi Y. V. Kurs teoryy veroiatnostei y matematycheskoi statystyky – M.: Nauka, 1968. – 576 s. 4. Tykhonov V. I., Dostyzhenye hranyts markovskykh protsessov // yzv. Vuzov radyotekhnyka, t. 15, # 4, 1972. – S. 253. 5. Zghoruvskyi M .Z., Pankratova N. D., Tekhnycheskoe predvydenye -K.: Polytekhnyka, 2005. – 165 s. 6. Demydovych B. P., Maron N. A., Shuvalova D. Z. Chyslenye metody analyza –M.: Nauka, 1967. – 242 s. 7. Kliamko Э. Y. Skhemnыi y testovыi kontrol avtomatycheskykh tsyfrovыkh vыchyslytelnыkh mashyn – M.: Sov. Radyo., 1983. – 320 s. 8. Sydorov A. M. Metodы kontrolia эlektronnыkh tsyfrovыkh mashyn. – M.: Sov. Radyo., 1986. – 342 s. 9. Zghurovskyi M. Z. Osnovy systemnoho analizu/ Zghurovskyi M. Z., Pankratova N. D. – K:VNU,2007–544 s.

УДК 35.078.3+340.68

ЄВРОПЕЙСЬКІ ВИМОГИ ЩОДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Олексій Мервінський

Національний технічний університет України «Київський політехнічний інститут»

Стаття: ***7 стор., 14 джерел.***

Розглядаються нормативно-правові акти Європейського Союзу, пов'язані із захистом і обробкою персональних даних у сфері електронної комерції і спрямовані на захист основоположних прав і свобод людини і громадянина, проведено їх аналіз.

Аналіз документів показує, що персональними даними у сфері електронної комерції вважаються відомості чи сукупність відомостей про фізичну особу, яка ідетніфіцірована або може бути конкретно ідентифікованою.

Суб'єкт персональних даних у сфері електронної комерції має право знати джерела отримання даних, місцезнаходження своїх даних, мету їх обробки, місцезнаходження (перебування) володільця чи розпорядника персональних даних, отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані, а також пред'являти вмотивовану вимогу щодо заборони обробки своїх персональних даних.

Наголошується, що суб'єкт персональних даних у сфері електронної комерції має право на захист своїх даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням або несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи порочать честь, гідність та ділову репутацію фізичної особи

Аналіз вивчених документів показує, що власники, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкової втрати або знищення, від незаконної обробки, у тому числі від незаконного знищення або доступу до персональних даних.

На жаль, нормативно-правові акти Євросоюзу, які поширюються на діяльність з обробкою персональних даних, що здійснюється з використанням автоматизованих засобів, все ще залишаються мало вивченими і слабо використовуються.

ЕВРОПЕЙСКИЕ ТРЕБОВАНИЯ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В СФЕРЕ ЭЛЕКТРОННОЙ КОММЕРЦИИ

Алексей Мервинский

Национальный технический университет Украины «Киевский политехнический институт»

Рассматриваются нормативно-правовые акты Европейского Союза, связанные с защитой и обработкой персональных данных в сфере электронной коммерции и направленные на защиту основополагающих прав и свобод человека и гражданина, проведен их анализ.

Анализ документов показывает, что персональными данными в сфере электронной коммерции считаются сведения или совокупность сведений о физическом лице, которое идетнифицировано или может быть конкретно идентифицированным.

Субъект персональных данных в сфере электронной коммерции имеет право знать источники получения данных, местонахождения своих данных, цель их обработки, местонахождения (пребывания) владельца или распорядителя персональных данных, получать информацию об условиях предоставления доступа к

персональным данным, в частности информацию о третьих лицах, которым передаются его персональные данные, а также предъявлять вмотивированное требование о запрете обработки своих персональных данных.

Отмечается, что субъект персональных данных в сфере электронной коммерции имет право на защиту своих данных от незаконной обработки и случайной потери, уничтожения, повреждения в связи с умышленным сокрытием, непредоставлением или несвоевременным их предоставлением, а также на защиту от предоставления сведений, которые являются недостоверными или порочат честь, достоинство и деловую репутацию физического лица.

Анализ изученных документов показыват, что владельцы, распорядители персональных данных и третьи лица обязаны обеспечить защиту этих данных от случайной потери или уничтожения, от незаконной обработки, в том числе от незаконного уничтожения или доступу к персональным данным.

К сожалению, нормативно-правовые акты Евросоюза, которые распространяются на деятельность с обработкой персональных данных, которая осуществляется с использованием автоматизированных средств, все еще остаются мало изученными и слабо используемыми.

EUROPEAN REQUIREMENTS FOR PERSONAL DATA PROTECTION IN E-COMMERCE

Olexsiy Mervinskiy
National Technical University of Ukraine "Kyiv Polytechnic Institute"

The article reviews normative acts, regulations, constitutive or other documents European Union involving protection and processing of personal data in the field of e-commerce and aim to protect the fundamental rights and freedoms of natural persons, particularly the right to privacy in relation to the processing of personal data and includes statistical analysis.

Publications analysis shows that the p*ersonal data shall* in the field of e-commerce mean information or aggregate information about a natural person who is identified or may be identified.

The personal data subject in the field of e-commerce shall have the right to know about the location of base of personal data which contains his/her personal data, its purpose and name, location and/or place of residence (staying) of the controller or processor of such personal data, Receive the information concerning the conditions of access to personal data, in particular information about third persons who obtain his/her personal data also Submit motivated requests to a personal data controller objecting against processing his/her personal data.

It is noted that for The personal data subject in the field of e-commerce shall have the right to Protect of his/her personal data from illegal processing and accidental loss, destruction, damage due to a deliberate concealing, failure to provide them or provision of such data with delay, as well as to protection from provision of information which is inaccurate or are disgraceful for the honor, dignity and business reputation of a natural person

Publications analysis shows that the subjects of relations related to personal data shall undertake to provide protection of such data from unauthorized processing, including its loss, illegal or accidental destruction, as well as from unauthorized access.

Unfortunately, documents European Union, which shall apply to personal data processing activities performed with the use of automated means, are poorly studied and little used.

Spysok vykorystanoi literatury: 1. Zakon Ukrainy «Pro elektronnu komertsiiu». [Elektronnyi resurs]. – Rezhym dostupu: http://zakon0.rada.gov.ua/laws/show/675-19 2. Zakon Ukrainy «Pro zakhyst personalnykh danykh». http://zakon3.rada.gov.ua/laws/show/2297-17 3. Budapeshtska konventsiia pro zlochynnist v kiberprostori. [Elektronnyi resurs]. – Rezhym dostupu: http://zakon0.rada.gov.ua/laws/show/994_575 4. Rezoliutsiia Parlamentskoi Asamblei Rady Yevropy vid 2011 roku pro zakhyst osobystoho zhyttia ta personalnykh danykh v Interneti [Elektronnyi resurs]. – Rezhym dostupu: http://www.khpg.org/index.php?id=1329990005 5. Dyrektyva Yevropeiskoho Parlamentu ta Rady YeS 2000/31/YeS vid 08.06.2000 roku pro deiaki pravovi aspekty informatsiinykh posluh na vnutrishnomu rynku, zokrema pro elektronnu komertsiiu (Dyrektyva pro elektronnu komertsiiu) Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). [Elektronnyi resurs]. – Rezhym dostupu: http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri= CELEX:32000L0031:en:HTML 6. Dyrektyva 95/46/YeS Yevropeiskoho Parlamentu i Rady «Pro zakhyst fizychnykh osib pry obrobtsi personalnykh danykh i pro vilne peremishchennia takykh danykh» vid 24 zhovtnia 1995 roku, Yevropeiskyi Soiuz; Dyrektyva, Mizhnarodnyi dokument vid 24.10.1995 #95/46/YeS. [Elektronnyi resurs]. – Rezhym dostupu: http://zakon4.rada.gov.ua /laws/show/994_242 7. Vysnovok 1/2000 Robochoi hrupy iz zakhystu fizychnykh osib pry obrobtsi personalnykh danykh, stvorenoi vidpovidno do Statti 29 «Shchodo pevnykh aspektiv zakhystu

danykh v svitli elektronnoi komertsii», pryiniatyi 3-ho liutoho 2000 roku: WP 28 (5007/00/EN/final). [Elektronnyi resurs]. – Rezhym dostupu: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000 /wp28_en.pdf 8. Dyrektyva #2002/58/ES Evropeiskoho Parlamenta y Soveta ES v otnoshenyy obrabotky personalnыkh dannыkh y zashchyty konfydentsyalnosty v sektore эlektronnыkh sredstv sviazy (Dyrektyva o konfydentsyalnosty y эlektronnыkh sredstvakh sviazy), Dyrektyva, Mizhnarodnyi dokument vid 12.07.2002 #200/58/YeS. [Elektronnyi resurs]. – Rezhym dostupu:http://zakon4.rada.gov.ua/laws/show/994_243 9. Vysnovok 3/99 shchodo Informatsii publichnoho sektoru ta zakhystu personalnykh danykh, pryiniatyi 3 travnia 1999 roku: WP 20 (5055/99). [Elektronnyi resurs]. – Rezhym dostupu: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2000/wp28_en.pdf 10. Rekomendatsiia 1/99 stosovno nevydymoi ta avtomatyzovanoi obrobky personalnykh danykh v Interneti za dopomohoiu prohramnykh i aparatnykh zasobiv, ukhvalena 23 liutoho 1999 roku: WP 17 (5093/98). [Elektronnyi resurs]. – Rezhym dostupu: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/ 1999/wp17 _en.pdf 11. Rekomendatsiia 3/99 stosovno zberezhennia Internet-provaideramy informatsii pro trafik z metoiu zabezpechennia pravoporiadku, ukhvalena 7 veresnia 1999 roku: WP 25 (5085/99). [Elektronnyi resurs]. – Rezhym dostupu:http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files /1999 /wp25_en.pdf 12. Robochyi dokument Robochoi hrupy iz zakhystu fizychnykh osib pry obrobtsi personalnykh danykh, stvorenoi vidpovidno do Statti 29: Obrobka personalnykh danykh v merezhi Internet. Pryiniatyi 3 liutoho 1999 roku, WP 16 (5013/99). [Elektronnyi resurs]. – Rezhym dostupu: http://ec.europa.eu/justice/policies /privacy/docs/wpdocs/1999/wp16en.pdf 13. Dyrektyva 97/7/YeS Yevropeiskoho Parlamentu ta Rady «Pro zakhyst prav spozhyvachiv v dystantsiinykh kontaktakh» vid 20 travnia 1997 roku. [Elektronnyi resurs]. – Rezhym dostupu:http://zakon1.rada.gov.ua/laws/show/994_245 14. Dyrektyva #2002/65/ES Evropeiskoho Parlamenta y Soveta o dystantsyonnom marketynhe potrebytelskykh fynansovыkh usluh y o vnesenyy yzmenenyi v Dyrektyvu Soveta #90/619/EЭS y Dyrektyvы # 97/7/ES y 98/27/ES ot 23 sentiabria 2002 hoda. [Elektronnyi resurs]. – Rezhym dostupu:http://zakon1.rada.gov.ua/laws/show/994_b31

УДК 004.056

ПРОБЛЕМАТИКА ВИЗНАЧЕННЯ ІНВЕСТИЦІЇ В ІНФОРМАЦІЙНУ БЕЗПЕКУ НА ОСНОВІ ЕКОНОМІКО-ВАРТІСНИХ МОДЕЛЕЙ

Олександр Архипов, Андрій Скиба
Національний технічний університет України "Київський Політехнічний Інститут"

Стаття: 6 ***стор, 11 джерел.***

Для вибору моделі визначення оптимальних інвестицій в інформаційну безпеку компанії автори приводять аналіз двох економіко-вартісних моделей. Не зважаючи на абсолютно різні підходи, на яких базуються ці моделі, вони дають доволі близькі результати, але мають ключові відмінності. Автори проводять порівняльний аналіз популярної для визначення інвестицій в інформаційну безпеку моделі американських дослідників Гордона і Лоеба, а також економіко-вартісну модель, яка набула широкого застосування для визначення комплексної оцінки загального стану захищеності інформаційної безпеки компанії. Результат аналізу двох моделей на однаковій вибірці даних прозоро показує, як на практиці застосовується американська модель з формальним характером та явно вираженим наголосом на економіці та економіко-вартісна модель, яка ґрунтується на результатах аналізу реальних показників рівня захищеності інформаційної системи організації, потреб інформаційної безпеки, що вимагають використання реальних механізмів управління інформаційними ризиками, з урахування економічних тенденцій. Використовуючи обидві моделі можна отримати об'єктивні результати; але слід зауважити, що, як показує практичне застосування моделей, досягнення більш об'єктивних результатів при проведенні оцінки оптимального обсягу інвестицій в систему захисту інформації дають ті моделі, в яких максимально враховані показники рівня захищеності, що впливають на стан безпеки підприємства.

ПРОБЛЕМАТИКА ОПРЕДЕЛЕНИЯ ИНВЕСТИЦИЙ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ НА ОСНОВЕ ЭКОНОМИКО-СТОИМОСТНЫХ МОДЕЛЕЙ

Александр Архипов, Андрей Скиба
Национальный технический университет Украины "Киевский Политехнический Институт"

Для выбора модели определения оптимальных инвестиций в информационную безопасность компании авторы приводят анализ двух экономико-стоимостных моделей. Несмотря на совершенно разные подходы, на которых базируются эти модели, они обе дают довольно близкие результаты, но имеют ключевые отличия. Авторы проводят сравнительный анализ популярной для определения инвестиций в информационную безопасность модели американских исследователей Гордона и Лоэба, а также экономико-стоимостную модель, которая получила широкое применение для определения комплексной оценки общего состояния защищенности информационной безопасности компании. Результат анализа двух моделей на одинаковой выборке данных прозрачно показывает, как на практике применяется американская модель с формальным характером и явно выраженным акцентом на экономике и экономико-стоимостная модель, которая основывается на результатах анализа реальных показателей уровня защищенности информационной системы организации, потребностей информационной безопасности, требующих использования реальных механизмов управления информационными рисками, с учетом экономических тенденций. Используя обе модели можно получить объективные результаты; но следует заметить, что, как показывает практическое применение моделей, достижения более объективных результатов при проведении оценки оптимального объема инвестиций в систему защиты информации дают те модели, в которых максимально учтены показатели уровня защищенности, влияющие на состояние безопасности предприятия.

THE ISSUE OF DEFINITION OF INVESTMENT IN INFORMATION SECURITY THROUGH ECONOMIC AND COST MODELS

Oleksandr Arkhypov, Andrii Skyba
National Technical University of Ukraine "Kyiv Polytechnic Institute"

Authors analyze two economic-cost models for determine optimal investment in information security of the company. Despite the very different approaches, which these models are based on, they both give quite similar results, but with key differences. The analysis of two models on the same sample data transparently shows how in practice the american model with formal and explicit focus on the economy and economic-cost model, which is based on an analysis of actual indicators of information security system, information security needs that require the usage of information risk management mechanisms with taking into account economic trends, are used. Objective results are achieved using both models in research, but it should be noted that as the practical usage of models to achieve a more objective results of the evaluation of optimal investments in information security is preferred the model, which takes into account most indicators which affects information security.

Spysok vykorystanoi literatury: 1. Lukackij, A. V. Percentage of security - available at: http://www.it-world.ru/safety/58323.html. 2. Gordon L. A. and Loeb M. P. The Economics of Information Security Investment // ACM Transaction on Information and System Security - 2002 - Vol. 5, #.4. - pp. 438-457. 3. Arkhypov O. Ye., Skyba A. V. Informatsiini ryzyky: metody ta sposoby doslidzhennia, modeli ryzykiv i metody yikh identyfikatsii // Zakhyst informatsii. – 2013. – Tom15, #4. – S.366 – 375. 4. Arkhypov A. E., Arkhypova S. A., Skyba A. V. Prymenenye zatratno-stoymostnыkh modelei dlia otsenyvanyia veroiatnostnыkh parametrov ynformatsyonnыkh ryskov // Informatsiina bezpeka. – 2013. – #2(10). – C. 11-18. 5. Skyba A. V., Khorina O. I. Prohnozuvannia sotsialno-psykholohichnykh ta sytuatsiinykh chynnykiv aktyvatsii zlochynnykh dumok i namiriv u sferi informatsiinoi bezpeky // Bezpeka informatsii – 2015 - #21(2) – S. 165-173. 6. Arkhypov O. Ye., Skyba A. V., Khorina O. I. Rozshyrennia ekonomiko-vartisnykh modelei informatsiinykh ryzykiv za rakhunok vykorystannia sotsialno-psykholohichnykh typiv zlovmysnyka. // Zakhyst informatsii – 2015 - # 1(17) - C. 60-72. 7. Skyba A. V., Khorina O. I. Prohnozuvannia sotsialno-psykholohichnykh ta sytuatsiinykh chynnykiv aktyvatsii zlochynnykh dumok i namiriv u sferi informatsiinoi bezpeky.// Bezpeka informatsii – 2015 - #21(2), S. 165-173. 8. Gordon L., Loeb M., Lucyshyn W., Zhou L. Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. // Journal of Information Security – 2015 - #6 – pp. 24-30. 9. Willemson J. On the Gordon &

Loeb Model for Information Security Investment // Proceedings of The Fifth Workshop on the Economics of Information Security (WEIS 2006), 2006. pp.101-112 10. Willemson J. Extending the Gordon&Loeb Model for Information Security Investment // Fifth International Conference on Availability, Reliability, and Security (ARES 2010), 2010. pp 258-261. 11. Arkhypov A. E. Prymenenye эkonomyko-motyvatsyonnыkh sootnoshenyi dlia otsenyvanyia veroiatnostnыkh parametrov ynformatsyonnыkh ryskov // Zakhyst informatsii – 2011. – #2 (51) – S. 69-76.

УДК 004.056.5

ПІДХОДИ ДО ОЦІНКИ НЕБЕЗПЕКИ АТАК В ІНФОРМАЦІЙНИХ СИСТЕМАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Сергій Гончар, Геннадій Леоненко, Олексій Юдін
ДержНДІ Спецзв'язку

Стаття: ***6 стор, 7 джерел.***

На сьогодні практично всі держави світу залежать від автоматизації виробничих процесів, а саме: від безперебійної роботи автоматизованих систем управління технологічними процесами (АСУ ТП). Найбільш значущими АСУ ТП є ті, що забезпечують роботу об'єктів критичної інфраструктури (ОКІ). Під ОКІ будемо розуміти атомні і гідроелектростанції, нафто - і газопроводи, національні мережі розподілу електроенергії, транспортні системи національного і світового рівня, загальнодержавні системи зв'язку, галузеутворюючі підприємства і таке інше. Викладене робить актуальною задачу оцінки небезпеки атак на ОКІ

В статті запропонована до розгляду класифікація загроз за категоріями і видами, а також визначені підходи до оцінки коефіцієнту небезпеки загроз в інформаційних системах ОКІ.

За вихідні дані для оцінки коефіцієнту прийняті загрози безпеці інформації, можливі атаки, взаємозв'язок між можливими атаками та загрозами, взаємозв'язок між можливими атаками і наслідками від їх реалізації.

ПОДХОДЫ К ОЦЕНКЕ ОПАСНОСТИ АТАК В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ

Сергей Гончар, Геннадий Леоненко, Алексей Юдин
ГосНИИ Спецсвязи

Сегодня практически все государства мира зависят от автоматизации производственных процессов, а именно: от бесперебойной работы автоматизированных систем управления технологическими процессами (АСУ ТП). Наиболее значимыми АСУ ТП являются те, которые обеспечивают работу объектов критической инфраструктуры (ОКИ). Под ОКИ понимаются атомные и гидроэлектростанции, нефте – и газопроводы, национальные сети распределения электроэнергии, транспортные системы национального и мирового уровня, общегосударственные системы связи, отраслеобразующие предприятия и тому подобное. Изложенное делает актуальной задачу оценки опасности атак на ОКИ.

В статье предложена к рассмотрению классификация угроз по категориям и видам, а также определены подходы к оценке коэффициента опасности угроз в информационных системах ОКИ.

За исходные данные для оценки коэффициента взяты угрозы безопасности информации, возможные атаки, взаимосвязь между возможными атаками и угрозами, взаимосвязь между возможными атаками и последствиями от их реализации.

APPROACHES TO ASSESSING THE RISK OF ATTACKS ON INFORMATION SYSTEMS OF CRITICAL INFRASTRUCTURE OBJECTS

Sergii Gonchar, Gennadii Leonenko, Oleksii Yudin
SRI for STIP

Today almost all states of the world depend on computer-aided manufacturing, but exactly from uninterruptable work of industrial control systems (ICS). The most significant ICS are there, which providing work of critical infrastructure objects (CIO). CIO means nuclear power plants and hydroelectric power plants, oil pipeline and gasmains, national energy management networks, transport systems national's and world's level, nationwide systems of communication, branchgenerating enterprises etc. The foregoing makes it urgent task of assessing the risk of attacks on the CIO.

The paper proposes to review the classification of threat categories and types, and the approach to the assessment of the hazard ratio threats in the information systems of the CIO.

Initial data for the evaluation factor is the threat of information security, possible attacks, the relationship between the possible attacks and threats, the relationship between a possible attack and the consequences of their implementation.

Spysok vykorystanoi literatury: 1. Metodolohichni zasady rozrobky ta vprovadzhennia system zakhystu informatsii na obiektakh krytychnoi infrastruktury / Honchar S. F., Leonenko H. P., Yudin O. Yu. // Spetsialni telekomunikatsiini systemy ta zakhyst informatsii. – 2014. Vypusk 1 (25). 2. Osobennosty obespechenyia kyberbezopasnosty yndustryalnыkh system upravlenyia / Honchar S. F. // Tezy dopovidei mizhnarodnoi naukovo-praktychnoi konferentsii "Problemy ta perspektyvy rozvytku enerhetyky, elektrotekhnolohii ta avtomatyky v APK", Kyiv, – 2013. – S. 36-37. 3. Mokhor V. V. Nastavlenyia po kyberbezopasnosty (ISO/IEC 27032:2012) / V. V. Mokhor, A. M Bohdanov, A. S. Kylevoi – K.: OOO «TryK», 2013. – 129 s. 4. Hrytsai H., Tymoryn A., Holtsev Yu., Ylyn R. Bezopasnost promыshlennыkh system v tsyfrakh. – M.: Positive Technologies, 2012. 5. Teoretyko-metodolohichnyi aspekt zabezpechennia informatsiinoi bezpeky obiektiv krytychnoi infrastruktury / Honchar S. F., Leonenko H. P., Yudin O. Yu. // Visnyk Natsionalnoho universytetu "Lvivska politekhnika": "Kompiuterni systemy ta merezhi". #806. – 2014. – 34 s. 6. Industrial communication networks – Network and system security: IEC 62443-1-1. – Part 1-1: Terminology, concepts and models. 7. Power systems management and associated information exchange – Data and communications security: IEC 62351-1. – Part 1: Communication network and system security – Introduction to security issues.

УДК 004.056.53(045)

СУЧАСНІ МЕТОДИ ГОМОМОРФНОГО ШИФРУВАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Анна Ільєнко
Національний авіаційний університет

Стаття: ***6 стор., 9 джерел.***

Проведено порівняльний аналіз гомоморфних методів шифрування інформаційних ресурсів на основі забезпечення цілісності та конфіденційності в сучасних інформаційно-комунікаційних системах та мережах. В роботі описані сучасні гомоморфні системи шифрування, а саме частково гомоморфні системи та повністю гомоморфні. Розглянуто криптосистеми RSA, Ель-Гамаля, Пейє та Гентрі.

В результаті визначено особливості застосування гомоморфних криптосистем та алгоритмів при забезпеченні цілісності та конфіденційності інформаційних ресурсів, їх класифікація, властивості та складена порівняльна таблиця оцінки ефективності використання даних алгоритмів. Для кожного з алгоритмів визначені недоліки, переваги, сфера застосування, можливість практичної реалізації. Визначені подальші шляхи удосконалення алгоритму повного гомоморфного шифрування, а також перспективи його використання при здійсненні хмарних обчислень.

СОВРЕМЕННЫЕ МЕТОДЫ ГОМОМОРФНОГО ШИФРОВАНИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Анна Ильенко
Национальный авиационный університет

Проведен сравнительный анализ гомоморфного методов шифрования информационных ресурсов га основе обеспечения целостности и конфиденциальности в современных информационно-комуникцаийних системах и сетях. В работе описаны современные гомоморфные системы шифрования, а именно частично гомоморфные системы и полностью гомоморфные. Рассмотрены криптосистеми RSA, Эль-Гамаля, Пейе и Гентри.

В результате определены особенности применения гомоморфных криптосистем и алгоритмов при обеспечении целостности и конфиденциальности информационных ресурсов, их классификация, свойства и составлена сравнительная таблица оценки эффективности использования данных алгоритмов. Для каждого из алгоритмов определенные недостатки, преимущества, область применения, возможность практической реализации. Определены дальнейшие пути совершенствования алгоритма полного гомоморфного шифрования, а также перспективы его использования при осуществлении облачных вичислений.

MODERN METHOD OF HOMOMORPHIC ENCRYPTION OF INFORMATION RESOURCES

Anna Ilienko
National Aviation University

In the article the comparative analysis of homomorphic encryption methods of information resources by ensuring the integrity and confidentiality of modern information systems and networks. The paper describes modern homomorphic encryption, namely partially homomorphic systems and fully homomorphic encryption. Considered cryptosystem RSA, El-Gamal, Peyia and Gentry.

As a result defined characteristics of the homomorphic cryptosystems and algorithms ensuring the integrity and confidentiality of information resources, their classification, properties and compiled a comparative table assessing the effectiveness of the use of these algorithms. For each of the algorithms are certain disadvantages, advantages, applications, possibility of practical realization. The further ways to improve the algorithm for full homomorphic encryption, as well as prospects for its use in the cloud computing.

Spysok vykorystanoi literatury: 1. Chunarova A. V. Analiz suchasnykh alhorytmiv homomorfnoho shyfruvannia / A. V. Chunarova, D. M. Mykolyshyn // Naukpwa przestrzen europy – 2014: X miedzynarodowej naukowi-praktycznej konferencji, 07-15 kwietnia 2014 r.: abstracts. – Przemysl (Polska), 2014. – V.33. – P. 98-101. 2. Ilienko A. V. Zabezpechennia konfidentsiinosti informatsiinykh resursiv na osnovi metodiv homomorfnoho shyfruvannia / A. V. Ilienko, R. V. Ziubina // Avia-2015: XII mizhnarodna naukovo-tekhnichna konferentsii, 28-29 kvitnia 2015 r.: tezy dop. – K., 2015. – S. 5.25-5.29. 3. «Osnovы kryptohrafyy» / [Alferov A. P., Zubov A. Iu., Kuzmyn A. S., Cheremushkyn A. V.]. – Moskva: Helyos – ARV, 2002. – 471 s. 4. N. P. Varnovskyi. Homomorfnoe shyfrovanye. [Elektronnyi resurs] / Varnovskyi N. P. , Shokurov A. V // RFFY. – 2011. – №6. – S. 27 – 36. 5. C. Gentry , S. Halevi. Implementing gentry's fully-homomorphic encryption scheme // Gentry C., Halevi S./ Springer . – 2011. – C. 129–148. 6. Hrytsyk V. V. RSA ta yoho optymizatsiia / V.V Hrytsyk, N.I. Pelykh, D.A. Yanush // Naukovi pratsi. – 2009. – T.106. – S. 81 – 86. 7. Yvanov M. A. Kryptohrafycheskye metodы zashchytы ynformatsyy v kompiuternыkh systemakh y setiakh / M. A. Yvanov. –Moskva: Kudyts – Obraz, 2007. – 368 s. 8. Akbarov D. E. Kryptohrafyia, standartы alhorytmov kryptohrafycheskoi zashchytы ynformatsyy y ykh prylozhenyia. – Tashkent, 2007. – 188 s. 9. Shnaier B. Prykladnaia kryptohrafyia. Protokolы, alhorytmы, yskhodnыe teksty na yazыke Sy. – Moskva: TRYUMF, 2002. – 816 s.

УДК 681.06

ОСОБЛИВОСТІ ВИНИКНЕННЯ КАНАЛУ ВИТОКУ ІНФОРМАЦІЇ ЗА РАХУНОК ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ І НАВЕДЕННЯ

Юрій Хлапонін
Національний авіаційний університет

Стаття: *6* ***стор, 9 джерел.***

Одним з можливих каналів витоку інформації є випромінювання елементів комп'ютера, точніше, елементів основних технічних засобів (ОТЗ), якщо говорити про захищені автоматизовані системи (АС). Цей канал витоку інформації називається ПЕМВН (побічного електромагнітного випромінювання і наведення). Для стандартного комп'ютерного монітора перехоплення інформації можливе на частотах до 50 гармоніки тактової частоти. Характер ПЕМВН визначається призначенням, схемними рішеннями, елементної базою, потужністю пристрою, а також матеріалами, з яких виготовлений корпус, і його конструкцією. Випромінювання може відбуватися в широкому діапазоні частот (від одиниць Гц до ГГц), а дальність реального перехоплення інформації досягати сотень метрів. Показано, що інформативність сигналів ПЕМВН суттєва на частотах одиниць Ггц. Тому постає питання необхідності спеціальних досліджень на частотах кількох Ггц, хоча методика цього не вимагає.

Одночасно з питанням прихованої передачі даних каналом побічних електромагнітних випромінювань за допомогою програмних засобів (Soft Tempest) засобами розвідки може бути перехоплений світловий потік екрану монітора, який відбивається від стін. Сучасна техніка дозволяє відновити зображення на моніторі, прийняте після багаторазових відбиттів його від стін і всіх предметів.

Показано, що всупереч поширеній думці заземлення не відіграє визначної ролі щодо захисту інформації від витоку каналом ПЕМВН. Заземлення необхідно тільки за вимогами техніки електробезпеки. В деяких випадках при підключенні заземлення рівень побічних випромінювань може і збільшитися. Тому, чим якісніше виконано екранування корпусу (включаючи і якість фільтрів в колах електроживлення), тим менше позначається на рівні побічних випромінювань наявність або відсутність заземлення.

Показано, що в більшості практичних випадків кабельна система – це відмінна антена для всіх побічних випромінювань обладнання, підключеного до мережі. Побічні випромінювання, що виникають в елементах комп'ютера, наводяться на всі проводи кабелю локальної мережі.

Показана небезпека формування каналу витоку мовної інформації складовими комп'ютера, що обробляє інформацію, та волоконно-оптичними лініями зв’язку.

ОСОБЕННОСТИ ВОЗНИКНОВЕНИЯ КАНАЛА УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ И НАВЕДЕНИЯ

Юрий Хлапонин
Национальный авиационный университет

Одним из возможных каналов утечки информации является излучение элементов компьютера, точнее, элементов основных технических средств (ОТС), если говорить о защищеных автоматизированных системах (АС). Этот канал утечки информации называется ПЭМИН (побочного электромагнитного излучения и наводения). Для стандартного компьютерного монитора перехват информации возможен на частотах до 50 гармоники тактовой частоты. Характер ПЕМВН определяется назначением, схемными решениями, элементной базой, мощностью устройства, а также материалами, из которых изготовлен корпус, и его конструкцией. Излучение может происходить в широком диапазоне частот (от единиц Гц до ГГц), а дальность реального перехвата информации достигать сотен метров. Показано, что информативность сигналов ПЭМИН существенная на частотах единиц ГГц. Поэтому возникает вопрос о необходимости специальных исследований на частотах нескольких ГГц, хотя методика этого не требует.

Одновременно с вопросом скрытой передачи данных по каналу побочных электромагнитных излучений с помощью программных средств (Soft Tempest) средствами разведки может быть перехвачен световой поток

экрана монитора, который отражается от стен. Современная техника позволяет восстановить изображение на мониторе, принятое после многократных отражений его от стен и всех предметов.

Показано, что вопреки распространенному мнению заземление не играет определяющей роли в защите информации от утечки каналом ПЭМИН. Заземление необходимо только по требованиям электробезопасности. В некоторых случаях при подключении заземления уровень побочных излучений может и увеличиться. Поэтому, чем качественнее выполнено экранирование корпуса (включая и качество фильтров в цепях электропитания), тем меньше сказывается на уровне побочных излучений наличие или отсутствие заземления.

Показано, что в большинстве практических случаев кабельная система – это отличная антенна для всех побочных излучений оборудования, подключенного к сети. Побочные излучения, возникающие в элементах компьютера, приводятся на все провода кабеля локальной сети.

Показана опасность формирования канала утечки речевой информации компонентами компьютера и волоконно-оптическими линиями связи в процессе обработки и передачи информации.

FEATURES OF CHANNEL INFORMATION LEAKAGE DUE TO ADVERSE ELECTROMAGNETIC RADIATION AND GUIDANCE

Yuriy Hlaponin
National Aviation University

One of the possible channels of information leakage is a computer radiation elements, more precisely, the main elements of technical means, in terms of secure automated systems (AS). This channel of information leakage is called TEMPEST (spurious electromagnetic radiation and direction). For a standard computer monitor interception is possible at frequencies up to 50 harmonics of the clock frequency. Character TEMPEST is determined with purpose, schematics, element base, device power, and materials of the shell and its design. Emission can occur over a wide range of frequencies (from several Hz to GHz) and the range of real interception reach hundreds of meters. It is shown that the information content of signals is significant at frequencies GHz TEMPEST units, and there is the need for special studies at frequencies of several GHz, although the method does not require it.

Along with the issue of secure communication channel by electromagnetic radiation by means of software (Soft Tempest) reconnaissance can be intercepted by the light output of the monitor screen, which is reflected from the walls. Modern technology makes it possible to restore the image on the monitor, taken after his multiple reflections from the walls and all objects.

It is shown that, contrary to popular belief grounding does not play a determining role in the protection of information from leakage channel TEMPEST. Grounding is only necessary for the requirements of electrical safety. In some cases, when you connect the ground level of spurious emissions may increase. Therefore, the better the screening carried out of the body (including the quality of filters in power supply), the lower the impact on the level of spurious presence or absence of grounding.

It is shown that, in most practical cases, the cable system is a great dish for all spurious equipment connected to the network. Spurious emissions arising in the components of the computer are directed on all the wires of the cable network.

It shows the danger of leakage passage forming speech information computer components, and fiber optic lines in the processing and transmission of information.

Spysok vykorystanoi literatury: 1. Markus G. Kuhn, Ross J. Anderson. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations / University of Cambridge, Computer Laboratory, New Museums Site, Pembroke Street, Cambridge CB2 3QG, United Kingdom, fmgk25,rja14g@cl.cam.ac.uk. 2. Lenkov S.V., Perehudov D.A., Khoroshko V.A. Metodы y sredstva zashchytы ynformatsyy / Pod red. V.A. Khoroshko. – K.: Aryi, 2010. – Tom I. Nesanktsyonyrovannoe poluchenye ynformatsyy. – 464 s. 3. Piatachkov A.H. Zashchyta ynformatsyy, obrabatыvaemoi vыchyslytelnoi tekhnykoi, ot utechky po tekhnycheskym kanalam /A.H. Piatachkov. M.: NP RTsYB «Fakel», 2007. 4. http://www.epos.ua/view.php/ aboutpubs _archive? Subaction =showfull&id=1037743200&archive=&start_from=&ucat=2&. 5. Markus G. Kuhn. Optical Time-Domain Eavesdropping Risks of CRT Displays/ University of Cambridge, Computer Laboratory, JJ Thomson Avenue, Cambridge CB3 0FD, UK, mgk25@cl.cam.ac.uk 6. Analyz zashchytы kompiutera ot utechky po tsepiam pytanyia y zazemlenyia. Stechenko V. N., Naidenko V. I., Prokofev M. Y., Kurashkevych A. /Pravove, normatyvne ta metrolohichne zabezpechennia systemy zakhystu informatsii v ukraini, vyp. 1(14), 2007 r. 165. 7. HOST R 50571.22-2000 Эlektroustanovky zdanyi. Trebovanyia k spetsyalnыm эlektroustanovkam. Zazemlenye oborudovanyia

obrabotky ynformatsyy. 8. Aizenberh H. Z. y dr. Korotkovolnovыe antennы. M.: Radyo y sviaz, 1985. 9. Hryshachev V. V., Khaliapyn D. B., Shevchenko N. A. Opasnosty voznyknovenyia kanalov utechky konfydentsyalnoi rechevoi ynformatsyy po volokonno-optycheskym strukturyrovannыm kabelnыm systemam // Materyalы X Mezhdunarodnoi nauchno-praktycheskoi konferentsyy „Ynformatsyonnaia bezopasnost". Ch. 2. – Tahanroh: Yzd-vo TTY YuFU, 2008. –103 – 105 s.

УДК 004.93

ПОБУДОВА ГОЛОСОВОЇ СИСТЕМИ АУТЕНТИФІКАЦІЇ ДИСПЕТЧЕРІВ З ПІДВИЩЕНОЮ ШВИДКОДІЄЮ І ДОСТОВІРНІСТЮ РОБОТИ

Володимир Темніков, Ігор Конфорович, Олена Темнікова*

Національний авіаційний університет,

*Національний технічний університет України «Київський політехнічний інститут»**

Стаття: ***5 стор, 6 джерел.***

У даній статті представлені концепція побудови і структура розробленої авторами автоматичної голосової системи перманентної аутентифікації диспетчерів під час виконання ними своїх професійних обов'язків, завданням якої є запобігання доступу несанкціонованих осіб до інформаційних ресурсів, використовуваних диспетчерами в процесі роботи.

Розроблена система аутентифікації диспетчерів (САД) побудована на основі таких принципів:

- аутентифікація проводиться по виділених з безперервної мови диспетчера, так званим, ключовим мовним фрагментам, які формуються на основі слів і словосполучень, часто вживаних диспетчерами в процесі роботи, а для авіадиспетчерів - входять до складу нормативно встановленої фразеології;
- система побудована на основі теорії розпізнавання образів із застосуванням методу короткочасного аналізу і розробленої системи інформативних параметрів мовних сигналів;
- для здійснення пошуку і виділення з безперервної мови диспетчера ключових мовних фрагментів до складу САД введені модуль сегментації безперервної мови на мовні фрагменти і підсистема їх розпізнавання, що складається з модулів параметризації, класифікації та прийняття рішення про віднесення мовних фрагментів до класу «ключових».

Концепція розроблена з урахуванням особливостей практичного застосування системи: невеликі відстані від джерел звуку до САД, відносно малі значення шумів в аналізованих мовних сигналах, малі кількості контрольованих осіб, наявність специфічних вимог до диспетчерів.

Метою досліджень, проведених у процесі розробки системи, було одержання можливо більшої достовірності її роботи при забезпеченні функціонування системи в режимі реального часу. Підвищення достовірності роботи і швидкодії розробленої САД було досягнуто шляхом побудови модулів класифікації основних підсистем САД (розпізнавання мовних фрагментів і власне аутентифікації) на основі штучних нейронних мереж (ШНМ) з декількома виходами, навчених на розпізнавання відповідно мовних фрагментів і контрольованих осіб (диспетчерів), а також обґрунтованого вибору параметрів ШНМ (значення параметрів були визначені в процесі тестування).

Експериментальні дослідження показали, що застосування наведених у статті способів підвищення достовірності роботи і швидкодії САД дозволило забезпечити роботу системи в режимі реального часу і отримати процент правильної аутентифікації диспетчерів на рівні понад 98%.

Розробка системи аутентифікації є важливим етапом на шляху створення комплексної автоматичної системи контролю доступу диспетчерів до інформаційних ресурсів, що забезпечує проведення аутентифікації контрольованих осіб, їх ідентифікації у випадку непроходження процедури аутентифікації і контролю (моніторингу) психофізіологічного (емоційного) стану.

Застосування розробленої системи аутентифікації дозволяє істотно підвищити безпеку на транспорті і в енергетиці, різко зменшити кількість аварій та аварійних ситуацій внаслідок зниження впливу людського фактора.

ПОСТРОЕНИЕ ГОЛОСОВОЙ СИСТЕМЫ АУТЕНТИФИКАЦИИ ДИСПЕТЧЕРОВ С ПОВЫШЕННЫМИ БЫСТРОДЕЙСТВИЕМ И ДОСТОВЕРНОСТЬЮ РАБОТЫ

Владимир Темников, Игорь Конфорович, Елена Темникова*

Национальный авиационный университет,

*Национальный технический университет Украины «Киевский политехнический институт»**

В настоящей статье представлены концепция построения и структура разработанной авторами автоматической голосовой системы перманентной аутентификации диспетчеров во время выполнения ими своих профессиональных обязанностей, задачей которой является предотвращение доступа несанкционированных лиц к информационным ресурсам, используемым диспетчерами в процессе работы.

Разработанная система актентификации диспетчеров (САД) построена на основе следующих принципов:

- аутентификация проводится по выделенным из непрерывной речи диспетчера, так называемым, ключевым речевым фрагментам, которые формируются на основе слов и словосочетаний, часто употребляемых диспетчерами в процессе работы, а для авиадиспетчеров – входящих в состав нормативно установленной фразеологии;
- система построена на основе теории распознавания образов с применением метода кратковременного анализа и разработанной системы информативных параметров речевых сигналов;
- для осуществления поиска и выделения из непрерывной речи диспетчера ключевых речевых фрагментов в состав САД введены модуль сегментации непрерывной речи на речевые фрагменты и подсистема их распознавания, состоящая из модулей параметризации, классификации и принятия решения об отнесении речевых фрагментов к классу «ключевых».

Концепция разработана с учетом особенностей практического применения системы: небольшие расстояния от источников звука до САД, относительно малые значения шумов в анализируемых речевых сигналах, малые количества контролируемых лиц, наличие специфических требований к диспетчерам.

Целью исследований, проведенных в процессе разработки системы, являлось получение возможно большей достоверности ее работы при обеспечении функционирования системы в режиме реального времени. Повышение достоверности работы и быстродействия разработанной САД было достигнуто путем построения модулей классификации основных подсистем САД (распознавания речевых фрагментов и собственно аутентификации) на основе искусственных нейронных сетей (ИНС) с несколькими выходами, обученных на распознавание соответственно речевых фрагментов и контролируемых лиц (диспетчеров), а также обоснованного выбора параметров ИНС (значения параметров были определены в процессе тестирования).

Экспериментальные исследования показали, что применение приведенных в статье способов повышения достоверности работы и быстродействия САД позволило обеспечить работу системы в режиме реального времени и получить процент правильной аутентификации диспетчеров на уровне более 98%.

Разработка системы аутентификации является важным этапом на пути создания комплексной автоматической системы контроля доступа диспетчеров к информационным ресурсам, обеспечивающей проведение аутентификации контролируемых лиц, их идентификации в случае непрохождения процедуры аутентификации и контроля (мониторинга) психофизиологического (эмоционального) состояния.

Применение разработанной системы аутентификации позволяет существенно повысить безопасность на транспорте и в энергетике, резко уменьшить количество аварий и аварийных ситуаций вследствие снижения влияния человеческого фактора.

BUILDING A TRAFFIC CONTROLLERS VOICE AUTHENTICATION SYSTEM WITH IMPROVE SPEED AND RELIABILITY OF OPERATION

Volodymyr Temnikov, Igor Konforovich, Olena Temnikova*
National Aviation University,
*National Technical University of Ukraine "Kyiv Polytechnic Institute"**

This article presents the concept of construction and structure of the authors' permanent authentication automated voice system of traffic controllers during the fulfillment of their professional duties, which task is to prevent access by unauthorized persons to information resources used by traffic controllers in the operation.

The developed traffic controllers authentication system (TCAS) is based on the following principles:

- authentication is carried by key speech fragments extracted from uninterrupted traffic controllers speech, which are formed on the basis of words and phrases commonly used by traffic controllers in the operation;
- the system is based on the theory of pattern recognition using the method of short-term analysis and developed system of informative parameters of speech signals;
- for the fulfillment of the search and extracted from a uninterrupted traffic controllers speech key speech fragments into the TCAS introduced segmentation module of continuous speech in the speech fragments and their recognition subsystem, consisting with modules of parameterization, classification and for the classification of speech fragments classified as "key".

The concept was developed taking into account the peculiarities of the practical application of the system: a short distance from the sound source to the TCAS, the relatively small values of noise in the analyzed speech signals, small amounts of controlled entities, the presence of specific requirements for traffic controllers.

The aim of research carried out in the process of developing the system was to obtain the greatest possible reliability of its operation while ensuring the functioning of the system in real time. Increasing of the reliability and speed of TCAS was achieved by constructing a classification modules of main subsystems of TCAS (speech fragments recognition and actual authentication) based on artificial neural networks (ANN) with multiple outputs, trained to recognize speech fragments and controlled entities (traffic controllers) respectively, and grounded choice of ANN parameters (parameter values were determined during the testing process).

Experimental researches have shown that the use of the methods provided in article to improve the reliability and speed of TCAS allowed to provide the system operation in real time and to get the percentage of correct traffic controllers authentication at more than 98%.

Development of the authentication system is an important step towards the establishment of an integrated automated system of access control to information resources inholding the authentication of controlled entities, their identification in the event of failure to authentication procedures and control (monitoring) psychophysiological (emotional) condition.

The application of authentication systems allows essentially enhance the safety on transport and in power engineering, sharply reduce the amount of accidents and emergencies due to the reduction of the human factor.

Spysok vykorystanoi literatury: ***1.*** *Ramyshvyly H. S. Avtomatycheskoe opoznavanye hovoriashcheho po holosu. // M.: Radyo y sviaz, 1981. – 224 s.* ***2.*** *S. Khaikyn Neironnыe sety. // 2-e yzd. Per. s anhl. – M.: Yzdatelskyi dom "Vyliams", 2006. – 1104 s.* ***3.*** *Rabyner L., Hould B. Teoryia y prymenenye tsyfrovoi obrabotky syhnalov. // M: Myr, 1978. – 848 s.* ***4.*** *Temnykov V. A., Sharyi T. V., Temnykova E. L., Konforovych Y. V. Holosovaia autentyfykatsyia operatorov, yspolzuiushchykh v protsesse rabotы normatyvno ustanovlennuiu frazeolohyiu. // Informatsiina bezpeka. – 2011. – №1(5). – S.125-130.* ***5.*** *Bishop C. Pattern Recognition and machine learning (Information Science and Statistics). // Springer-Verlag New York, Inc. Secaucus, NJ, USA, 2006. – 738 r.* ***6.*** *Markel Dzh., Hrei A. X. Lyneinoe predskazanye rechy. // Per. s anhl. — Pod red. Iu. N. Prokhorova y V. S. Zvezdyna. — M.: Sviaz, 1980. – 308 s.*

УДК 621.3.038

ТЕПЛОВА НАДІЙНІСТЬ РАДІОЕЛЕКТРОННОЇ АПАРАТУРИ ЗАХИСТУ ІНФОРМАЦІЇ

Борис Уваров, Юрій Зіньковський
Національний технічний університет України "Київський політехнічний інститут"

Стаття: ***9 стор., 7 джерел.***

Внутрішні фізичні процеси, що відбуваються у радіоелектронному апараті (РЕА) при функціонуванні, призводять до виділення теплоти в елементах його електронної структури (ЕЕС), й кількість цієї теплоти залежить від їх енергетичної досконалості, яка повинна бути визначена допустимою температурою їх корпуса. Коефіцієнти енергетичної досконалості $\eta_{ед}$ ЕЕС нульового функціонального рівня – резисторів, конденсаторів, індуктивностей – одержані за допомогою еквівалентних схем двополюсників. Їх значення більші, ніж значення коефіцієнтів корисної дії η елементів, що дає можливість розширити діапазон використання ЕЕС в реальних умовах застосування.

Теплові процеси в РЕА визначають температури ЕЕС та показники як їх надійності, так й надійності всього РЕА. У статті запропоновані методи розрахунку температур ЕЕС в основних структурно-конструктивних модулях першого рівня (СКМ1) – чарунках та мікрозбірках (МЗб).

Теплова модель для МЗб враховує тепловіддачу від ЕЕС, розташованих на ній, теплопровідністю до пластини-основи, конвекцією до оточуючого повітря, радіацією до стінок корпусу РЕА. Враховується також тепловіддача з торців пластини, що може суттєво впливати на тепловий режим МЗб. Розв'язання диференціальних рівнянь математичної моделі проведено методом скінчених інтегральних перетворень.

Наведені рівняння, що пов'язують температури ЕЕС з показниками їх надійності. Таким чином, під час проектування можливо розрахувати показники надійності всіх ЕЕС, окремих МЗб та всього РЕА.

ТЕПЛОВАЯ НАДЕЖНОСТЬ РАДИОЭЛЕКТРОННОЙ АППАРАТУРЫ ЗАЩИТЫ ИНФОРМАЦИИ

Борис Уваров, Юрий Зиньковский
Национальный технический университет Украины "Киевский политехнический нститут"

Внутренние физические процессы, происходящие в радиоэлектронном аппарате (РЭА) при функционировании, приводят к выделению теплоты в элементах его электронной структуры (ЭЭС), и количество этой теплоты зависит от их энергетического совершенства, которое должно определяться допустимой температурой их корпуса. Коэффициенты энергетического совершенства ηэс ЭЭС нулевого функционального уровня – резисторов, конденсаторов, индуктивностей – получены при помощи эквивалентных схем двухполюсников. Их значения больше, чем значения коэффициентов полезного действия η элементов, что дает возможность расширить диапазон использования ЭЭС в реальных условиях применения.

Тепловые процессы в РЭА определяют температуры ЭЭС и показатели как их надежности, так и надежности всего РЭА. В статье предложены методы расчета температур ЭЭС в основных структурно-конструктивных модулях первого уровня (СКМ1) – ячейках и микросборках (МСб).

Тепловая модель для МСб учитывает теплоотдачу от ЭЭС, размещенных на ней, теплопроводностью к пластине-основе, конвекцией к окружающему воздуху, радиацией к стенкам корпуса РЭА. Учитывается также теплоотдача с торцев пластины, что может существенно влиять на тепловой режим МСб. Решение дифференциальных уравнений математической модели проведено методом конечных интегральных преобразований.

Приведены уравнения, связывающие температуры ЭЭС с показателями их надежности. Таким образом, в процессе проектирования можно рассчитывать показатели надежности всех ЭЭС, отдельных МСб и всего РЭА.

THERMAL RADIO EQUIPMENT RELIABILITY OF INFORMATION

Borys Uvarov, Yurij Zinkovsky
National Technical University of Ukraine "Kyiv Polytechnic Institute"

The internal physical processes occurring in the radioelectronic device (RED) at functioning, result in allocation of heat in elements of its electronic structure (EES), and the amount of this heat depends on their power perfection, which should be defined in allowable temperature of their case. The factors of power perfection of EES for a zero functional level - resistors, condensers, inductors are received through the equivalent circuits of two-pole's. Their meanings are more, than meaning of efficiency of elements, that enables to expand a range of use EES in real conditions of application.

The thermal processes in RED define temperatures EES and parameters both their reliability, and reliability all RED. In clause the methods of account of temperatures EES in the basic structural - constructive modules of the first level (SCM1) - cells and microassembly (MAs) are offered.

The thermal model for MAs takes into account heat transfer from EES, placed on her, thermal conductivity to a plate - basis, convection to air, radiation to walls of the case RED. It is taken into account also heat transfer with ends of a plate, that can essentially influence a thermal mode MAs. The decision of the differential equations of mathematical model is carried out by a method of final integrated transformations.

The equations connecting temperatures EES with parameters of their reliability are given. Thus, during designing it is possible to expect parameters of reliability all EES, separate MAs and all RED.

Spysok vykorystanoi literatury: 1. Uvarov B. M., Zinkovskyi Yu. F. Optymizatsiia teplovykh rezhymiv ta nadiinosti konstruktsii radioelektronnykh zasobiv z imovirnisnymy kharakterystykamy: – Kyiv, "Korniichuk", 2011.−248 s. 2. Lыkov A. V. Teplomassoobmen(Spravochnyk). 2-e yzd., pererab. y dop. — M.: Эnerhyia, 1978. — 480 s. 3. DSTU2860-94.Nadiinist tekhniky.Terminy ta vyznachennia. 4. DSTU 2862-94. Metody rozrakhunku pokaznykiv nadiinosti. 5. Prыtkov S. F., Horbacheva V. M., Martыnova M. N., Petrov H. A. Nadezhnost эlektroradyoyzdelyi/Spravochnyk. — MO RF y NYY "Эlektronstandart", 2004. — 620 c. 6. Strelnykov V. P., Fedukhyn A. V. Otsenka y prohnozyrovanye nadezhnosty эlektronnыkh эlementov y system. – K.: Lohos, 2002. 7. Strelnykov V. P. Otsenka resursa yzdelyi эlektronnoi tekhnyky // Matematychni mashyny ta systemy, 2004, # 2.

УДК 638.235.231

ПІДВИЩЕННЯ ВИЯВЛЯЮЧОЇ ЗДАТНОСТІ НЕЛІНІЙНИХ РАДІОЛОКАТОРІВ

Максим Зінченко
Національний технічний університет України «Київський політехнічний інститут»

Стаття: ***5 стор., 5 джерел.***

Використання ефекту нелінійного розсіювання в багатьох сферах людської діяльності сприяло появі численних фундаментальних досліджень за тематикою нелінійної радіолокації. Більшість проведених робіт за цим напрямом присвячені задачі підвищення ефективності виявлення, ідентифікації та локалізації нелінійних розсіювачів (НРс) на фоні різних завад. Як правило, підвищення ефективності використання нелінійних радіолокаторів (НР) у теперішній час зводиться до збільшення потужності випромінюваного НВЧ-сигналу, підвищення чутливості приймачів, вибору оптимальних параметрів зондуючого сигналу (ЗС) тощо. Все це вимагає вирішення досить складних схемотехнічних та конструкторських задач електромагнітної сумісності, забезпечення високої точності вихідних параметрів, завадостійкості тощо, при цьому виграш в більшості незначний та не відповідає витратам. Закладний пристрій як НРс, у своєму складі має струмопровідні елементи − ансамбль «випадкових» антен, в навантаженні котрих можуть знаходитися напівпровідникові прилади. При цьому майже всі «випадкові» антени з нелінійним навантаженням «електрично малі», тобто набагато менше довжини хвилі ЗС НР. Наведений у такій антені струм буде незначним, а створюване їм поле дуже слабким у зв'язку з відсутністю ефективного поглинання НРс енергії ЗС через малі розміри прийомної поверхні. Тому подальший якісний розвиток технології нелінійної радіолокації безпосередньо пов'язаний з максимізацією «нав'язування» енергії зондуючого сигналу НРс. Так як максимально ефективно НРс поглинається енергія тих спектральних складових зондуючого сигналу, довжини хвиль яких зрівнянні з довжинами його «випадкових» антен, тому раціональним для практики є використання чергування різних за амплітудою і формою зондуючих сигналів, що представляють реалізацію випадкового процесу із суцільним спектром.

ПОВЫШЕНИЕ ВЫЯВЛЯЮЩЕЙ СПОСОБНОСТИ НЕЛИНЕЙНЫХ РАДИОЛОКАТОРОВ

Максим Зинченко
Национальный технический университет Украины «Киевский политехнический институт»

Использование эффекта нелинейного рассеяния во многих сферах человеческой деятельности способствовало появлению многочисленных фундаментальных исследований по тематике нелинейной радиолокации. Большинство проведенных работ по этому направлению посвящены задаче повышения эффективности выявления, идентификации и локализации нелинейных рассеивателей (НРс) на фоне различных помех. Как правило, повышение эффективности использования нелинейных радиолокаторов (НР) в настоящее время сводится к увеличению мощности излучаемого СВЧ-сигнала, повышению чувствительности приемников, выбору оптимальных параметров зондирующего сигнала (ЗС) и др. Все это требует решения достаточно сложных схемотехнических и конструкторских задач электромагнитной совместимости, обеспечения высокой точности выходных параметров, помехоустойчивости и т.д., при этом выигрыш в большинстве незначителен и не соответствует затратам. Закладное устройство как НРс, в своем составе имеет токопроводящие элементы – ансамбль «случайных» антенн, в нагрузке которых могут находиться полупроводниковые приборы. При этом почти все «случайные» антенны с нелинейной нагрузкой «электрически малые», то есть намного меньше длины волны ЗС НР. Приведенный в такой антенне ток будет незначительным, а создаваемое им поле очень слабым в связи с отсутствием эффективного поглощения НРс энергии ЗС из-за малых размеров приемной поверхности. Поэтому дальнейшее качественное развитие технологии нелинейной радиолокации непосредственно связано с максимизацией «навязывания» энергии зондирующего сигнала НРс. Так как максимально эффективно НРс поглощается энергия тех спектральных составляющих зондирующего сигнала, длины волн которых сравнимы с длинами его «случайных» антенн, поэтому рациональным для практики является использование чередования различных по амплитуде и форме зондирующих сигналов, представляющих реализацию случайного процесса со сплошным спектром.

THE INCREASING OF NONLINEAR RADAR DETECTION CAPABILITY

Maksym Zinchenko
National Technical University of Ukraine “Kyiv Polytechnic Institute”

Using the effect of nonlinear scattering in many spheres of human activity contributed to the emergence of numerous fundamental studies on nonlinear radar. Most of the works on this subject are devoted to the problem of increasing the efficiency of detection, identification and localization of the nonlinear scatterers (NS) on a different noise acting. As a rule, now more efficient usage of nonlinear radar (NR) is converges to the higher power of the radiated microwave signal, improving receiver sensitivity, the choice of optimum parameters of a probing signal (PS) and others. All of this needs to be addressed fairly complex circuitry and design problems of electromagnetic compatibility, high accuracy of output parameters, noise immunity etc., while the gain in most cases is negligible and does not corresponds to costs. The secret intelligence device as the NS, has in its composition conductive elements - the ensemble of "random" antennas in which load semiconductor devices may be. Moreover, almost all the "random" antennas with nonlinear load are "electrically small", that is much smaller than the wavelength of PS of NR. Induced in such an antenna current is negligible and the produced field is very weak due to the lack of effective energy absorption of PS by NS because of the small size of the receiving antenna. Therefore, further qualitative development of the nonlinear radar technology is directly related to maximizing the "imposition" of the energy of the probing signal NS. Because of the most effective absorption of the energy of the spectral components of the probing signal by NS, which wavelengths are matched with its "random" antennas length, it is rational in practice to use signals alternation of different amplitude and shape that represent the realization of a random process of continuous spectrum.

Spysok vykorystanoi literatury: 1. Khoroshko V. A. Metodы y sredstva zashchytы ynformatsyy / V. A. Khoroshko, A. A. Chekatkov – K. : «Yunyor», 2003. – 504s. 2. Horbachev A. A. Amplytudnыe kharakterystyky nelyneinыkh rasseyvatelei / A. A. Horbachev, S. V. Lartsov, S. P. Tarakanov, E. P. Chyhyn // Radyotekhnyka y эlektronyka. – 1996. – T. 41, # 5. – S. 558–562. 3. Zynchenko M. V. Rasseyvanye ploskykh voln systemoi symmetrychnыkh vybratorov s nelyneinыmy nahruzkamy pry vozdeistvyy nelyneinoho radyolokatora / M. V. Zynchenko, Yu. F. Zynkovskyi // Yzvestyia vыsshykh uchebnыkh zavedenyi. Radyoэlektronyka. NTUU «KPY». – 2010. – Tom 53. – # 10. – S. 24–34. 4. Semenov Э. V. Yssledovanye nelyneinosty preobrazovanyia determynyrovannыkh sverkhshyrokopolosnыkh syhnalov putem lyneinoho kombynyrovanyia otklykov obъekta na lyneino zavysymыe testovыe syhnalы / Э. V. Semenov // Yzv. Tomsk.polytekhn. un-ta. - 2004. - T. 307, # 4. - S. 18-21. 5. Davenport V. B. Vvedenye v teoryiu sluchainыkh syhnalov y shumov / V. B. Davenport, V. L. Rut. − M. : Yzd-vo Ynostrannoi Lyteraturы, 1960. − 468 s.