4 Реферати

УДК 355.433.4:004.324 (045.5)

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СУЧАСНОЇ ІНФОРМАЦІЙНОЇ ЗБРОЇ

Володимир Хорошко, Тетяна Козел, Ольга Ярошенко
Національний авіаційний університет

Стаття: ***5 стор, 7 джерел***.

В сучасній інформаційній війні неможливо досягти поставлених цілей без постійного здійснення заходів інформаційної боротьби та впливів не тільки в ході, але ж ще задовго до її початку та після завершення. Тому фахівці виділяють її як самостійний вид зброї – інформаційну зброю, яка розглядається як засіб ведення інформаційної боротьби. На сьогоднішній день інформаційна зброя є єдиною ефективною зброєю, яка, в умовах науково-технічного прогресу здатна провести одну з протидіючих сторін до перемоги, в той час, як застосування арсеналу сучасної традиційної зброї в глобальному або відносно глобальному конфлікті здатна привести до знищення всіх учасників протистояння або, принаймні, до непоправних втрат в структурі національної безпеки, економіки, оборони та інших важливих сферах життєвої діяльності конфліктуючих сторін такою мірою, що жодна з них не зможе скористатися результатами перемоги. Наводиться класифікація інформаційної зброї та способи, методи та прийоми її застосування.

Інформаційна зброя найбільшу небезпеку становить через те, що її застосування має знеособлений характер і легко маскується під заходи захисту. А в разі створення програмних продуктів у великому обсязі неважко утворити зони по декілька команд, які під час експлуатації програмної системи сформуються в дефект будь-якого типу. Крім того, така зброя дозволяє навіть вести наступальні дії анонімно, без оголошення війни.

В роботі наведені та розглядаються концепції C^4I та C^4IFTW , які передбачають погоджений розвиток систем управління, обчислювальної техніки, зв'язку та розвідки.

Крім того, розглядаються алгоритми "завжди перемоги" та проведення, впливу гіпнотичного стану на суспільство.

Виділяють такі основні види інформаційної зброї як: інформаційно-технічна зброя, що впливає на інформаційні ресурси, інформаційну інфраструктуру збройних сил, держави в цілому та інформаційно-психологічна зброя, що впливає на морально-психологічний стан людини, соціальних та інших груп населення, суспільства в цілому.

ОСОБЕННОСТИ ПРИМЕНЕНИЯ СОВРЕМЕННОЙ ИНФОРМАЦИОННОЙ ОРУЖИЯ

Владимир Хорошко, Татьяна Козел, Ольга Ярошенко
Национальный авиационный университет

В современной информационной войне невозможно достичь поставленных целей без постоянного осуществления мер информационной борьбы не только в ходе, но еще задолго до ее начала и после завершения. Поэтому специалисты выделяют как самостоятельный вид оружия - информационное оружие, которое рассматривается как средство ведения информационной борьбы. В настоящее время информационное оружие является единственным эффективным оружием, которое, в условиях научно-технического прогресса способно провести одну из противоборствующих сторон к победе, в то время, как применение арсенала современного традиционного оружия в глобальном или относительно глобальном конфликте способно привести к уничтожению всех участников противостояния или, по крайней мере, к невосполнимым потерям в структуре национальной безопасности, экономики, обороны и в других важных сферах жизненной деятельности конфликтующих сторон в такой степени, что ни одна из них не сможет воспользоваться результатами победы. Приводится классификация информационного оружия, способы, методы и приемы ее применения.

Информационное оружие наибольшую опасность представляет потому, что его применение имеет обезличенный характер и легко маскируется под меры защиты. А в случае создания программных продуктов

в большом объеме нетрудно создать зоны по несколько команд, которые во время эксплуатации программной системы сформируются в дефект любого типа. Кроме того, такое оружие позволяет даже вести наступательные действия анонимно, без объявления войны.

В работе приведены и рассматриваются концепции C^4И и C^4 FTW, предусматривающих согласование развитие систем управления, вычислительной техники, связи и разведки.

Кроме того, рассматриваются алгоритмы "всегда победы" и проведения, влияния гипнотического состояния на общество.

Выделяют следующие основные виды информационного оружия: информационно-техническая оружие, которое влияет на информационные ресурсы, информационную инфраструктуру вооруженных сил, государства в целом, и информационно-психологическое оружие, которое влияет на морально-психологическое состояние человека, социальных и других групп населения, общества в целом.

FEATURES OF MODERN WEAPONS OF INFORMATION

Vladimir Khoroshko, Kozel Tatiana, Olga Yaroshenko
National Aviation University

In the current information war can not achieve its goals without the constant fighting taking measures of information not only during, but long before the beginning and after. Therefore, experts distinguish as an independent weapons - information weapons, which is seen as a means of keeping information struggle. Nowadays, information weapons is the only effective weapon, which, in terms of scientific and technological progress is able to hold one of the opposing sides to victory, while as the use of traditional arsenal of modern weapons globally or with respect to the global conflict can lead to the destruction of all opposition members or at least to irreparable loss in structure of national security, economic, defense and other vitally important areas of the conflicting parties to such an extent that none of them can take advantage of the victory. A classification of information weapons and methods, techniques and methods of application.

Information is the most dangerous weapon because its use is impersonal in nature and easily disguised protection measures. And in the case of software products in large volume is easy to create a zone of several teams that during the operation software system will form a defect of any kind. In addition, this allows even carry weapons offensive anonymously, without declaring war.

The article describes the concept and considered S4I and C4 FTW, which provide for the approval of control systems development, computing, communications and intelligence.

In addition, the algorithms are considered "always win" and holding, hypnotic state influence on society.

There are following types of information weapons as information-technology weapons that affects the information resources, information infrastructure of the armed forces, the state in general and information and psychological weapon that affects the moral and psychological condition, social and other groups in society general.

Spisok vikoristanoï literaturi: 1. Levchenko O. Zavdannya, ob'ekti ta formi vedennya informatsiynoï borot'bi/Levchenko O.//Visnik voєnnoï rozvidki. — K.: VDA GUR MOU Ukraïni, Vip.21, 2010. — S.7-11. 2. Rogovskiy YE. A. Pentagon usilivayet kiberoboronu/Rogovskiy YE.A., Sharikov P.A.//Nauchnyy i obshchestvenno-politicheskiy zhurnal "SSHA – Kanada. Ekonomika – politika – kul'tura", №1, yanvar' 2011. — S.51-60. 3. Shafrans'kiy R. Teoriya informatsiynoï zbroï. / Per. V. Kazennova. — M:VIKA, 2002,189 s. 4. Istoriya informatsiyno-psikhologichnogo protiborstva : pidruch. /[Ya. M. Zharkov, L. F. Kompantseva, V. V. Ostroukhov V. M. Petrik, M. M. Prisyazhnyuk, Є. D. Skulish]/ — K. : Nauk. —vid. viddil NA SB Ukraïni, 2012. — 212 s. 5. Prigozhin A. I. Osobennosti chetvertoy mirovoy voyny // Vestnik Moskovskogo universiteta. Ser. 18. Sotsiologiya i politologiya. — 2004. — № 3. — S. 60. 6. Pocheptsov G. G. Informatsiya i dezinformatsiya. — K.: Nika-Tsentr, El'ga, 2001. — 256s. 7. Panarin I. N. Tekhnologiya informatsionnoy voyny. — M.: „KSP+", 2003. — 320 s.

УДК 004.056

ОЦІНЮВАННЯ КОЕФІЦІЄНТА ЯКОСТІ ШУМОВОЇ ЗАВАДИ В СИСТЕМАХ АКТИВНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Михайло Прокофьєв, Вадим Куліш, Микола Ващенко, Володимир Дворський, Василь Стеченко, Андрій Тодоренко
НДЦ «ТЕЗІС» НТУУ «КПІ»

Стаття: *6* ***стор, 8 джерел***.

Захист інформації на об'єктах інформаційної діяльності заснований на ослабленні або маскуванні рівнів інформативних електромагнітних випромінювань і наведень на границі контрольованої зони. Частіше для цього використовують активний захист, при якому формуються та випромінюються на цих об'єктах сигнали завади, рівень яких за потужністю перевищують рівні інформативних випромінювань. У системах просторового зашумлення в основному використовуються завади типу "білий шум" з енергетичним спектром, близьким до рівномірного, з спектральною щільністю потужності, достатньої для надійного маскування інформативних випромінювань. При цьому джерела маскуючих завад мають забезпечувати відповідне значення коефіцієнта якості шуму, що враховує відмінність щільності ймовірностей розподілу миттєвих значень амплітуд компонент ЕМП шуму від щільності ймовірностей їх нормального гаусового розподілу.

Один з основних методів оцінювання коефіцієнта якості шуму генераторів маскуючих завад у сфері ТЗІ заснований на розкладанні функції щільності ймовірностей миттєвих значень завади у ряд Еджворта. Застосовують і метод, заснований на визначенні коефіцієнта якості шуму через ентропію завади. В статті обґрунтовано доцільність застосування методу визначення коефіцієнта якості шуму через ентропію завади. Цей метод дозволяє вирішити задачу з використанням більш простого алгоритму. Завдяки цьому практичну його реалізацію можна здійснити не тільки за допомогою спеціалізованих приладів, але і за допомогою сучасних осцилографів з вбудованими процесорами. Процесори осцилографів дозволяють здійснювати необхідні для цих цілей математичні операції.

Наведено результати експериментальних досліджень генераторів маскуючих завад «Волна-4Р» і «Дельта-7» з визначення їх статистичних характеристик маскуючи завад. Для порівняння особливостей реалізації методів наведено результати досліджень генераторів на двох стендах. До складу першого стенду входили прилади Х6-4, Х6-5 і осцилограф TDS-2012B (виробник Textronix). До складу другого стенду входили універсальний осцилограф DS-1150C (виробник ROHDE&SCHWARZ) і персональний комп'ютер. Осцилограф DS-1150C використовувався як індикатор функції щільності розподілу ймовірностей. Персональний комп'ютер використовувався для розрахунку статистичних параметрів за даними гістограм. В якості приймальної антени використовувалася антена АИЗ-3. Для посилення шумових сигналів, прийнятих антеною, на вході Б приладу Х6-5 встановлювався широкосмуговий підсилювач з смугою пропускання до 1 ГГц.

Результати експериментальних досліджень свідчать, що дані, отримані при дослідженні генераторів на обох стендах (що реалізують методи, засновані на розкладанні функції у ряд по ортогональним поліномам Чебишева-Ерміта і ентропії) практично співпадають. Відмінність даних не перевищує декількох процентів.

ОЦЕНИВАНИЕ КОЭФФИЦИЕНТА КАЧЕСТВА ШУМОВОЙ ПОМЕХИ В СИСТЕМАХ АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Михаил Прокофьев, Вадим Кулиш, Николай Ващенко, Владимир Дворский, Василий Стеченко, Андрей Тодоренко
НИЦ «ТЕЗИС» НТУУ «КПИ»

Защита информации на объектах информационной деятельности основана на ослаблении или маскировке уровней информативных электромагнитных излучений и наводок на границе контролируемой зоны. Чаще для этого используют активную защиту, при котором формируются и излучаются на этих объектах сигналы помехи, уровень которых по мощности превышают уровни информативных излучений. В системах пространственного зашумления в основном используются помехи типа «белый шум» с энергетическим спектром, близким к равномерному, со спектральной плотностью мощности, достаточной для надежного маскировки информативных излучений. При этом источники маскирующих помех должны обеспечивать

соответствующее значение коэффициента качества шума, учитывающее отличие плотности вероятностей распределения мгновенных значений амплитуд компонент ЭМП шума от плотности вероятностей их нормального гауссова распределения.

Основными методами оценки коэффициента качества шума генераторов маскирующих помех в сфере ТЗИ являются методы, основанные на разложении функции плотности вероятности мгновенных значений помехи в ряд Эджворта, и методы, основанные на определении коэффициента качества шума через энтропию помехи. Обоснована целесообразность применения метода определения коэффициента качества шума через энтропию помехи. Этот метод позволяет решить задачу с использованием более простого алгоритма и благодаря этому практическую его реализацию не только с помощью специализированных приборов но и с помощью современных осциллографов со встроенными процессорами, которые позволяют осуществлять необходимые для этих целей математические операции.

Приведены результаты экспериментальных исследований генераторов маскирующих помех «Волна-4Р» и «Дельта-7» по определению статистических характеристик генераторов маскирующих помех на примере двух стендов. В состав первого стенда входили приборы Х6-4, Х6-5 и осциллограф TDS-2012B (производитель Textronix), а в состав второго стенда универсальный осциллограф DS-1150C (производитель ROHDE & SCHWARZ) и персональный компьютер. Осциллограф DS-1150C использовался как индикатор функции плотности распределения вероятностей. Персональный компьютер использовался для расчета статистических параметров по данным гистограмм. В качестве приемной антенны использовалась антенна АИЗ-3. Для усиления шумовых сигналов, принятых антенной, на входе Б прибора Х6-5 устанавливался широкополосный усилитель с полосой пропускания до 1 ГГц.

Результаты экспериментальных исследований свидетельствуют, что данные, полученные при использовании стендов, реализующих методы, основанные на разложении функции в ряд по ортогональным полиномам Чебышева-Эрмита и энтропии, практически совпадают. Отличие данных не превышает нескольких процентов.

EVALUATION OF FACTOR QUALITY NOISE HURT IN SYSTEMS OF ACTIVE INFORMATION PROTECTION

Mikhail Prokofiev, Vadim Kulish, Mykola Vaschenko, Vladimir Dvorsky, Vasil Stechenko, Andrey Todorenko

SRC "TEZIS" NTUU "KPI"

Data protection information activities at the sites is based on weakening or disguise levels of informative electromagnetic radiation and interference in the border of controlled area. Active defense is mostly often used for this purpose due which are formed and emitted signals at these sites interference level of which exceeds the power level of informative radiation. In systems of spatial noise mainly used noise of "white noise" type with energy spectrum close to uniform, with spectral power density sufficient for reliable masking of informative radiation. This masking noise source should provide appropriate coefficient as noise, taking into account the difference between probability of density distribution of instantaneous values of amplitude component EMF noise and probability density of the normal Gaussian distribution.

The main methods of evaluating quality factor masking noise generator noise in the proofing methods are based on the decomposition of probability density function of instantaneous values of noise in a number of Edgeworth and methods based on determining the quality factor by entropy noise disturbance. The expediency of the method of determining the quality factor by entropy noise disturbance is presented. This method allows to solve the problem using of simple algorithm and thus its practical implementation not only through specialized devices but with modern oscilloscopes with embedded processors to allow necessary for this purpose mathematical operations.

The results of experimental studies masking noise generators "Wave-4R" and "Delta-7" to determine the statistical characteristics of masking noise generators the example of two stands. The structure of the stand were the first instruments X6-4, X6-5 and oscilloscope TDS-2012B (manufacturer Textronix), and of the second stand universal oscilloscope DS-1150C (manufacturer ROHDE & SCHWARZ) and personal computer. DS-1150C oscilloscope was used as an indicator of the probability distribution density function. The personal computer was used to calculate statistical parameters according to histograms. AY3-3 antenna is used as the receiving antenna. To enhance the noise signal received antenna inlet B H6-5 device installed broadband amplifier with bandwidth up to 1 GHz.

The results of experimental studies indicate that the data obtained by using stands, implementing methods based on the decomposition of functions in series of orthogonal polynomials Chebyshev-Hermite and entropy coincide. The difference between data does not exceed a few percents.

Spisok vikoristanoї literaturi:1. Rubichev N. A. Ocenka i izmerenie iskajenii radiosignalov. _ M._ «Sovetskoe radio»_ 1978. – 168 s. 2. Kolmogorov A. N._. Fomin S. V. Elementi teorii funkcii i funkcionalnogo analiza. – M._ FIZMATLIT_ 2004. – 372 s. 3. Levin B. R. Teoreticheskie osnovi statisticheskoi radiotehniki. Kniga pervaya. _ M._ «Sov. radio»_ 1974. _ 552 s. 4. Tihonov V. I. Statisticheskaya radiotehnika. _M._ «Sov. radio»_ 1966 _ 678 s. 5. Kramer Garold_ Matematicheskie metodi statistiki. _ M._ «Mir»_ 1975. – 720 s. 6. Goryainov V. T._ Juravlev A. G._ Tihonov V. I. Primeri i zadachi po statisticheskoi radiotehnike. – M._ «Sovetskoe radio»_ 1970. – 600 s. 7. Dmitriev V. I. Prikladnaya teoriya informacii. – M._ Visshaya shkola_ 1989. – 320 s. 8. Kupriyanov A. I._ Saharov A. V. Teoreticheskie osnovi radioelektronnoi borbi. – M._ Vuzovskaya kniga_ 2007. – 470 s.

УДК 004.43(031):681.3.01(02)

ВИКОРИСТАННЯ БАЗ ДАНИХ ПРИ ПРОЕКТУВАННІ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Володимир Луценко
НТУУ «КПІ», ФТІ

Стаття: ***7 стор, 6 джерел.***

Складні системи при своєму проектуванні передбачають необхідність прийняття рішень при суперечливих або неповних даних. Також спостерігається наявність великої кількості неузгоджених параметрів у вигляді початкових даних про об’єкт проектування. Показано, що за таких умов на двох етапах проектування КСЗІ, а саме, на етапі обстеження об’єктів при визначенні дестабілізуючих факторів, котрі створюють загрози, та на етапі переходу від загроз до контрдій, рішення носять суб’єктивний характер. Для підвищення об’єктивності прийняття рішень при проектуванні необхідним є максимальна автоматизація процесу проектування. Специфіка середовища проектування вимагає залучення відносно складних методів, таких як логіко-семантичні методи, нечіткі множини або системи інтелектуальної підтримки прийняття рішень при неповністю визначених вхідних даних, моделювання образів об’єктів та ін. У будь якому випадку, мова йде про математичні, логічні або семантичні процедури над великою кількістю даних у вигляді змістовно-образних масивів. Тобто неминучою є необхідність використання специфічних баз даних (БД) для зберігання, поповнення та взаємодії інформаційних масивів опису об’єктів, можливих дестабілізуючих факторів, загроз та контрдій для об’єктів будь-якої складності. Відомі бази даних та їх моделі мають і переваги і недоліки. На думку автора визначені в роботі недоліки можна компенсувати створенням системи автоматизованого проектування КСЗІ при використанні пам’яті з вибіркою за змістом запиту (асоціативною пам’яттю – АП), наприклад, на базі моделі нейроподібної ансамблевої сітки з навчанням. Тоді завданням роботи стає знаходження доказової бази щодо незворотності такого підходу з одного боку, а з другого, щодо дійсних можливостей реального створення такої системи проектування. Методологія створення такої системи та її використання має забезпечувати головні властивості КСЗІ, а саме дієвість реалізації та об’єктивність у прийнятті рішень при функціонуванні незалежно від складності об’єкту та умов його життєдіяльності.

ИСПОЛЬЗОВАНИЕ БАЗ ДАННЫХ ПРИ ПРОЕКТИРОВАНИИ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Владимир Луценко
НТУУ «КПИ», ФТИ

Сложные системы при своем проектировании предусматривают необходимость принятия решений при противоречивых или не полных данных. Также наблюдается наличие большого количества несогласованных параметров в виде начальных данных об объекте проектирования. Показано, что на двух этапах проектирования решения субъективны. Это такие этапы, как обследование объектов при определении дестабилизирующих факторов, создающих угрозы, и на этапе перехода от угроз к контрдействиям. Для увеличения объективности принятия решений необходима максимальная автоматизация процедуры

проектирования. Специфика среды проектирования требует привлечения относительно сложных методов проектирования, таких, как логико-семантических, нечетких множеств или систем интеллектуальной поддержки принятия решений при неопределенных входных данных, методов моделирования образов объектов и др. В любом случае речь идет о математической, логической или семантической процедуре над большим количеством данных в виде смысловых образных массивов. Неизбежна необходимость применения специфических баз данных для хранения, пополнения и взаимодействия информационных массивов описания объектов, возможных дестабилизирующих факторов, угроз и контрдействий на объектах любой сложности. Известные базы и их модели имеют и преимущества и недостатки. По мнению автора недостатки могут быть компенсированы созданием систем автоматического проектирования комплексных систем защиты информации с использованием памяти с выборкой по содержанию запроса (иначе – ассоциативной памяти АП). Пример – модель нейроподобная ансамблевая сеть с обучением. Следующей задачей является нахождение доказательной базы необратимости такого подхода с одной стороны, и возможности создания такой системы, с другой. Методология создания такой системы и ее использование должно обеспечить главные свойства комплексных систем защиты информации. Это действенность реализации и объективность принятия решений независимо от сложности объекта и условий его жизнедеятельности.

USE OF DATABASES AT DESIGNING OF COMPLEX SYSTEMS OF PROTECTION OF THE INFORMATION

Vladimir Lutsenko
NTUU "KPI", PhTI

Difficult systems at the designing provide necessity of decision-making at inconsistent or not the full data. Also presence of a considerable quantity of not co-ordinated parametres in the form of the initial data about installation of designing is observed. It is shown that at two design stages of the solution are subjective. These are such stages, as diagnostic study of installations at definition of factors of the destabilization creating threats, and at a stage of transition from threats to counteractions. For maximum automation of procedure of designing is necessary for increase in objectivity of decision-making. Specificity of medium of designing demands attraction concerning difficult methods of designing. These are logiko-semantic methods, illegible assemblage or systems of an intellectual support of decision-making at an uncertain input information, methods of modelling of images of installations, etc. Anyway it is a question of mathematical, logic or semantic procedure over a considerable quantity of the data in the form of semantic figurative files. Necessity of application of specific databases for storage, replenishments and interactings of the informational files of the description of installations, possible factors of destabilization, threats and counteractions on installations of any complexity is inevitable. Known baselines and their models have also merits and demerits. According to the author deficiencies can be compensated creation of systems of automatic designing of complex systems of protection of the information with use of memory with sample under the inquiry maintenance (differently – associative memory AM). An instance – model neuronal assambly network with instruction. From this point on a work problem is the finding of demonstrative baseline of irreversibility of such approach on the one hand, and possibilities of creation of such system, with another. Methodology of creation of such system and its use should provide the main properties of complex systems of protection of the information. It is effective implementation and objective decision-making irrespective of complexity of installation and conditions of its ability to live.

Spisok vikoristanoï literaturi: 1. DSTU ISO/IEC TR 13335:2003. Informatsiyni tekhnologiï // Nastanovi z keruvannya bezpekoyu informatsiynikh tekhnologiy. Chastina 1: Kontseptsiï ta modeli bezpeki informatsiynikh tekhnologiy. Chastina 2: Keruvannya ta planuvannya bezpeki informatsiynikh tekhnologiy. Chastina 3: Metodi keruvannya bezpekoyu informatsiynikh tekhnologiy. 2. DSTU 3396.1-96. Zakhist informatsiï // Tekhnichniy zakhist informatsiï. Poryadok provedennya robit. 3. Lutsenko V. M. Viznachennya urazlivosti ob'єktiv informatsiynoï diyal'nosti yak skladova poryadku rozrobki sistem zakhistu informatsiï / Lutsenko V. M., Khudyakov V. O. // Pravove, normativne ta metrologichne zabezpechennya sistemi zakhistu informatsiï v Ukraïni. .-K.: CHP «EKMO», NITS «TEZIS» NTUU «KPI», 2011. Vip. 2 (21) s. 49–55. 4. Gerasimenko V. A. Zashchita informatsii v avtomatizirovannykh sistemakh obrabotki dannyakh / Kn. 1 – M.: Energoatomizdat, 1994 – 400 s. 5. IT Baseline Protection Manual. YElektronniy resurs: http://www.bsi.bund.de/gshb/English/t/t1000.htm na termin 04.2010 r. 6. GOST R ISO MEK TO 10032-2007.

УДК 65.012.8+34

ОКРЕМІ АСПЕКТИ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ ВІЙНІ В УКРАЇНІ

Віталій Носов, Олександр Манжай
Харківський національний університет внутрішніх справ

Стаття: ***7 стор, 16 джерел.***

В роботі проаналізовано зміст та структуру інформаційного протиборства, наведено визначення ключових понять у даній сфері (інформаційне протиборство, інформаційна війна, інформаційний тероризм, інформаційна експансія тощо), визначено мету та форми ведення інформаційної війни. Підкреслено, що інформаційна війна складається із сукупності інформаційних атак, об'єднаних єдиним замислом. Авторами встановлено, що характерними рисами інформаційної війни, які відрізняють її від звичайної, є: відсутність видимих фізичних руйнувань, непередбачуваність засобів ведення інформаційної війни, встановлення контролю над свідомістю людських ресурсів противника, вибірковість за принципом досягнення найбільшого ефекту, неефективність у випадку слабкої інформаційної інфраструктури країни впливу, нівелювання розуміння правди, вплив на хід думок супротивника з метою прийняття останнім вигідного для атакуючого рішення, переведення переваг супротивника в його недоліки, гра на емоціях, відволікання розуму на негідний об'єкт. На підставі вивчення літературних джерел та аналітичного матеріалу запропоновано окремі заходи протидії інформаційній війні та інформаційно-психологічному впливу. Підкреслюється суттєва роль засобів масової інформації та громадськості як у веденні, так і в протидії інформаційній війні. Наведено конкретні приклади спроб інформаційного впливу, розглянуто структуру відповідних повідомлень та методику їх аналізу. Запропоновано створити центр реагування та проведення спеціальних операцій з метою нейтралізації інформаційних загроз, впровадити в освітній процес заняття з «Основ інформаційної безпеки», активізувати наукові пошуки у сфері інформаційного протиборства, активізувати дискусію на міжнародному рівні щодо врегулювання визначення понять та заборони інформаційної агресії й інформаційної зброї.

НЕКОТОРЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ ИНФОРМАЦИОННОЙ ВОЙНЕ В УКРАИНЕ

Виталий Носов, Александр Манжай
Харьковский национальный университет внутренних дел

В работе проанализированы содержание и структура информационного противостояния, приведены определения ключевых понятий в данной сфере (информационное противостояние, информационная война, информационный терроризм, информационная экспансия и тому подобное), определенны цель и формы ведения информационной войны. Подчеркнуто, что информационная война состоит из совокупности информационных атак, объединенных единым замыслом. Авторами установлено, что характерными чертами информационной войны, которые отличают ее от обычной, являются: отсутствие видимых физических разрушений, непредсказуемость средств ведения информационной войны, установления контроля над сознанием человеческих ресурсов противника, выборочность по принципу достижения наибольшего эффекта, неэффективность в случае слабой информационной инфраструктуры страны влияния, нивелирование понимания правды, влияние на ход мысли противника с целью принятия последним выгодного для атакующего решения, перевод преимуществ противника в его недостатки, игра на эмоциях, отвлечение разума на негодный объект. На основании изучения литературных источников и аналитического материала предложены отдельные мероприятия по противодействию информационной войне и информационно психологическому влиянию. Подчеркивается существенная роль средств массовой информации и общественности как в ведении, так и в противодействии информационной войне. Приведены конкретные примеры попыток информационного влияния, рассмотрена структура соответствующих сообщений и методика их анализа. Предложено создать центр реагирования и проведения специальных операций с целью нейтрализации информационных угроз, внедрить в образовательный процесс занятия по «Основам информационной безопасности», активизировать научные поиски в сфере информационного противостояния, активизировать дискуссию на международном уровне относительно урегулирования определения понятий и запрета информационной агрессии и информационного оружия.

SOME ASPECTS OF INFORMATION WAR COUNTERACTION IN UKRAINE

Vitalii Nosov, Oleksandr Manzhai
Kharkiv National University of Internal Affairs

In this paper maintenance and structure of the information confrontation are analysed, the definitions of key concepts in this sphere are presented (information confrontation, information war, information terrorism, information expansion and others like that), the forms and aim of infowar are defined. Underline, that information war consists of aggregate of informative attacks, incorporated the unique idea. It is set by authors, that the personal touches of information war, which distinguish it from ordinary is: absence of visible physical destructions, unpredictability of facilities of information war conducting, instituting control above consciousness of human sources of opponent, selectivity on principle of achievement of most effect, inefficiency in the case of weak information infrastructure of country of influence, leveling of understanding of true, influence on motion of opinions of opponent with the purpose of decision acceptance advantageous for attacking side, conversion of opponent advantages to his failings, playing on emotions, distraction of mind to an unworthy object. On the basis of study of literary sources and analytical materials the separate measures of combating infowar and information psychological influence are offered. The substantial role of mass and public medias is underlined both in a conduction and in counteraction of information war. The specific examples of attempts of information influence are presented, the structure of the proper messages and method of their analysis are considered. It is suggested to create the center of reacting and conducting of the special operations with the purpose of neutralization of information threats, to inculcate training of «Basics of Information Security» in an educational process, to activate scientific searches in the field of the information confrontation, to activate a discussion at an international level in relation to the settlement of definition of concepts and prohibition of information aggression and information weapon.

Spisok vikoristanoï literaturi: 1. Konstitutsiya Ukraïni vid 28.06.1996 // Vidomosti Verkhovnoï Radi Ukraïni. – 1996. – № 30 (23.07.1996). 2. Turchinov: Prioritetnym napravleniyem informbezopasnosti yavlyayetsya obespecheniye nastupatel'nosti [YElektronniy resurs]. – Rezhim dostupu: http://112.ua/obshchestvo/turchinov-prioritetnym-napravleniem-informbezopasnosti-yavlyaetsya-obespechenie-nastupatelnosti-218242.html. 3. Panarin I. N. Informatsionnaya voyna i geopolitika / I.N. Panarin. – M. : Izdatel'stvo «Pokoleniye», 2006. – 560 s. 4. Leontєva L. Informatsiyna viyna v yepokhu globalizatsiï [YElektronniy resurs] / L. Leont'єva. – Rezhim dostupu: http://www.ji-magazine.lviv.ua/seminary/2000/sem13-04.htm. 5. Manzhay O. V. Pravovi zasadi zakhistu informatsiï: navchal'niy-posibnik / O.V. Manzhay. – Kharkiv : Nika Nova, 2014. – 104 s. – z il. 6. Zelenina YE. V Korolevstve krivykh zerkal… / YE. Zelenina // Vremya. – Vtornik. – Dekabr' 17. 2013. – № 181 (17337). – S. 1-2. 7. Medvedєv V. K. Suchasna informatsiyna viyna ta ïï obris / V. K. Medvedєv, Yu. F. Kucherenko, R. M. Guz'ko // Sistemi ozbroєnnya i viys'kova tekhnika. – 2008. – № 1. – S. 52-54. 8. Sharma S. Securing Information Infrastructure from Information Warfare / Sushil K. Sharma, Jatinder N.D. Gupta // Logistics Information Management. – 2002. – № 15(5/6). – P. 414-422. 9. Poda T. A. Informatsiyna viyna yak strategiya formuvannya politichnoï svidomosti(sotsial'no-filosofs'kiy analiz) / T. A. Poda // Visnik Natsional'nogo aviatsiynogo universitetu. Ser. : Filosofiya. Kul'turologiya. – 2014. – № 1. – S. 67-70. 10. Yushchenko A. G. Ukraina obyazana vyigrat' informatsionnuyu voynu / A. G. Yushchenko // Ukraïna tretє tisyacholittya. – 2014. – № 3. – S. 21-23. 11. Saprikin O. Informatsiyna yekspansiya, informatsiyna viyna ta informatsiyna ataka u zasobakh masovoï informatsiï na prikladi Євro-2012 / O. Saprikin // Visnik Knizhkovoï palati. – 2013. – № 1. – S. 40-43.. 12. Smol'ts S. P. Informatsiyna viyna yak chinnik formuvannya suspil'nogo buttya / S. P. Smol'ts // Visnik Natsional'nogo tekhnichnogo universitetu Ukraïni «Kiïvs'kiy politekhnichniy institut». Filosofiya. Psikhologiya. Pedagogika. – 2011. – № 3. – S. 70-74. 13. Kondratyuk M. O. Informatsiyna viyna ta rol' mas-media v mizhnarodnikh konfliktakh / M. O. Kondratyuk // Visnik Kharkivs'koï derzhavnoï akademiï kul'turi. – 2013. – Vip. 41. – S. 108-113. 14. Osepashvili D. New Media and Russian-Georgian August 2008 War / Dali Osepashvili // Journalism and Mass Communication. – 2014. – Vol. 4, No. 6. – P. 360-366. 15. Protivodeystviye negativu v informatsionnom prostranstve: metodicheskiye rekomendatsii / Z. Chistyakov, M. Shpachenko. – Agentstvo konfliktnogo PR - /PR i Z/, 2012. – 32 s. 16. Ryazantseva I. M. Problemni pitannya rozbudovi natsional'noï sistemi kiberbezpeki / I. M. Ryazantseva, V. V. Tulupov // Pravo i bezpeka. – 2014. –№ 2 (53). – S. 140-144.

УДК 621.391:519.2:519.7

ПОБУДОВА ВЕРХНІХ ОЦІНОК СЕРЕДНІХ ІМОВІРНОСТЕЙ ЦІЛОЧИСЕЛЬНИХ ДИФЕРЕНЦІАЛІВ КОМПОЗИЦІЇ МОДУЛЬНОГО КЛЮЧОВОГО СУМАТОРА, БЛОКА ПІДСТАНОВКИ ТА ЛІНІЙНОГО ОПЕРАТОРА, ЩО МАЄ БЛОКОВУ СТРУКТУРУ

Людмила Ковальчук, Наталія Кучинська, Леонід Скрипник
Інститут спеціального зв'язку та захисту інформації НТУУ "КПІ"

Стаття: *13* ***стор, 18 джерел.***

Для побудови оцінок стійкості блокового алгоритму шифрування до різницевого криптоаналізу та його різноманітних модифікацій, як правило, необхідно оцінити зверху середню імовірність раундового диференціалу. Раундові функції більшості сучасних блокових алгоритмів шифрування (AES, ГОСТ 28147, "Калина") містять композицію ключового суматора, блока підстановок і оператора, лінійного над полем F_2 або деяким його розширенням. Тому задача оцінювання стійкості блокових шифрів або зводиться до задачі побудови верхніх оцінок середніх імовірностей таких композицій, або містить її. В представленій роботі вперше отримано верхні оцінки середніх імовірностей цілочисельних диференціалів відображень, які є композиціями ключового суматора, блока підстановки та лінійного (над деяким кільцем) оператора, а також визначено параметри s-блоків, від яких залежать дані оцінки, та умови, що забезпечують якомога менші значення цих оцінок. Також наведено статистичні розподіли для вказаних параметрів. Отримані результати дозволяють аналізувати різницеві властивості раундових функцій блокового алгоритму шифрування, а, отже, і всього алгоритму.

ПОСТРОЕНИЕ ВЕРХНИХ ОЦЕНОК СРЕДНИХ ВЕРОЯТНОСТЕЙ ЦЕЛОЧИСЛЕННЫХ ДИФФЕРЕНЦИАЛОВ КОМПОЗИЦИИ МОДУЛЬНОГО КЛЮЧЕВОГО СУММАТОРА, БЛОКА ПОДСТАНОВКИ И ЛИНЕЙНОГО ОПЕРАТОРА С БЛОЧНОЙ СТРУКТУРОЙ

Людмила Ковальчук, Наталия Кучинская, Леонид Скрыпник
Институт специальной связи и защиты информации НТУУ "КПИ"

Для построения оценок стойкости блочного алгоритма шифрования к разностному криптоанализу и различным его модификациям, как правило, необходимо оценить сверху среднюю вероятность раундового дифференциала. Раундовые функции большинства современных блочных алгоритмов шифрования (AES, ГОСТ 28147, "Калина") содержат композицию ключевого сумматора, блока подстановки и оператора, линейного над полем F_2 или некоторым его расширением. Поэтому задача оценивания стойкости блочных шифров или сводится к задаче построения верхних оценок средних вероятностей таких композиций, или содержит её как подзадачу. В представленной работе впервые получены верхние оценки средних вероятностей целочисленных дифференциалов отображений, которые являются композициями ключевого сумматора, блока подстановки и линейного (над некоторым кольцом) оператора, а также определены параметры s-блоков, от которых зависят данные оценки, и условия, обеспечивающие как можно меньшие значения этих параметров. Полученные результаты позволяют анализировать разностные свойства раундовых функций блочного алгоритма шифрования, а, следовательно, и всего алгоритма.

THE UPPER BOUNDS OF THE INTEGER DIFFERENTIALS AVERAGE PROBABILITIES FOR COMPOSITION OF THE MODULAR KEY ADDER, SUBSTITUTION BLOCKS AND THE BLOCK-STRUCTURED LINEAR OPERATOR

Lyudmila Kovalchuk, Nataliia Kuchynska, Leonid Skrypnik
Institute of Special Communication and Information Security of National Technical University of Ukraine "Kyiv Polytechnic Institute"

To estimate a block cipher resistance to the differential cryptanalysis and its various modifications, as a rule, it is necessary to obtain the upper bounds of the round differential average probability. Round functions of most of the modern block encryption algorithms (e.g. AES, GOST 28147, "Kalina") contain the composition of the key adder, substitution blocks, and the operator, which is linear over F_2 or some its extension. Therefore, the problem of obtaining upper bounds for block ciphers resistance is reduced to the problem of constructing upper bounds for the average probability of such compositions, or consists it as a subtask. In this work, the upper bounds are obtained for the integer differentials average probability of maps which are compositions of the key adder, substitution blocks, and the linear (over some ring) operator. The parameters of s-blocks, on which these bounds are depended, are defined and conditions, to ensure the least possible values of these parameters, are given. Obtained results allow us to analyze the differential properties of the round function of block encryption algorithm and therefore the differential properties of the whole block encryption algorithm.

Spisok vikoristanoï literaturi:1. National Institute of Standards and Technology: The Advanced Encryption Standard (AES) – Rezhim dostupa: http://csrc.nist.gov/aes/ 2. GOST 28147-89. Sistemy obrabotki informatsii. Zashchita kriptograficheskaya. Algoritm kriptograficheskogo preobrazovaniya. – M.: Gosstandart SSSR, 1989. – 28s. 3. Gorbenko I. D., Tots'kiy O. S., Kaz'mina S. V. Perspektivniy blokoviy shifr "Kalina" – osnovni polozhennya ta spetsifikatsiya // Prikladna radioyelektronika. – 2007. - t.6, №2. –.S.195-208.4. Gorbenko I. D., Bondarenko M. F. ta in. Perspektivniy blokoviy shifr "Mukhomor" – osnovni polozhennya ta spetsifikatsiya // Prikladna radioyelektronika. – 2007. – t.6. №2. – S.147-157. 5. Kovalchuk L., Alekseyshuk A., Upper Bounds of Maximum Value of Average Differential and Linear Characteristic Probabilities of Feistel Cipher with Adder Modulo 2p, // Theory of Stochastic Processes. – 2006. – Vol. 12(28). – № 1, 2. – P. 20 – 32. 6. Koval'chuk L. Verkhniye otsenki srednikh veroyatnostey differentsial'nykh approksimatsiy bulevykh otobrazheniy // Trudy Chetvyortoy Obshcherossiyskoy nauchnoy Konferentsii "Matematika i bezopasnost' informatsionnykh tekhnologiy" (MaBIT-05), 2-3 noyabrya 2005. – S.163-167. 7. Koval'chuk L. Obobshchyonyye markovskiye shifry: otsenka prakticheskoy stoykosti k metodu differentsial'nogo kriptoanaliza // Trudy Pyatoy Obshcherossiyskoy nauchnoy Konferentsii "Matematika i bezopasnost' informatsionnykh tekhnologiy" – (MaBIT-06), 25-27 oktyabrya 2006. – S. 595-599. 8. Oleksiychuk A. N., Koval'chuk L. V., Pal'chenko S. V. Kriptografichni parametri vuzliv zamini, shcho kharakterizuyut' stiykist' GOST-podibnikh blokovikh shifriv vidnosno metodiv liniynogo ta riznitsevogo kriptoanalizu // Zakhist informatsiï. – 2007. – № 2. – S. 12 – 23 9. Alekseychuk A., Koval'chuk L., Shevtsov A., Skrypnik L. Otsenki prakticheskoy stoykosti blochnogo shifra «Kalina» otnositel'no raznostnogo, lineynogo bilineynogo metodov kriptoanaliza. // Trudy Sed'moy Obshcherossiyskoy nauchnoy Konferentsii "Matematika i bezopasnost' informatsionnykh tekhnologiy" – (MaBIT-08), 30 oktyabrya – 2 noyabrya 2008. – S. 15-20. 10. A. Alekseychuk, L. Koval'chuk., YE. Skrynnik, A. Shevtsov. Otsenki prakticheskoy stoykosti blochnogo shifra «Kalina» otnositel'no metodov raznostnogo, lineynogo kriptoanaliza i algebraicheskikh atak, osnovannykh na gomomorfizmakh. // Prikladnaya radioelektronika. – №1. – 2008. – S. 203–210. 11. X. Wang, H. Yu. How to Break MD5 and Other Hash Functions. // Advances in Cryptology EUROCRYPT'05, Lectures Notes in Computer Science 3494, Springer-Verlag, 2005, P. 19-35. 12. S. Cotini, R.L. Riverst, M.J.B. Robshaw, Y. Lisa Yin. Security of the RC6TM Block Cipher, http//www.rsasecurity.com/rsalabs/rc6/. 13. Tomas A.Berson Differential cryptanalysis mod with applications to MD5 // Advanced in Cryptology. – CRYPTO'98 (LNCS 372). – 1999. – P. 95-103. 14. Koval'chuk L. Postroyeniye verkhnikh otsenok srednikh veroyatnostey tselochislennykh differentsialov kompozitsii klyuchevogo summatora, bloka podstanovki i operatora sdviga. //«Kibernetika i sistemnyy analiz» – 2010, – №6, C. 89 – 96. 15. Koval'chuk L., Kuchinskaya N. Postroyeniye verkhnikh otsenok srednikh veroyatnostey tselochislennykh differentsialov raundovykh funktsiy blochnykh shifrov opredelennoy struktury. //«Kibernetika i sistemnyy analiz» – 2012, – №5, C. 71 – 81. 16. Kuchinskaya N. V. Postroyeniye verkhnikh otsenok srednikh veroyatnostey tselochislennykh differentsialov kompozitsii klyuchevogo summatora, bloka podstanovki i proizvol'nogo operatora tsiklicheskogo sdviga. // Zbirnik naukovikh prats' «Spetsial'ni telekomunikatsiyni sistemi ta zakhist informatsiï» – 2013, – №1 (23),

С. 18 – 24. 17. Kuchinskaya N. V., Skrypnik L. V. Postroyeniye verkhnikh otsenok srednikh veroyatnostey tselochislennykh raundovykh funktsiy opredelyonnoy struktury. // Zbirnik naukovikh prats' «Spetsial'ni telekomunikatsiyni sistemi ta zakhist informatsiï» – 2013, – №2 (24), С. 27 – 33. 18. Koval'chuk L., Kuchins'ka N., Bezditniy V. Pobudova verkhnikh otsinok serednikh imovirnostey tsilochisel'nikh diferentsialiv kompozitsiï modul'nogo klyuchovogo sumatora, bloku pidstanovki ta liniynogo operatora, shcho maє blokovu strukturu. // Naukovo-tekhnichniy zbirnik «Pravove, normativne ta metrologichne zabezpechennya sistemi zakhistu informatsiï v Ukraïni» – 2014, – №28, С.47 – 52.

УДК: 004.056.5

ПІДВИЩЕННЯ СТІЙКОСТІ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ВЕКТОРНИХ ЗОБРАЖЕННЯХ ДО АТАКИ ВИЯВЛЕННЯ МІСЦЯ ЇХ РОЗТАШУВАННЯ

Василь Карпінець, Юрій Яремчук
Вінницький національний технічний університет

Стаття: ***6 стор. 7 джерел.***

На сьогодні все більш актуальним стає вирішення проблеми захисту авторських прав векторних зображень. Для цього використовуються стеганографічні методи вбудовування цифрових водяних знаків (ЦВЗ), що дають змогу маркувати об’єкти захисту для подальшого виявлення неправомірного використання зображення.

Однак, внаслідок вбудовування ЦВЗ в деяких випадках максимальне відхилення точок досягає великих значень, яке може призвести до помітних спотворень окремих точок, що може бути неприпустимим для деяких зображень та додатків, що їх використовують.

В роботі запропоновано новий підхід до вбудовування ЦВЗ у частотну область векторних зображень на основі дискретного косинусного перетворення, що дозволяє зменшити максимальні відхилення координат точок до 20% порівняно з існуючим методом. Таке вдосконалення дозволяє зменшити вплив вбудовування ЦВЗ на візуальну якість векторних зображень, а також покращити статистичні характеристики зображення. Це забезпечує підвищення стійкості ЦВЗ до статистичних атак, спрямованих на виявлення місця їх розташування.

ПОВЫШЕНИЕ УСТОЙЧИВОСТИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ВЕКТОРНЫХ ИЗОБРАЖЕНИЯХ К АТАКЕ ОБНАРУЖЕНИЯ МЕСТА ИХ РАСПОЛОЖЕНИЯ

Василий Карпинец, Юрий Яремчук
Винницкий национальный технический университет

На сегодня все более актуальным становится решение проблемы защиты авторских прав векторных изображений. Для этого используются стеганографические методы встраивания цифровых водяных знаков (ЦВЗ), позволяющие маркировать объекты защиты для дальнейшего выявления неправомерного использования изображения.

Однако, вследствие встраивания ЦВЗ в некоторых случаях максимальное отклонение точек достигает больших значений, которое может привести к заметным искажениям отдельных точек, что может быть недопустимым для некоторых изображений и приложений, которые их используют.

В работе предложен новый подход к встраиванию ЦВЗ в частотную область векторных изображений на основе дискретного косинусного преобразования, что позволяет уменьшить максимальные отклонения координат точек до 20% по сравнению с существующим методом. Такое совершенствование позволяет уменьшить влияние встраивания ЦВЗ на визуальное качество векторных изображений, а также улучшить статистические характеристики изображения. Это обеспечивает повышение устойчивости ЦВЗ к статистическим атакам, направленных на выявление места их расположения.

INCREASING STABILITY OF DIGITAL WATERMARKS INTO VECTOR IMAGES TO DETECTION LOCATION ATTACK

Vasyl Karpinets, Yuriy Yaremchuk
Vinnitsa National Technical University

Today more urgent to solve the problem of copyright protection vector images. It uses steganographic method of embedding digital watermarks, allowing objects to mark protection to further identify misuse of images.

However, due to digital watermark embedding in some cases, the maximum deviation of points reaches high values, which could lead to significant distortions of some points that may be inappropriate for some images and applications that use them.

The paper presents a new approach to embedding digital watermarks in the frequency domain vector graphics based on the discrete cosine transform, which reduces the maximum deviation of the coordinate points to 20% compared with the existing method. Such improvements can reduce the effect of embedding watermark in visual quality vector images and improve the statistical characteristics of the image. This provides increased stability watermark to statistical attacks aimed at identifying their locations.

Spisok vikoristanoï literaturi: 1. V. O. Khoroshko, O. D. Azarov, M. Є. Shelest, Yu. Є. Yaremchuk. Osnovi komp'yuternoï steganografiï. Navchal'niy posibnik. – Vinnitsya: VDTU. – 2003. – 143 s. 2. Liangbin Zheng, Yulu Jia, Qun Wang. Research on Vector Map Digital Watermarking Technology // First International Workshop on Education Technology and Computer Science – 2009. – P. 303-307. 3. M. Voigt, B. Yang and C. Busch. Reversible watermarking of 2D vector data // ACM Mutimedia and Security Workshop. – 2004, – P. 160-165. 4. Karpinets' V. V., Yaremchuk Yu. Є. Virishennya problemi pogirshennya yakosti vektornikh zobrazhen' pri vbudovuvanni tsifrovikh vodyanikh znakiv // Pravove, normativne, ta metrologichne zabezpechennya sistemi zakhistu informatsiï v Ukraïni – 2010. – № 1(20). – S.73-83. 5. Karpinets' V. V., Yaremchuk Yu. Є. Analiz vplivu tsifrovikh vodyanikh znakiv na yakist' vektornikh zobrazhen' // Suchasniy zakhist informatsiï. – 2011. – №1. – S.72-82. 6. Karpinets' V. V., Yaremchuk Yu. Є. Zmenshennya vidkhilen' koordinat tochok vnaslidok vbudovuvannya tsifrovikh vodyanikh znakiv u vektorni zobrazhennya // Pravove, normativne, ta metrologichne zabezpechennya sistemi zakhistu informatsiï v Ukraïni – 2010. – № 2(21). – S.101-109. 7. Yaremchuk Yu. Є., Karpinets' V. V. Analiz stiykosti steganografichnogo peretvorennya do vbudovuvannya tsifrovikh vodyanikh znakiv u zobrazhennya // Informatsiyni tekhnologiï ta komp'yuterna inzheneriya.- 2007. - №1(8).- S. 212-217.

УДК 004.77

МОДЕЛЬ ЗАХИЩЕНОЇ СИСТЕМИ ПЕРЕДАЧІ ДАНИХ POS ТЕРМІНАЛЬНОГО ТРАФІКУ

Максим Шаповал
НТУУ «КПІ», ФТІ

Стаття : ***7 стор., 6 джерел***

Проаналізувавши існуючі способи захисту даних, що передаються між POS терміналом та процесинговим центром, можна зробити висновок, що всі ці методи не гарантують повної безпеки процесу обміну даними між POS-терміналами та Банком, а саме:

- забезпечення доступності і надійності каналів зв'язку між Хостом та POS-терміналами;
- двобічна авторизація (Хосту та POS-терміналів).

Для безпеки передачі даних найбільш істотною вимогою є двостороння автентифікація терміналу і хостового сервера. Для вирішення данного питання необхідно використовувати сертифікати достовірності. Проте постає питання обсуговування, адже кількість POS-терміналів може бути величезною. Існують два варіанти:

1) використання єдиного сертифікату для всіх POS-терміналів;

2) використання унікального сертифікату для кожного з POS-терміналів.

Недоліки першого способу полягають у тому, що при компрометації одного сертифікату (котрий встановлюється на POS-термінали) дані зі всіх POS-терміналів можуть бути скомпровентовані.

Отже необхідно зосередитися на унікальному сертифікаті для кожного терміналу та визначити наступні компоненти системи захищеної мережі POS-терміналів:

- комплекс POS-терміналів;
- центр цифрових-сертифікатів;
- модулі безпеки HSM;
- процесинг Банку;
- комплекс керування сертифікатами;
- рівеня захищених сокетів (SSL)-концентратор;
- сервер адміністрування POS-термінальною мережею;
- локальна обчислювальна мережа Банку;
- мережа інтернет-провайдери із наданням сервісу IP MPLS.

МОДЕЛЬ ЗАЩИЩЕННОЙ СИСТЕМЫ ПЕРЕДАЧИ ДАННЫХ POS ТЕРМИНАЛЬНОГО ТРАФИКА

Максим Шаповал
НТУУ «КПИ», ФТИ

Проанализировав существующие способы защиты данных, передаваемых между POS терминалом и процессинговым центром, можно сделать вывод, что все эти методы не гарантируют полной безопасности процесса обмена данными между POS-терминалами и Банком, а именно:

- обеспечение доступности и надежности каналов связи между Хостом и POS-терминалами;
- двусторонняя авторизация (Хоста и POS-терминалов).

Для безопасности передачи данных наиболее существенным требованием является двусторонняя аутентификация терминала и хостов сервера. Для решения данного вопроса необходимо использовать удостоверяющие сертификаты. При этом встает вопрос обсуживания, ведь количество POS-терминалов может быть огромным.

Существует два варианта решения данного вопроса:

1) использование единого сертификата для всех POS-терминалов;

2) использование уникального сертификата для каждого из POS-терминалов.

Недостатки первого способа заключаются в том, что при компрометации одного сертификата (который устанавливается на POS-терминалы) данные из всех POS-терминалов могут быть скомпрометированы. Следовательно, необходимо сосредоточиться на уникальном сертификате для каждого терминала и определить следующие компоненты системы защищенной сети POS-терминалов:

- комплекс POS-терминалов;
- центр цифровых сертификатов;
- модули безопасности HSM;
- процессинг Банка;
- комплекс управления сертификатами;
- SSL-концентратор;
- сервер администрирования POS-терминальной сетью;
- локальная вычислительная сеть Банка;
- сеть интернет-провайдера с предоставлением сервиса IP MPLS.

MODEL OF TRANSFERING POS TERMINAL TRAFFIC DATA SECURE SYSTEM

Maksym Shapoval
NTUU «KPI» PhTI

Analyzing existing methods of protection data transmittion between the POS terminal to the processing center may be done conclusion that these methods do not guarantee complete security of the exchange of data between POS-terminals and the Bank, including:

- Ensuring availability. Reliability communication channels between hosts and POS-terminals
- Two-way authentication (host and POS-terminals)

And for data safety most essential requirement is two-way authentication of terminal and the host server. To solve this issue should use certificates. But appears support question, because number of POS-terminals can be enormous.

There are two options:

1) use a single certificate for all POS-terminals;

2) using a unique certificate for each POS-terminals.

Disadvantages first method consists in the fact that when a compromised certificate (which is installed on the POS-terminals), data from all POS-terminals can be compromised

So it is necessary to focus on the unique certificate for each terminal and define the following components of the secure POS-terminals network:

- complex of POS-terminals;
- digital certificates center;
- security modules HSM;
- bank Processing;
- complex of certificate management;
- SSL-termination;
- server of POS-terminal network administration;
- bank Local Area Network;
- network ISP service provision with IP MPLS.

Spisok vikoristanoï literaturi: 1. Zbirnik naukovikh prats' "Spetsial'ni telekomunikatsiyni sistemi ta zakhist informatsiï" vipusk 2(26) 2014rik st.87-97 Shapoval M V. Porivnyal'niy analiz metodiv zakhistu danikh pos-terminal'nogo trafiku 2. Carlisle Adams Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations / Carlisle Adams, Steve Lloyd, Macmillan Technical Publishing 1999 – p. 296 3. PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) Version 3.0 is active from January 1, 2014 4. Alan G. Konheim Somputer security and cryptography / Alan G. Konheim - John Wiley & Sons, Inc., 2007 - p. 542 5. K.G. Yavlinskiy «Dinamicheskaya model' bankovskoy seti» / Kirill Grigoriyevich Yavlinskiy – 2-ye izdaniye, ispravlennoye i dopolnennoye -iz-vo DMK Fin., 2013 – 480 str.6. SOU N NBU 65.1 SUIB 1.0:2010 METODI ZAKHISTU V BANKIVS'KIY DIYAL'NOSTI SISTEMA UPRAVLINNYA INFORMATSIYNOYU BEZPEKOYU VIMOGI (ISO/IEC 27001:2005, mod)

УДК 004.056

КЛАСИФІКАЦІЯ ТА АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В КЛЮЧОВИХ СИСТЕМАХ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Юрій Васильєв

ДержНДІ Спецзв'язку

Стаття: ***5 стор., 2 джерела.***

Одним з основних аспектів проблеми забезпечення безпеки систем управління (СУ) ключовими системами інформаційної інфраструктури (КСІІ) є визначення, класифікація та аналіз можливих загроз для конкретної СУ КСІІ. Перелік найбільш актуальних загроз, оцінка їх ймовірності і модель зловмисника є базовою інформацією для побудови оптимальної системи захисту.

Аналіз загроз інформаційній безпеці СУ КСІІ дозволяє виділити складові сучасних комп'ютерних загроз – т їх джерела та сили, що їх рухають, способи і наслідки реалізації. Аналіз виключно важливий для отримання всієї необхідної інформації про інформаційні загрози, визначення потенційної величини збитку, як матеріального, так і нематеріального, і вироблення адекватних заходів протидії.

КЛАСИФИКАЦИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КЛЮЧОВЫХ СИСТЕМАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Юрий Васильев
ГосНИИ Спецсвязи

Одним из основных аспектов проблемы обеспечения безопасности систем управления (СУ) ключевыми системами информационной инфраструктуры (КСИИ) является определение, классификация и анализ возможных угроз конкретной СУ КСИИ. Перечень наиболее значимых угроз, оценка их вероятности и модель злоумышленника являются базовой информацией для построения оптимальной системы защиты.

Анализ угроз информационной безопасности СУ КСИИ позволяет выделить составляющие современных компьютерных угроз – их источники и движущие силы, способы и последствия реализации. Анализ исключительно важен для получения всей необходимой информации об информационных угрозах, определения потенциальной величины ущерба, как материального, так и нематериального, и выработки адекватных мер противодействия.

ANALYSIS OF INTERNATIONAL EXPERIENCE TO IDENTIFY KEY SYSTEMS OF INFORMATION INFRASTRUCTURE

Iurii Vasyliev
SRI for STIP

One of the key aspects of safety control systems (CS) key systems information infrastructure (KSII) is the definition, classification and analysis of potential threats to the particular CS KSII. A list of the most significant threats, assess their likelihood and model of the attacker are basic information for constructing an optimal protection.

Analysis of information security threats CS KSII allows you to select the components of modern computer threats - their sources and forces that move, methods and consequences of implementation. The analysis is extremely important to obtain all the necessary information about the information threats, determine the potential amount of damage, both tangible and intangible, and to develop appropriate countermeasures.

Spisok vikoristanoї literaturi: 1.Guide to BS 7799 risk assessment and risk management. – DISC, PD 3002, 1998 [YElektronniy resurs]. – Rezhim dostupu: www.riskserver.co.uk/bs7799. 2. Guide to BS 7799 auditing – DISC, PD 3004, 1998 [YElektronniy resurs]. – Rezhim dostupu: www.riskserver.co.uk/bs779. 3. ISO 15408 [YElektronniy resurs]. – Rezhim dostupu http://www.iso.org/iso/home/search.htm?qt=15408&sort=rel&type=simple&published=on.

УДК 621.391.82

АНАЛІЗ ЧАСТОТНИХ КРИТЕРІЇВ ВІДБОРУ НЕБЕЗПЕЧНИХ ЗАВАД ДЛЯ ЧАСТОТНИХ ПРИСВОЄНЬ РАДІОЕЛЕКТРОННИМ ЗАСОБАМ РАДІОМОВНОЇ СЛУЖБИ

Сергій Лазаренко
Навчально-науковий інститут захисту інформації Державного університету телекомунікацій

Стаття: ***8 стор., 9 джерела.***

Розглянуто поняття електромагнітної сумісності (ЕМС) радіоелектронних засобів (РЕЗ). Визначена актуальність проведення аналізу ЕМС РЕЗ радіомовної служби радіозв'язку. Зазначені етапи проведення аналізу ЕМС РЕЗ радіомовної служби радіозв'язку. Наведено принцип територіального і частотного відбору потенційних джерел завад. Надані частотні критерії для відбору потенційно небезпечних завад. Запропонована блок-схема узагальненого алгоритму розрахунків ЕМС, який використовують при здійсненні експертизи частотних присвоєнь РЕЗ радіомовної служби радіозв'язку.

АНАЛИЗ ЧАСТОТНЫХ КРИТЕРИЕВ ОТБОРА ОПАСНЫХ ПОМЕХ ДЛЯ ЧАСТОТНЫХ ПРИСВОЕНИЙ РАДИОЭЛЕКТРОННЫХ СРЕДСТВ РАДИОВЕЩАТЕЛЬНОЙ СЛУЖБЫ

Сергей Лазаренко
Учебно-научный институт защиты информации Государственного университета телекоммуникаций

Рассмотрено понятие электромагнитной совместимости (ЭМС) радиоэлектронных средств (РЭС). Определена актуальность проведения анализа ЭМС РЭС радиовещательной службы радиосвязи. Отмечены этапы проведения анализа ЭМС РЭС радиовещательной службы радиосвязи. Приведен принцип территориального и частотного отбора потенциальных источников помех. Приведены частотные критерии для отбора потенциально небезопасных помех. Предложена блок-схема обобщенного алгоритма расчета ЭМС, который используется при проведении экспертизы частотных присвоений РЭС радиовещательной службы радиосвязи.

ANALYSIS FREQUENCY SELECTION CRITERIA FOR HAZARDOUS NOISE FREQUENCY ASSIGNMENTS OF ELECTRONIC MEANS BROADCASTING SERVICE

Sergey Lazarenko
Educational and Research Institute of information security of the State University of Telecommunications

There were analised the concept of electromagnetic compatibility (EMC) of radio electronic devices (RED). Determined the relevance of the analysis of EMC RED of radio broadcasting service. Defined the stages of the analysis of EMC RED of radio broadcasting service. Shows the principle of territorial and frequency selection of potential sources of interference. Given the frequency criteria for the selection of potentially hazardous noise. There were proposed the block diagram of a generalized algorithm of calculations of EMC, which is used for the examination of frequency assignments RED of radio broadcasting service.

Spisok vikoristanoï literaturi: 1. Zakon Ukraïni Pro radiochastotniy resurs Ukraïni N 1770-III vid 01.06.2000 http://zakon.nau.ua/doc/?code=1770-14 2. Postanova Kabinetu Ministriv Ukraïni vid 29.07.2009 N 785 Pro zatverdzhennya Tekhnichnogo reglamentu z yelektromagnitnoï sumisnosti obladnannya. 3. Rishennya Natsional'noï radi Ukraïni z pitan' telebachennya i radiomovlennya vid 02.12.2008 № 2151 Pro zatverdzhennya Poryadku rozrobki visnovkiv shchodo yelektromagnitnoï sumisnosti radioyelektronnikh zasobiv movlennya, neobkhidnikh dlya stvorennya ta rozvitku kanaliv movlennya, merezh movlennya ta telemerezh. 4. Sedel'nikov Yu. YE. Elektromagnitnaya sovmestimost' radioelektronnykh sredstv: ucheb. posobiye/ Sedel'nikov Yu. YE. - Kazan'.: ZAO «Novoye znaniye», 2006. - 304 s. 5. Malkov, N. A. Elektromagnitnaya sovmestimost' radioelektronnykh sredstv: ucheb. posobiye / N.A. Malkov, A. P Pudovkin. - Tambov: Izd-vo Tamb. gos. tekhn. un-ta, 2007.- 88 s. 6. Bykhovskiy M. A. i dr. Upravleniye radiochastotnym spektrom i elektromagnitnaya sovmestimost' radiosistem. ucheb. posobiye/ Pod red. d.t.n., prof. Bykhovskogo M. A. – M.: Eko-Trendz, 2006. – 376 s. 7. Tekhnichna kolektsiya Schneider-Electric: vyp. 32. YEMS - Elektromagnitnaya sovmestimost', 2009, www.schneider-electric.com.ua. 8. Rekomendatsiï sektoru radiozv'yazku MSE: - MSE R BT.417 "Minimal'na napruzhenist' polya, zakhist yakoï mozhe buti neobkhidnim pri planuvanni poslug analogovogo nazemnogo televiziynogo movlennya"; - MSE R BT.470 "Standartni sistemi analogovogo telebachennya";- MSE-R BT.500 "Metodika sub'єktivnoï otsinki yakosti televiziynogo zobrazhennya". 9. GOST 29037-91 (2004) - Poryadok provedennya sertifikatsiynikh viprobuvan' na vidpovidnist' vimogam yelektromagnitnoï sumisnosti.

УДК 004.056.53:004.492.3(045)

ІНТЕГРОВАНА МОДЕЛЬ ПРЕДСТАВЛЕННЯ КРИЗОВИХ СИТУАЦІЙ ТА ФОРМАЛІЗОВАНА ПРОЦЕДУРА ПОБУДОВИ ЕТАЛОНІВ ІДЕНТИФІКУЮЧИХ ПАРАМЕТРІВ

Микола Карпінський, Анна Корченко*, Андрій Гізун*

*Університет Бєльсько-Бяла – Техніко-гуманітарна академія (м. Бєльсько-Бяла, Польща), *Національний авіаційний університет*

Стаття: ***9 стор, 13 джерел.***

Концепція управління безперервністю бізнесу передбачає процеси виявлення та усунення переривань діяльності інформаційних систем та інших бізнес-процесів в межах різноманітних установ, підприємств та організацій. Одним з важливих напрямів реалізації цієї концепції є захист інформаційно-комунікаційних систем та мереж від негативних впливів, що спричинені інцидентами інформаційної безпеки. Згідно з міжнародними стандартами перериванням може бути будь-який інцидент. Залежно від його складності або критичності згідно з принципом доцільності визначається адекватний набір засобів та заходів реагування. Найбільш критичні інциденти прийнято називати кризовими ситуаціями, однак на сьогодні не існує їх загальноприйнятих ознак та критеріїв. Встановлено, що деякі інциденти за умов відсутності контролю можуть набувати ознак, характерних кризовим ситуаціям. Тобто можна стверджувати, що існують причино-наслідкові зв'язки між кризовою ситуацією та інцидентом інформаційної безпеки з високим ступенем критичності, що визначається рівнем збитків, числом постраждалих та іншими характеристиками, тобто інцидентом-потенційною кризовою ситуацією. Тому розробка інтегрованої моделі представлення кризових ситуацій, що має стати базисом для створення методів та засобів їх виявлення та оцінки, є актуальною та важливою науковою задачею. В дослідженні запропонована інтегрована модель представлення кризових ситуацій, що за рахунок використання нечіткої логіки може бути використана для опису будь-якої категорії кризових ситуацій в умовах слабоформалізованого нечіткого середовища. Згідно з моделлю кризова ситуація представлена шестикомпонентним кортежем, компонентами якого є: ідентифікатор інциденту-потенційної кризової ситуації; підмножина ідентифікуючих параметрів; підмножина еталонів, описуючих значення ідентифікуючих параметрів; підмножина поточних значень нечітких ідентифікуючих параметрів; підмножини евристичних правил та рівень критичності ситуації. Кожен компонент детально охарактеризований в роботі, визначені множини ідентифікуючих параметрів та ідентифікаторів потенційних кризових ситуацій. Модель представлення кризових ситуацій шляхом узагальнення оціночних та ідентифікуючих параметрів в поєднанні з елементами нечіткої логіки та експертними підходами дозволяє будувати більш гнучкі та ефективні методи виявлення та оцінки кризових ситуацій, враховуючих можливість формування необхідних множин наборів параметрів та використання в умовах слабоформалізованого середовища. Крім того, в статті на базі методу лінгвістичних термів на основі статистичних даних запропонована формалізована процедура формування еталонів ідентифікуючих параметрів. Сформовані еталони необхідні для формування логічних правил, що дозволяють забезпечити функціонування системи виявлення та оцінки кризових ситуацій.

ИНТЕГРИРОВАННЯ МОДЕЛЬ ПРЕДСТАВЛЕНИЯ КРИЗИСНІХ СИТУАЦИЙ И ФОРМАЛИЗИРОВАННЯ ПРОЦЕДУРА ФОРМИРОВАНИЯ ЭТАЛОНОВ ИДЕНТИФИЦИРУЮЩИХ ПАРАМЕТРОВ

Николай Карпинский, Анна Корченко*, Андрей Гизун*

*Университет Бельско-Бяла – Технико-гуманитарная академия (г. Бельско-Бяла, Польша), *Национальный авиационный университет*

Концепция управления непрерывностью бизнеса предусматривает процессы выявления и устранения прерываний функционирования информационных систем и других бизнес-процессов в рамках различных учреждений, предприятий и организаций. Одним из важных направлений реализации этой концепции

является защита информационно-коммуникационных систем и сетей от негативных воздействий, вызванных инцидентами информационной безопасности. По международным стандартам прерыванием может быть любой инцидент. В зависимости от его сложности или критичности согласно принципу целесообразности определяется адекватный набор средств и мер реагирования. Наиболее критические инциденты принято называть кризисными ситуациями, однако на сегодняшний день не существует их общепринятых признаков и критериев. Установлено, что некоторые инциденты при отсутствии контроля могут приобретать признаки, характерные кризисным ситуациям. То есть можно утверждать, что существуют причинно-следственные связи между кризисной ситуацией и инцидентом информационной безопасности с высокой степенью критичности, которая определяется величиной ущерба, числом пострадавших и другими характеристиками, то есть инцидентом-потенциальной кризисной ситуацией. Поэтому разработка интегрированной модели представления кризисных ситуаций, которая должна стать базисом для создания методов и средств их обнаружения и оценки, является актуальной и важной научной задачей. В исследовании предложена интегрированная модель представления кризисных ситуаций, которая за счет использования нечеткой логики может быть применена для описания любой категории кризисных ситуаций в условиях слабоформализированой нечеткой среды. Согласно модели кризисная ситуация представлена шестикомпонентным кортежем, компонентами которого являются: идентификатор инцидента-потенциальной кризисной ситуации; подмножество идентифицирующих параметров; подмножество эталонов, описывающих значения идентифицирующих параметров; подмножество текущих значений нечетких идентифицирующих параметров; подмножества эвристических правил и уровень критичности ситуации. Каждый компонент подробно охарактеризован в работе, определены множества идентифицирующих параметров и идентификаторов потенциальных кризисных ситуаций. Модель представления кризисных ситуаций за счет обобщения оценочных и идентифицирующих параметров в сочетании с элементами нечеткой логики и экспертными подходами позволяет строить более гибкие и эффективные методы выявления и оценки кризисных ситуаций, учитывающих возможность формирования необходимых множеств наборов параметров и использования в условиях слабоформализированой среды. Кроме того, в статье на базе метода лингвистических термов на основе статистических данных предложена формализованная процедура формирования эталонов идентифицирующих параметров. Сформированные эталоны необходимы для формирования логических правил, позволяющих обеспечить функционирование системы выявления и оценки кризисных ситуаций.

INTEGRATED MODEL FOR CRISES PRESENTATION AND FORMALIZED PROCEDURES FOR IDENTIFYING PARAMETERS BUILDING

Mykolaj Karpinski, Anna Korchenko*, Andrii Gizun*

*University of Bielsko-Biala – Akademia Techniczno-Humanistyczna (Bielsko-Biala, Poland), *National Aviation University*

The concept of business continuity management involves the process of identification and elimination of interrupt information systems and other business processes within various institutions, enterprises and organizations. One of the important directions of this concept is to protect the information and communication systems and networks from negative influences caused by information security incidents. According to international standards any incident can be interruption. Depending on the complexity or criticality is determined according to the principle feasibility and adequate set of measures. The most critical incidents called crisis, but today there is no conventional signs and their criteria. Some incidents in the absence of monitoring can acquire features characteristic crisis. That is, it can be argued that there are cause-effect relationships between crisis management and information security incidents with a high degree of criticality, defined level of losses, the number of victims and other characteristics that incident, a potential crisis situation. Therefore, the development of an integrated model representation crisis that has become the basis for the creation of methods and means of detection and evaluation is relevant and important scientific problems. In this study integrated model representation crisis situations through the use of fuzzy logic can be used to describe any category of crisis in terms of weakly-formalized fuzzy environment was proposed. According to the model crisis presented by six component tuple: identifier of potential incident-crisis situation; subset of identifying parameters; subset of standards describing values identifying parameters; subset of fuzzy current values identifying parameters; subset of heuristic rules and the level of criticality of the situation. Each component is described in detail in the defined set of parameters and identifiers identifying potential crisis situations. Crisis representation model through synthesis and evaluation identifying parameters combined with elements of fuzzy logic and expert approach allows

you to build more flexible and effective methods for the detection and evaluation of crisis, given the possibility of forming sets of sets necessary parameters and use in weakly-formalized environment. In addition, the paper based on the method of linguistic terms based on statistics was offered a formalized procedure for forming standards identifying parameters. Standards necessary for the formation of logical rules that allow the system identification and evaluation of crisis were formed.

Spisok vikoristanoї literaturi: 1. Korchenko A. G. Integrirovannoye predstavleniye parametrov riska / Korchenko A. G., Ivanchenko YE. V., Kazmirchuk S. V. // Zashchita informatsii – 2011. – №1 (50). – S. 96-101. 2. Korchenko A. G. Sistemy analiza i otsenivaniya riskov informatsionnoy bezopasnosti / A. G. Korchenko, A. YE. Arkhipov, S. V. Kazmirchuk. – K. : Palmarium Academic Publishing, 2013. – 316 s. 3. Korchenko O.G. Postroyeniye sistem zashchity informatsii na nechetkikh mnozhestvakh [Tekst]: Teoriya i prakticheskiye resheniya / O. G. Korchenko. – K. : MK-Press, 2006. – 320 s. 4. Korchenko A. Metod viyavlennya ta identifikatsiї porushnika v informatsiyno-komunikatsiynikh sistemakh / A. Korchenko, A. Gizun, V. Volyans'ka, S. Gnatyuk // Zakhist informatsiї. – 2013. – T.15. – №4. – S. 387-393. 5. Korchenko A. O. Sistema viyavlennya ta identifikatsiї porushnika v informatsiyno-komunikatsiynikh merezhakh / A. O. Korchenko, V. V. Volyans'ka, A. I. Gizun // Bezpeka informatsiї. – 2013. – T.19. – №3. – S. 158-162. 6. Korchenko A. A. Sistema vyyavleniya anomal'nogo sostoyaniya v komp'yuternykh setyakh / A. A. Korchenko // Bezpeka informatsiї. – 2012. – № 2 (18). – S. 80-84. 7. Parametry prognozirovaniya i identifikatsii atak v informatsionno-komunikatsionnykh sistemakh / V. Azarskov, A. Gizun, A. Grekhov, S. Skvortsov // Zakhist informatsiї. – 2014. – Tom 16. – №1. – S. 89-95. 8. Gizun A. I. Osnovni parametri dlya identifikatsiї porushnika informatsiynoї bezpeki / A.I. Gizun, V. V. Volyans'ka, V. O. Rindyuk, S. O. Gnatyuk // Zakhist informatsiї. – 2013. – №1 (58). – S.66-75. 9. Stasyuk A. I. Bazovaya model' parametrov dlya postroyeniya sistem vyyavleniya atak / A. I. Stasyuk, A. A. Korchenko // Zakhist informatsiї. – 2012. – № 2 (55). – S. 47-51. 10. Korchenko A. A. Metod formirovaniya lingvisticheskikh etalonov dlya sistem vyyavleniya vtorzheniy / A. A. Korchenko // Zakhist informatsiї. – T.16, №1. – 2014. – S. 5-12. 11. Gizun A. I. Formalizovana model' pobudovi yevristichnikh pravil dlya viyavlennya intsidentiv // A.I. Gizun, V. O. Gnatyuk, O. M. Suprun / Visnik Inzhenernoї akademiї Ukraїni. – 2015. – №1. – S. 110-115. 12. Korchenko A.O. Metod otsinki rivnya kritichnosti dlya sistem upravlinnya krizovimi situatsiyami // A. O. Korchenko, V. A. Kozachok, A. I. Gizun // Zakhist informatsiї. – 2015.– T.17. – №1. – S. 86-98. 13. Korchenko A. O. Kortezhnaya model' formirovaniya nabora bazovykh komponent dlya vyyavleniya kiberatak / A.A. Korchenko // Pravove, normativne ta metrologichne zabezpechennya sistemi zakhistu informatsiї v Ukraїni. – 2014. – V.2 (28). – S. 29-36.

УДК 004.056.5

ЗАГАЛЬНА МОДЕЛЬ ЗАГРОЗ БЕЗПЕЦІ ІНФОРМАЦІЇ АСУ ТП

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

Стаття: ***5 стор, 8 джерел.***

Наразі 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. Від ступеню захищеності АСУ ТП ОКІ залежить не тільки прибуток крупних компаній (корпорацій), але й національна або регіональна безпека. Викладене робить актуальною задачею розробку та впровадження систем захисту ОКІ, в тому числі і АСУ ТП.

В статті запропонована до розгляду загальна модель загроз захисту інформації в АСУ ТП, яка враховує технічний та соціокультурний компоненти системи захисту інформації. Також, в матеріалах статті:

- узагальнено та систематизовано вимоги щодо основних складових частин систем захисту інформації на ОКІ, в тому числі і в АСУ ТП;
- показано, що значний вплив на інформаційну безпеку ОКІ буде мати соціокультурний аспект;
- запропонована формула розрахунку ймовірності реалізації загрози безпеці інформації в АСУ ТП з урахуванням дестабілізуючих впливів на соціокультурний компонент.

ОБЩАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ АСУ ТП

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. Таким образом, от степени защищенности АСУ ТП ОКИ зависит не только прибыль крупных компаний (корпораций), а и национальная или региональная безопасность. Изложенное делает актуальной задачу разработки и внедрения систем защиты ОКИ, в том числе и АСУ ТП.

В статье предложена к рассмотрению общая модель угроз защиты информации в АСУ ТП, которая учитывает технический и социокультурный компоненты системы защиты информации. Также в материалах статьи:

- обобщены и систематизированы требования, предъявляемые к основным составным частям систем защиты информации ОКИ, в том числе и АСУ ТП;
- показано, что существенное влияние на информационную безопасность ОКИ будет иметь социокультурный аспект;
- предложена формула расчета вероятности реализации угрозы безопасности информации в АСУ ТП с учетом дестабилизирующих влияний на социокультурный компонент.

THE GENERAL MODEL OF INFORMATION SECURITY THREATS OF THE INDUSTRIAL CONTROL SYSTEMS

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. In this way, the degree of protection ICS CIO depends not only on profit large companies (corporations), and national or regional security. Stated makes the task actual of developing and introduction of the systems of protection of CIO, including ICS.

In article proposed for consideration general model of information security threats of the ICS, which takes into account technical and sociocultural components of information protection system. Also in materials of article are:

- generalized and systematized requirements, criteria for the main constituent parts of information protection systems of CIO, including ICS;
- shown that sociocultural aspect will have significant influence on information security of CIO;
- offered formula for calculating the probability realization of the threats of security information in ICS in view of destabilizing influences on sociocultural component.

Spisok vikoristanoï literaturi: 1. Vasil'єv Yu. K. Analiz mizhnarodnogo dosvidu shchodo viznachennya klyuchovikh sistem informatsiynoï infrastrukturi / Vasil'єv Yu. K. // Pravove, normativne ta metrologichne zabezpechennya sistemi zakhistu informatsiï v Ukraïni. – 2014. – Vip. 1(27). – S. 43-47. 2. Leonenko G. P., Yudin A. Yu. Problemy obespecheniya informatsionnoy bezopasnosti sistem kriticheski vazhnoy informatsionnoy infrastruktury Ukrainy // Information Technology and Security. -2013. – Vip. 1(3). - S. 44. 3. Gonchar S. F. Metodologichni zasadi rozrobki ta vprovadzhennya sistem zakhistu informatsiï na ob'єktakh kritichnoï infrastrukturi / Gonchar S. F., Leonenko G. P., Yudin O. Yu. // Spetsial'ni telekomunikatsiyni sistemi ta zakhist informatsiï. – 2014. Vip. 1(25). – S. 158-163. 4. Gonchar S. F. Analiz ugroz i uyazvimostey industrial'nykh avtomatizirovannykh sistem upravleniya / Gonchar S. F., Leonenko G. P., Yudin A. Yu. // Pravove, normativne ta metrologichne zabezpechennya sistemi zakhistu informatsiï v Ukraïni. – 2013. – Vip. 2(26). – S. 9-14. 5. Analiz ugroz setevoy bezopasnosti [YElektronniy resurs]. – Rezhim

dostupu: http://ypn.ru/138/analysis-of-threats-to-network-security/6/. 6. Lukatskiy Aleksey. Statistika real'nykh intsidentov IB v industrial'nykh sistemakh [YElektronniy resurs]. – Rezhim dostupu: http://www.securitylab.ru/blog/personal/Business_without_danger/38672.php. 7. Gonchar S. F., Leonenko G. P., Yudin O. Yu. Sotsiokul'turniy aspekt zabezpechennya informatsiynoï bezpeki ob'єktiv kritichnoï infrastrukturi : tezi dopovidey KhX Vseukraïns'koï naukovo-praktichnoï konferentsiï «Problemi stvorennya, rozvitku ta zastosuvannya visokotekhnologichnikh sistem spetsial'nogo priznachennya», Zhitomir, – 2014. S. 195-196. 8. Lovtsov D. A., Sergeyev N. A. Upravleniye bezopasnost'yu ergasistem / Pod red.. D. A. Lovtsova, - 2-ye izd. ispr. i dop. – M.: RAU-Universitet, 2001. 224 s.

УДК 504.455.064.3:574 (262.5)

ЗАХИСТ ІНФОРМАЦІЇ В СИСТЕМАХ МОНІТОРИНГУ НАДЗВИЧАЙНИХ СИТУАЦІЙ

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

Стаття: ***5 стор., 10 джерел***

Розвиток систем моніторингу надзвичайних ситуацій дозволяє своєчасно виявляти появу негативних факторів, виявляти несприятливі тенденції розвитку подій, організовувати і завчасно проводити заходи, спрямовані на запобігання аварій і катастроф. Одним із видів подібних систем є системи моніторингу морських поховань бойових отруйних речовин. Структурний аналіз їх елементів та розв'язуваних ними завдань, порядок їх функціонування і похибки роботи дозволяють зробити висновок, що ці системи є гібридними системами з аналого-цифровою обробкою переданої інформації.

Інформація, що циркулює в системі моніторингу морських поховань бойових отруйних речовин, повинна бути захищена, щоб уникнути паніки серед населення під час виконання заходів, спрямованих на запобігання екологічних лих.

ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМАХ МОНИТОРИНГА ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Елена Азаренко, Олег Бляшенко, Михаил Дивизинюк, Валерия Ковач
Государственное учреждение «Институт геохимии окружающей среды НАН Украины»

Развитие систем мониторинга чрезвычайных ситуаций позволяет своевременно обнаруживать появление негативных факторов, выявлять неблагоприятные тенденции развития событий, организовывать и заблаговременно проводить мероприятия , направленные на предотвращение аварий и катастроф. Одним из видов подобных систем являются системы мониторинга морских захоронений боевых отравляющих веществ. Структурный анализ их элементов и решаемых ими задач, порядок их функционирования и погрешности работы позволяют сделать вывод, что эти системы являются гибридными системами с аналого-цифровой обработкой передаваемой информации.

Информация, циркулирующей в системе мониторинга морских захоронений боевых отравляющих веществ, должна быть защищена, чтобы избежать паники среди населения во время выполнения мероприятий направленных на предотвращение экологических бедствий.

INFORMATION PROTECTION IN THE MONITORING SYSTEMS OF EMERGENCIES

Elena Azarenko, Oleg Bliashenko, Mikhail Diviziniuk, Valeriia Kovach
State Institution "Institute of Environmental Geochemistry of the National Academy of Sciences of Ukraine"

The development of systems for monitoring emergency allows to detect the occurrence of negative factors, to identify adverse trends of events, organize and carry out activities in advance to prevent accidents and disasters. One type of such systems are the system of monitoring sea burial of chemical warfare agents. Structural analysis of the

elements and of their tasks, the order of operation and accuracy of the work leads to the conclusion that these systems are hybrid systems with analog-to-digital processing of the transmitted information.

Protection of information circulating in the system for monitoring marine burial of chemical warfare agents, must be protected in order to avoid panic among the population during the implementation of measures aimed at preventing environmental disasters.

Spisok ispol'zovannykh istochnikov: 1. Azarenko YE. V. Problema upravleniya ekologicheskoy bezopasnost'yu pribrezhnykh vod i puti yeye resheniya/ YE. V. Azarenko, Yu. Yu. Goncharenko, M. M. Divizinyuk // Zbirnik naukovikh prats' «Sistemi obrobki informatsiï». – Kharkiv: KHUPS im. Ivana Kozheduba, 2012. – Vip.2 (100). – S. 271 – 275. 2. Azarenko YE. V. Komp'yuternyy ekologo – ekonomicheskiy monitoring kak informatsionno – tekhnicheskoye sredstvo upravleniya ekologicheskoy bezopasnost'yu / YE. V. Azarenko, Yu. Yu. Goncharenko, M. M. Divizinyuk // Nauk.-tekhn. zhurnal «Suchasniy zakhist informatsiï». – Kiïv: DUIKT, 2012. – Spetsvipusk. – S. 53 – 56. 3. Goncharenko Yu.Yu. Iprit i osobennosti yego transformatsii // Sb. nauch. tr. MGI NAN Ukrainy «Sistemy kontrolya okruzhayushchey sredy». – Sevastopol': MGI, 2012. – Vypusk 18. – S. 25-29. 4. Azarenko YE. V. Zakonomernosti transformatsii iprita v emul'girovannoye sostoyaniye / YE. V. Azarenko, Yu. Yu. Stolyarchuk // Zbirnik naukovikh prats' «Sistemi ozbroєnnya ta viys'kova tekhnika». – Kharkiv: KHUPS im. Ivana Kozheduba, 2014. – Vip.4 (40). - S. 147-150. 5. Azarenko YE. V. Faktory opredelyayushchiye ekologicheskuyu obstanovku v rayone svala morskikh glubin severo – zapadnoy chasti Chernogo morya / YE. V. Azarenko, S. A. Chernyavskaya, Yu. Yu. Goncharenko, // Zbirnik naukovikh prats' SNUYAYEtaP. - Sevastopol': SNUYAYEtaP, 2013. – Vip. 3 (47). – S. 202 – 208. 6. Azarenko YE. V. Sistema monitoringa chrezvychaynykh situatsiy v rayonakh morskikh zakhoroneniy boyevykh otravlyayushchikh veshchestv/ YE. V. Azarenko, O. V. Blyashenko, M. M. Divizinyuk, V. YE. Kovach// Zbirnik naukovikh prats' «Modelyuvannya ta informatsiyni tekhnologiï». – Kiïv:Institut problem modelyuvannya v yenergetitsi im.. G.S. Pukhova, 2014. – Vip. 73. – S. 79 – 86. 7. Azarenko YE. V. Komp'yuternyy ekologo – ekonomicheskiy monitoring kak informatsionno – tekhnicheskoye sredstvo upravleniya ekologicheskoy bezopasnost'yu/ Nauk.-tekhnich. Zhurnal «Suchasniy zakhist informatsiï». – Kiïv: DUIKT, 2012. – Spetsvipusk. – S. 53 -56. 8. Divizinyuk M. M. Klassifikatsiya chrezvychaynykh situatsiy sotsial'nogo kharaktera/ M.M. Divizinyuk, O.V. Blyashenko,T.V. Kovalyuk// Zbirnik naukovikh prats' SNUYAYEtaP. – Sevastopol': SNUYAYEtaP, 2012.- Vip. 2(42). – S. 217 – 220. 9. Khoroshko V. A. Proyektirovaniye sistem tekhnicheskoy zashchity informatsii /V. A. Khoroshko, M. M. Divizinyuk, Yu. Yu. Goncharenko i dr. Ucheb. posobiye. – Sevastopol': SNUYAEiP, 2011. – 235 s. 10. Khoroshko V. O. Metodi keruvannya informatsiynoyu bezpekoyu /V.. Khoroshko, M. M. Divizinyuk, Yu. Yu. Goncharenko ta insh. Navch. Posibnik. – Sevastopol': SNUYAYEtaP, 2010. – 328 s.

УДК 638.235.231

ДОСЛІДЖЕННЯ ЕЛЕМЕНТА АНТЕННОЇ РЕШІТКИ ЯК ОПРОМІНЮВАЧА ПАРАБОЛІЧНОЇ АНТЕНИ ДЛЯ СТАНЦІЙ ТРОПОСФЕРНОГО ЗВЯ'ЗКУ

Андрій Паламарчук, Дмитро Вергелес, Володимир Гуменюк, Юрій Васильєв, Олег Белас*, Олег Іванько*, Сергій Мазор*

*ДержНДІ Спецзв'язку,*ІСЗЗІ НТУУ "КПІ"*

Стаття: ***11 стор., 4 джерел***

Внаслідок великого ослаблення поля при тропосферному поширенні радіохвиль та виникнення спотворень сигналів необхідно забезпечувати значну ефективно ізотропну випромінювану потужність (ЕІВП). Це можливо забезпечити шляхом збільшення коефіцієнта підсилення антени та потужності передавача.

Для отримання необхідної ЕІВП розглянуто можливість використання параболічної антени та розроблення багатоелементного опромінювача, який представляє собою решітку із двох груп лінійних симетричних вібраторів – опромінювачів. Антена з такими опромінювачами та певною кількістю малопотужних підсилювачів може забезпечити необхідну ЕІВП. Але це передбачає специфічне технічне рішення для опромінювачів.

ИССЛЕДОВАНИЕ ЭЛЕМЕНТА АНТЕННОЙ РЕШЕТКИ В КАЧЕСТВЕ ОБЛУЧАТЕЛЯ ПАРАБОЛИЧЕСКОЙ АНТЕННЫ ДЛЯ СТАНЦИЙ ТРОПОСФЕРНОЙ СВЯЗИ

Андрей Паламарчук, Дмитрий Вергелес, Владимир Гуменюк, Юрий Васильев, Олег Белас*, Олег Иванько*, Сергей Мазор*

*ГосНИИ Спецсвязи, *ИССЗИ НТУУ ”КПИ”*

Вследствие ослабления поля при тропосферном распространении радиоволн и возникновения искажений сигналов необходимо обеспечивать значительную эффективную изотропную излучаемую мощность (ЭИИМ). Это возможно обеспечить за счет увеличения коэффициента усиления антенны и мощности передатчика.

Для получения необходимой ЭИИМ, рассмотрена возможность использования параболической антенны и разработки многоэлементного облучателя, который представляет собой решетку из двух групп линейных симметричных вибраторов – облучателей. Антенна с такими облучателями и определенным количеством маломощных усилителей может обеспечить необходимую ЭИИМ. Но это предполагает специфическое техническое решение для облучателей.

RESEARCH OF ANTENNA ARRAY ELEMENTS AS IRRADIATOR PARABOLIC ANTENNA FOR THE STATION TROPOSPHERIC COMMUNICATION

Andrey Palamarchuk, Dmitriy Vergeles, Vladimir Gumenuk, Iurii Vasyliev, Oleg Belas*, Oleg Ivanko*, Sergey Mazor*

*SRI for STIP, *ISCDI NTUU ”KPI”*

Due to the weakening of the field in the tropospheric propagation and occurrence of distortion signals necessary to provide substantial effective isotropic radiated power (EIRP). This may be achieved by the antenna gain and transmit power.

To obtain the necessary EIRP, consider using a parabolic antenna and feed the development of a multi-element, which is a lattice of two groups of linear dipoles – irradiators. Antenna such irradiators and a certain number of low-power amplifier can provide the necessary EIRP. But this presupposes a specific solution for the irradiators.

Spisok vikoristanoï literaturi: 1. Gavelya N. P. i dr. Antenny. Chast' 1 / N. P. Gavelya i dr. – Leningrad, 1963. – 629s. 2. YErokhin G. A. Antenno-fidernyyeustroystva i rasprostraneniyeradiovoln / G. A. YErokhin, O. V. Chernyshev, N. D. Kozyrev, V. G. Kocherzhevskiy. – Moskva, 2004, Vypusk 2. – 491s. 3. Mazor S. Yu., Belas O. M. “Oprominyuvach liniynoï polyarizatsiï dlya parabolichnoï anteni”.– K.: VIKNU. Zbirnik naukovikh prats' Viys'kovogo institutu Kiïvs'kogo natsional'nogo universitetu im.. Tarasa Shevchenka.– Vip. 46. 2014r. – s. 6-12. 4. Sergey Mazor, Andrey Demash, Andrey Palamarchuk, Sergey Usenko, Aleksey Yudin. Nekotoryye rezul'taty natural'nykh issledovaniy maketa priyemnogo modulya stantsii troposfernoy svyazi novogo pokoleniya. - Sb. Pravove, normativne ta metrologichne zabezpechennya sistem zakhistu informatsiï v Ukraïni,- vip. 1 (27). 2014 r.

УДК 681.35

ЗАБЕЗПЕЧЕННЯ РОБОЧОГО РЕЖИМУ РАДІОЕЛЕКТРОННИХ КОМПОНЕНТІВ В МЕТОДІ ВЛАСНОГО ВИПРОМІНЮВАННЯ

Василь Кузавков

Військовий інститут телекомунікацій та інформатизації Державного університету телекомунікацій

Стаття: ***5 стор.,5 джерел***

Основою застосування методу власного випромінювання для виробів радіоелектроніки є наявність прямого зв'язку ресурсу радіоелектричних компонентів (РЕК) з їхньою температурою. Для низки компонентів (транзисторів, діодів, оксидних катодів, резисторів) існують розраховані статистичні залежності. Використання методу власного випромінювання можливе навіть на недостатньо пристосованих до діагностування зразках РЕО на місці експлуатації цих засобів. За допомогою методу виявляються елементи, що відпрацювали тривалий час і перебувають в перед відмовному стані. Заміна їх призводить до підвищення коефіцієнту готовності РЕО та зниження вартості забезпечення його життєвого циклу. Оперативність методу власного випромінювання наочно проявляється при дослідження великої кількості однотипних цифрових блоків (РЕК).

Аналіз джерел показав, що теплові поля однотипних виробів добре корельовані, а використання методу власного випромінювання в автономній автоматизованій системі діагностування дозволяє здійснювати високопродуктивну безконтактну діагностику із застосуванням комп'ютерної техніки для обробки отриманих результатів.

Діагностичний параметр в методі власного випромінювання – температура поверхні РЕК, що змінюється під дією спеціально побудованої тестової послідовності, реєструється відповідно до способу переносу теплової енергії (теплопровідність, конвекція, теплове випромінювання) і може бути представлений не лише набором числових значень, але й у вигляді двовимірних (тривимірних) термограм. Після формування набору інформативних ознак можливе застосування обчислювальної техніки та алгоритмів розпізнавання образів.

Процес локалізації несправності пов'язаний з визначенням несправного РЕК шляхом реєстрації та обробки діагностичного параметру – теплового відгуку на вхідні тестові послідовності для цього РЕК. Використання методу власного випромінювання потребує створення діагностичних моделей, що відображують зв'язок діагностичного параметру з фізико хімічними властивостями як самого РЕК, так і захисного шару, що вкриває напівпровідниковий кристал РЕК. Для побудови моделі переносу тепла від «розігрітого» кристалу на поверхню РЕК (задача нестаціонарної теплопровідності) проведено аналіз технології виготовлення та структури сучасного напівпровідникового РЕК. Метою статті є визначення часу прояву діагностичного параметру на поверхні РЕК в методі власного випромінювання для безперервного та детермінованого за часом вхідного впливу.

ОБЕСПЕЧЕНИЕ РАБОЧЕГО РЕЖИМА РАДИОЭЛЕКТРОННЫХ КОМПОНЕНТОВ В МЕТОДЕ СОБСТВЕННОГО ИЗЛУЧЕНИЯ

Василий Кузавков

Военный институт телекоммуникаций и информатизации Государственного университета телекоммуникаций

В основе применения метода собственного излучения для изделий радиоэлектроники лежит наличие прямой связи ресурса работы радиоэлектрических компонентов (РЕК) с его температурой. Для ряда компонентов (транзисторов, диодов, оксидных катодов, резисторов) существуют рассчитанные статистические зависимости. Применение метода собственного излучения возможно даже на недостаточно приспособленных для диагностирования образцах радиоэлектроники на местах их эксплуатации. С помощью указанного метода представляется возможность локализовать РЕК, которые отработали продолжительное время и находятся в предотказном состоянии, что приводит к повышению коэффициента готовности РЕО и к снижению стоимости обеспечения его жизненного цикла. Оперативность метода наглядно проявляется при исследование большого числа однотипных цифровых блоков (РЕК).

Анализ источников показал, что тепловые поля однотипных изделий хорошо коррелированы, а использование метода собственного излучения в системе диагностирования позволяет осуществлять высокопроизводительную бесконтактную диагностику с применением компьютерной техники для обработки полученных результатов.

Диагностический параметр в методе – температура поверхности РЕК, изменяется под действием специально построенной проверочной тестовой последовательности, регистрируется в соответствии со способом переноса тепловой энергии (теплопроводность, конвекция, тепловое излучение) и может быть представлен не только набором числовых значений, но и в виде двумерных (трехмерных) термограмм. После формирования набора информативных признаков возможно применение вычислительной техники и алгоритмов распознавания образов.

Процесс локализации места неисправности в цифровом блоке связан с определением неисправного компонента путем регистрации и обработки диагностического параметра – теплового отклика на входные тестовые последовательности для данного компонента. Использование метода собственного излучения невозможно без создании диагностических моделей, которые отображают связь диагностического параметра с физико-химическими свойствами не только самого РЕК, но и защитного слоя, который накрывает полупроводниковый кристалл РЕК. Для построения модели переноса тепла от "разогретого" кристалла на поверхность РЕК (задача нестационарной теплопроводности) проведен анализ технологии изготовления и структуры современного полупроводникового РЕК. Целью статьи являются определения времени проявления диагностического параметра на поверхности РЕК в методе собственного излучения для непрерывного и детерминированного по времени входного воздействия.

PROVIDING OF OPERATING CONDITION OF RADIO ELECTRONIC COMPONENTS IN METHOD OF OWN RADIATION

Vasiliy Kuzavkov

The military institute of telecommunications and informatization of the State university of telecommunications

In basis of application of method of own radiation for the wares of radio electronics lies presence of direct connection of resource of work of the REC with his temperature. For the row of components (transistors, diodes, oxide cathodes, resistors) there are the expected statistical dependences. Application of the method of own radiation is possible even on the standards of radio electronics adjusted not enough to diagnose on the places of their exploitation. With the help of this method are determined by the components that have worked for a long time and are abandoned before the state, which leads to increased availability ratio of REE and to reduce the cost of software lifecycle. The operationability of method evidently shows up at research of large number of the same type digital blocks (REC).

The analysis of sources showed that the thermal fields of the same type wares well correlated, and the use of method of own radiation in the system of diagnostics allows to carry out high-performance non contact diagnostics with the use of computer technique for treatment of the got results.

A diagnostic parameter in a method is a temperature of surface of the REC, changes under the action of the specially built verification test sequence, registers one self in accordance with the method of transfer of thermal energy (heat conductivity, convection, thermal radiation) and can be presented by not only the set of numerical values but also as two-dimensional (three-dimensional) thermograms. After forming of set of informing signs application of the computing engineering and algorithms of recognition is possible.

The process of localization of place of disrepair in a digital block is related to determination of defective component by registration and treatment of diagnostic parameter – thermal response on entrance test sequences for this component. Use of method of own radiation, it is impossible without creation of diagnostic models, that represent connection of DP with physical and chemical properties not only the REC but also protective layer that covers the semiconductor crystal of the REC.

For the construction of model of transfer of heat from a "warmed-up" crystal on the surface of the REC (task of non-stationary heat conductivity) the analysis of technology of making and structure is conducted modern semiconductor the REC. The aim of the article are determinations of time of display of diagnostic parameter on the surface of the REC in the method of own radiation for continuous and determined on by time of entrance influence.

Spisok vikoristanoï literaturi: 1. Kutateladze S. S. Teploperedacha i gidrodinamicheskoye soprotivleniye. - Spravochnoye posobiye. - M.: Energoatomizdat, 1990. 2. Vavilov V. P. Teplovyye metody kontrolya kompozitsionnykh struktur i izdeliy radioelektroniki M Radio i svyaz', 1984 162 s. 3. Kontsevoy Yu. A., Kudin V. D. Metody kontrolya tekhnologii proizvodstva poluprovodnikovykh priborov M: Energiya, 1973 140 s. 4. Danilin N. S., Baklanov O. D., Zagorovskiy Yu. I. Teoriya i metody nerazrushayushchego infrakrasnogo kontrolya radioelektronnykh skhem M Izd MO SSSR, 1974 164 s. 5. Kuzavkov V. V., Yankovs'kiy O. G., Zastosuvannya metodu vlasnogo viprominyuvannya dlya tekhnichnoï diagnostiki radioyelektronnikh blokiv. Zbirnik naukovikh prats' Odes'ka derzhavna akademiya tekhnichnogo regulyuvannya ta yakosti – O.: ODATRYA, 2014. – Vip. №9 .s.30-37. 6. Lebedev N. N., Skal'skaya I. P., Uflyand Ya. S. "Sbornik zadach po matematicheskoy fizike". M.: Gostekhteorizdat, 1955.

УДК 004.931

КОНЦЕПЦІЇ ПОБУДОВИ ГОЛОСОВИХ СИСТЕМ КОНТРОЛЮ ДОСТУПУ ДО ИНФОРМАЦІЙНИХ РЕСУРСІВ ДЛЯ РІЗНИХ УМОВ ЗАСТОСУВАННЯ

Володимир Темніков, Олена Темнікова*
Національний авіаційний університет
**Національний технічний університет України «Київський політехнічний інститут»*

Стаття: ***5 стор, 11 джерел.***

Найбільш значущими наразі завданнями, пов'язаними із забезпеченням автоматизованого контролю доступу людей до ресурсів інформаційних систем по голосу, є:

- контроль віддаленого доступу клієнтів банків та абонентів довідкових служб до інформаційних ресурсів банківських і довідкових інформаційних систем із застосуванням телефону або іншого аналогічного пристрою;
- перманентний контроль доступу операторів до інформаційних ресурсів транспортних і енергетичних ергатичних систем в процесі виконання ними своїх функціональних обов'язків.

У статті на основі аналізу особливостей умов застосування розроблені концепції побудови двох типів систем контролю доступу (СКД). Кожен з варіантів застосування СКД має свої специфічні особливості, які обумовлюють вимоги до відповідних систем.

Впровадження концепції побудови систем контролю віддаленого доступу абонентів до інформаційних ресурсів банків дозволить забезпечити значне підвищення функціональності СКД порівняно з існуючими за рахунок додаткового проведення контролю емоційного стану (ЕмС) абонента, а також ідентифікації абонентів на предмет їх відсутності в «чорних списках» і виявлення шахраїв.

Розробка концепції побудови СКД для другого варіанту їх застосування була націлена на проведення аутентифікації, контролю ЕмС та ідентифікації операторів по безперервній мові, а також контролю ступеня втоми операторів за параметрами, що характеризують стан серцево-судинної системи.

Для кожного типу СКД наведені пропозиції щодо складу та побудові підсистем і їх складових, викладені принципи функціонування модулів залежно від умов, що характеризують сферу застосування.

Поєднання різних методів та підходів до побудови підсистем СКД (методів вейвлет-перетворень, кепстрального аналізу, кластеризації та ін.), застосування штучних нейронних мереж і алгоритмів, заснованих на метриках, дозволяє створити системи контролю доступу, які мають більш високі точність і швидкодію порівняно з існуючими системами при застосуванні їх в різних конкретних умовах експлуатації.

КОНЦЕПЦИИ ПОСТРОЕНИЯ ГОЛОСОВЫХ СИСТЕМ КОНТРОЛЯ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ ДЛЯ РАЗЛИЧНЫХ УСЛОВИЙ ПРИМЕНЕНИЯ

Владимир Темников, Елена Темникова*
Национальный авиационный университет
**Национальный технический университет Украины «Киевский политехнический институт»*

Наиболее значимыми в настоящее время задачами, связанными с обеспечением автоматизированного контроля доступа людей к ресурсам информационных систем по голосу, являются:

– контроль удаленного доступа клиентов банков и абонентов справочных служб к информационным ресурсам банковских и справочных информационных систем с применением телефона или другого аналогичного устройства;
– перманентный контроль доступа операторов к информационным ресурсам транспортных и энергетических эргатических систем в процессе выполнения ими своих функциональных обязанностей.

В статье на основе анализа особенностей условий применения разработаны концепции построения двух типов систем контроля доступа (СКД). Каждый из вариантов применения СКД имеет свои специфические особенности, которые обусловливают требования к соответствующим системам.

Внедрение концепции построения систем контроля удаленного доступа абонентов к информационным ресурсам банков позволит обеспечить значительное повышение функциональности СКД по сравнению с существующими за счет дополнительного проведения контроля эмоционального состояния (ЭмС) абонента, а также идентификации абонентов на предмет их отсутствия в «черных списках» и выявления мошенников.

Разработка концепции построения СКД для второго варианта их применения была нацелена на проведение аутентификации, контроля ЭмС и идентификации операторов по непрерывной речи, а также контроль степени утомления операторов по параметрам, характеризующим состояние сердечно-сосудистой системы.

Для каждого типа СКД приведены предложения по составу и построению подсистем и составляющих их модулей, изложены принципы функционирования модулей в зависимости от условий, характеризующих область применения.

Сочетание различных методов и подходов к построению подсистем СКД (методов вейвлет-преобразований, кепстрального анализа, кластеризации и др.), применение искусственных нейронных сетей и алгоритмов, основанных на метриках, позволяет создать системы контроля доступа, имеющие более высокие точность и быстродействие по сравнению с существующими системами, при применении их в различных конкретных условиях эксплуатации.

THE CONCEPT OF BUILDING SYSTEMS OF ACCESS CONTROL TO INFORMATION RESOURCES BY VOICE FOR DIFFERENT CONDITIONS OF APPLICATION

Volodymyr Temnikov, Olena Temnikova*

National Aviation University

**National Technical University of Ukraine "Kyiv Polytechnic Institute"*

The most important tasks which currently associated with the automated control people's access to resources of information systems for voice, are:

- Control of the remote access of banks clients and inquiry services subscribers to information resources and reference information bank systems using a phone or other similar device;
- Permanent control of operators access to information resources of transport and energy ergatic systems during the execution of their duties.

On the basis of analyzing the conditions of the application are developed the concepts of building two types of access control systems (ACS). Each of the applications ACS has its own specific characteristics that determine the requirements for the respective systems.

The introduction of the concept of building control systems of remote access users to the information resources of banks will allow for a significant increase in functionality of the ACS compared to the existing ones due to the additional control of the emotional state (EmS) of a subscriber and identification of subscribers for their lack of "blacklists" and detect scams.

Development of the concept of building access control for the second version of their application was aimed at carrying out authentication, EmS control, identification of operators by continuous speech and control over the degree of fatigue of operators by the parameters that characterize the state of the cardiovascular system.

For each type of ACS presented proposals for the composition and construction of sub-systems and their constituent units, described the principles of operation of modules depending on the conditions which that characterize the area of application.

A combination of different methods and approaches to building subsystems ACS (methods of wavelet transforms, cepstrum analysis, clustering, etc.), using artificial neural networks and algorithms that based on metrics allows to create an access control system with higher accuracy and speed comparing to existing systems, for use in various specific operating conditions.

Spisok ispol'zovannoy literatury: 1. Ramishvili G. S. Avtomaticheskoye opoznavaniye govoryashchego po golosu. // M.: Radio i svyaz', 1981. – 224 s. 2. Rabiner L., Gould B. Teoriya i primeneniye tsifrovoy obrabotki signalov. // M: Mir, 1978. – 848 s. 3. Temnikov V. A., Shariy T. V., Temnikova YE. L., Konforovich I. V. Golosovaya autentifikatsiya operatorov, ispol'zuyushchikh v protsesse raboty normativno ustanovlennuyu frazeologiyu // Informatsiyna bezpeka. – 2011. – №1(5). – S.125-130. 4. Temnikov V. A., Temnikova YE. L., Konforovich I. V. Vybor parametrov sistemy autentifikatsii cheloveka po golosu // Informatsiyna bezpeka. – 2012.– №2(8). – S.151-157. 5. Donoho, D. L. De-Noising by soft-thresholding // IEEE Trans. on Inform. Theory. - Vol.41. - №3. - 1995. - P.613-627. 6. Smolentsev N.

K. Osnovy teorii veyvletov. – M.: DMK, 2005. − 303 s. 7. Temnikov V. A., Ponomarenko L. V. Metodika provedeniya shumoochistki rechevogo signala v protsesse raspoznavaniya // Vestnik Vostochnoukrainskogo natsional'nogo universiteta im. V. Dalya. - №5 (111). – Ch.1. – 2007. – S.123-127. 8. Astaf'yeva N. M. Veyvlet-analiz: osnovy teorii i primery primeneniya // Uspekhi fizicheskikh nauk. – 1996. – T.166. – №11. – S. 1145-1170. 9. Bayevskiy R. M. Analiz variabel'nosti serdechnogo ritma: istoriya i filosofiya, teoriya i praktika // Klinicheskaya informatika i telemeditsina. - 2004. – №1.- S. 54-64. 10. Kal'nish V. V., Romanenko YE. V., Samoylov V. D. Arkhitektura sistemy i razrabotka programmnykh sredstv avtomatizatsii diagnostiki psikhologicheskikh i psikhofiziologicheskikh kachestv operativno-dispetcherskogo personala. – K.: IPME, 1989. – 53 s. 11. Temnikov V. A., Temnikova YE. L. Opredeleniye psikhofiziologicheskogo sostoyaniya operatora v sisteme avtomaticheskogo vnutrismennogo monitoringa po golosu // Vestnik Vostochnoukrainskogo natsional'nogo universiteta im. V. Dalya. - №6 (136). – Ch.1. – 2009. – S.294-297.

УДК 654.924

ПІДХІД ДО ОЦІНКИ ЙМОВІРНОСТІ ВИЯВЛЕННЯ ЗАГРОЗИ ІНТЕГРОВАНОЇ СИСТЕМИ БЕЗПЕКИ

Сергій Малишкін

Санкт-Петербурзький національний дослідницький університет інформаційних технологій, механіки та оптики

Стаття: ***6 стор., 8 джерел***

У широко застосовуваних на сьогоднішній день інтегрованих системах безпеки (ІСБ) підсистеми об'єднані каналами зв'язку і мають спільні засоби збирання, обробки інформації та управління. Внаслідок інтеграції підсистем на тому чи іншому рівні можна говорити про збільшення ймовірності виявлення загроз за рахунок правильної організації взаємодії між підсистемами ІСБ. Як правило, для аналізу ефективності ІСБ в цілому необхідно знати внесок не тільки окремих підсистем, а й окремих засобів виявлення в процес виявлення загроз. Мета цієї статті – дати оцінку ймовірності виявлення загрози інтегрованою системою безпеки з урахуванням можливості підвищення ймовірності виявлення за рахунок інтеграції підсистем ІСБ.

Розглядається модель об'єкта забезпечення безпеки, обладнаного інтегрованою системою безпеки. Модель об'єкта може включати множину загроз даному об'єкту, підсистем системи безпеки і зон об'єкта. Множини можуть утворювати відповідності, що характеризують особливості конкретного об'єкта. Наприклад, множини зон і підсистем утворюють відповідності, що характеризують розміщення підсистем в різних зонах.

Аналізується окремий випадок з виявленням довільної загрози з множини загроз об'єкту в межах однієї зони виявлення з множини зон об'єкта, яка може бути обладнана засобами виявлення різних підсистем з множини підсистем. Аналізується сумарна ймовірність виявлення зазначеної довільної загрози за допомогою формули повної ймовірності.

У загальному випадку при наявності I зон на об'єкті кожна зона характеризується певною ймовірністю реалізації загрози, зумовленої характером загрози і характером прояву даної загрози в зоні. В результаті аналізу та з урахуванням сумарної ймовірності виявлення довільної загрози, отримано вираз для вектора результуючої ймовірності виявлення різних загроз на об'єкті з урахуванням ймовірностей їх реалізації. Даний вектор може служити оцінкою ефективності системи безпеки.

Також як окремий випадок розглянута загроза несанкціонованого проникнення порушника на об'єкт. Об'єкт у даному випадку характеризується множиною зон, а також множиною бар'єрів на шляху проникнення порушника. Ймовірність виявлення порушника аналізується з урахуванням маршруту проникнення, а також з урахуванням принципу своєчасного виявлення, тобто коли у сил реагування ще достатньо часу для припинення проникнення порушника.

У роботі отримані наступні результати:

1. формула розрахунку ймовірності виявлення загрози інтегрованою системою безпеки з урахуванням ймовірності її реалізації в різних зонах об'єкта;

2. вираз для розрахунку ймовірності своєчасного виявлення порушника на маршруті проникнення інтегрованою системою безпеки.

ПОДХОД К ОЦЕНКЕ ВЕРОЯТНОСТИ ОБНАРУЖЕНИЯ УГРОЗЫ ИНТЕГРИРОВАННОЙ СИСТЕМОЙ БЕЗОПАСНОСТИ

Сергей Малышкин

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

В широко применяемых на сегодняшний день интегрированных системах безопасности (ИСБ) подсистемы объединены каналами связи и имеют общие средства сбора и обработки информации и управления. Вследствие интеграции подсистем на том или ином уровне можно говорить об увеличении вероятности обнаружения угроз за счет правильной организации взаимодействия между подсистемами ИСБ. Как правило, для анализа эффективности ИСБ в целом необходимо знать вклад не только отдельных подсистем, но и отдельных средств обнаружения в процесс обнаружения угроз. Цель настоящей статьи - дать оценку вероятности обнаружения угрозы интегрированной системой безопасности с учетом возможности повышения вероятности обнаружения за счет интеграции подсистем ИСБ.

Рассматривается модель объекта обеспечения безопасности, оборудованного интегрированной системой безопасности. Модель объекта может включать множества угроз данному объекту, подсистем системы безопасности и зон объекта. Множества могут образовывать соответствия, характеризующие особенности конкретного объекта. Например, множества зон и подсистем образуют соответствие, характеризующее размещение подсистем в различных зонах.

Анализируется частный случай с обнаружением произвольной угрозы из множества угроз объекту в пределах одной зоны обнаружения из множества зон объекта, которая может быть оборудована средствами обнаружения различных подсистем из множества подсистем. Анализируется суммарная вероятность обнаружения указанной произвольной угрозы с помощью формулы полной вероятности.

В общем случае при наличии I зон на объекте каждая зона характеризуется определенной вероятностью реализации угрозы, обусловленной характером угрозы и характером проявления данной угрозы в зоне. В результате анализа и с учетом суммарной вероятности обнаружения произвольной угрозы, получено выражение для вектора результирующей вероятности обнаружения различных угроз на объекте с учетом вероятностей и реализации. Данный вектор может служить оценкой эффективности системы безопасности.

Также как частный случай отдельно рассмотрена угроза несанкционированного проникновения нарушителя на объект. Объект в данном случае характеризуется множеством зон, а также множеством барьеров на пути проникновения нарушителя. Вероятность обнаружения нарушителя анализируется с учетом маршрута проникновения, а также с учетом принципа своевременного обнаружения, т.е. когда у сил реагирования еще достаточно времени для пресечения проникновения нарушителя.

В работе получены следующие результаты:

1. формула расчета вероятности обнаружения угрозы интегрированной системой безопасности с учетом вероятности ее реализации в различных зонах объекта;
2. выражение для расчета вероятности своевременного обнаружения нарушителя на маршруте проникновения интегрированной системой безопасности.

APPROACH FOR ESTIMATION OF THREAT DETECTION PROBABILITY OF INTEGRATED SECURITY SYSTEM

Sergei Malishkin

St. Petersburg National Research University of Information Technologies, Mechanics and Optics

In the typical integrated security systems (ISS) their subsystems are interconnected by the communication channels and have join data collection and processing means. As a result of the integration of the subsystems at one or another level, we can speak about the threat detection probability is increased by correct organization of the interaction between the ISS subsystems. Generally, for the effectiveness analyze on the whole it is necessary to know a contribution both separate subsystems and the separate means of detecting to the threat detection. The object of this paper is to provide the evaluation of the threat detection probability of the ISS taking into account the detection probability is able to increase by a cooperation of the ISS subsystems.

Secure object model equipped with the ISS is considered. The object model can include a sets of the threats to the object, the ISS subsystems, and the object zones. The said sets can form a correspondence characterizing the features

of the specific object. For example, the sets of the zones and the subsystems form a correspondence which could characterize the arrangement of the subsystems in the different zones.

A particular case of detection of a arbitrary threat from the set of the threats within a detection zone from the set of the object zones, the zone could be equipped with the detection means of the different subsystems from the set of the subsystems is viewed. The total probability of said random threat with the help of the Bayes' theorem is analyzed.

Next, a common case of I object zones is examined. Each zone is characterized by a certain threat implementation probability determined by the nature of the threat and by the character of the effect of said threat within a zone. As a result of the analyze, with regard to the total probability of the random threat detection, the vector of the result probability of the different threats within the object is obtained given their implementation probabilities. Said vector can serve as an effectiveness evaluation of the security system.

A particular case of the intruder unauthorized penetration into the object is also considered. In this case the object is characterized by the set of zones as well as a set of barriers on the intruder penetration route. The intruder detection probability is analyzed with regard to the timely detection principle, e.g. when the response forces have enough time for suppression of the intruder penetration yet.

In this work the following results are obtained:

1. The formula for the threat detection probability of the ISS is obtained with regard to their implementation probability within the different object zones.

2. The formula for the intruder timely detection probability of the ISS on the penetration route is obtained.

Spisok ispol'zovannoy literatury: 1. Volkhonskiy V.V., Krupnov A. G. Osobennosti razrabotki struktury sredstv obnaruzheniya ugroz okhranyayemomu ob"yektu // Nauchno-tekhnicheskiy vestnik Sankt-Peterburgskogo gosudarstvennogo universiteta informatsionnykh tekhnologiy, mekhaniki i optiki. – 2011. – № 4(74). – S. 131-136. 2. Volkhonskiy V. V., Vorob'yev P. A. Metodika otsenki veroyatnosti obnaruzheniya nesanktsionirovannogo proniknoveniya optikoelektronnym izveshchatelem // Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki. – 2012. – № 1(77). – S. 120-123. 3. Volkhonskiy V. V. Optimizatsiya struktury i algoritmov raboty kombinirovannykh sredstv obnaruzheniya proniknoveniya narushitelya // Vestnik Voronezhskogo instituta MVD Rossii. – 2012. – № 2. – S. 91-97. 4. Volkhonskiy V. V. Kriterii vybora kontroliruyemykh sredstvami obnaruzheniya parametrov v sisteme bezopasnosti // Priborostroyeniye. – SPb.: – 2013. – № 1. – S. 8-12. 5. Volkhonskiy, V. V. Sistemy okhrannoy signalizatsii / V. V. Volkhonskiy – 2-ye izd., dop. i pererab. – SPb.: Ekopolis i kul'tura, 2005. – 204 s. 6. Volkhonskiy, V. V. Teoreticheskiye i metodologicheskiye osnovy funktsionirovaniya ustroystv i sistem obespecheniya kompleksnoy bezopasnosti ob"yektov informatizatsii [Elektronnyy resurs] / V. V. Volkhonskiy. – Rezhim dostupa: http://vak1.ed.gov.ru/common//img/uploaded/files/VolkhonskiyVV.pdf – Zagl. s ekrana. – 15.04.2014. 7. Garsia M. L. Proyektirovaniye i otsenka sistem fizicheskoy zashchity / M.L. Garsia ; per. s angl. pod red. R. G. Magauyenova. – M.: Izd-vo Mir, 2003. – 386 s. 8. Venttsel', YE. S. Teoriya veroyatnostey i yeye inzhenernyye prilozheniya: Ucheb. posobiye dlya stud. vtuzov / YE. S. Venttsel', L. A. Ovcharov. – 3-ye izd., pererab. i dop. – M.: Izdatel'skiy tsentr «Akademiya», 2003. – 464 s.