4 Реферати

УДК 004.056:519.7

МЕТОД ВИЗНАЧЕННЯ ЧАСУ НА СТВОРЕННЯ ІННОВАЦІЙНОГО ПІДПРИЄМСТВА ЯК ФАКТОРУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Лілія Нікіфорова, Юрій Яремчук, Анатолій Шиян
Вінницький національний технічний університет

Стаття: ***4 стор, 9 джерел.***

Інноваційне підприємство утворюється, як правило, в результаті колективної діяльності. Тому наявність широкого інформаційно-комунікативного простору при його створенні є обов'язковою умовою. Комунікація між людьми, особливо коли необхідно прийняти рішення про їх допуск до ноу хау, триває досить довго. В статті запропоновано новий метод визначення часу на створення інноваційного підприємства, який враховує необхідність створення команди для супроводу інновації, що дозволило зв'язати відповідний час із специфічними властивостями комунікації людей для спільної діяльності. Кількість комунікантів для інвестора моделюється монотонно зростаючою випуклою вниз функцією. Враховано, що в інноваційну команду входить лише частина комунікантів. Враховано, що ефективність діяльності інноваційного підприємства має максимум при деякій кількості працівників. Виведено формули для розрахунку часу на створення інноваційного підприємства залежно від необхідної кількості працівників та ефективності комунікації. Показано, що припущення методу відповідають статистичним даним і сучасним результатам у сфері економіки та поведінки людини. Обговорено особливості використання часу на створення інноваційного підприємства в задачах інформаційної безпеки.

МЕТОД ОПРЕДЕЛЕНИЯ ВРЕМЕНИ НА СОЗДАНИЕ ИННОВАЦИОННОГО ПРЕДПРИЯТИЯ КАК ФАКТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лилия Никифорова, Юрий Яремчук, Анатолий Шиян
Винницкий национальный технический университет

Инновационное предприятие создается, как правило, в результате коллективной деятельности. Поэтому наличие обширного информационно-коммуникативного пространства при его создании является обязательным условием. Коммуникация между людьми, особенно в случае, когда необходимо принять решение об их допуске к ноу хау, требует достаточно большого времени. В статье предложен новый метод определения времени на создание инновационного предприятия, который учитывает необходимость создания команды для сопровождения инновации, что позволило связать соответствующее время со специфическими особенностями коммуникации людей с целью их совместной деятельности. Количество коммуникантов для инвестора моделируется монотонно возрастающей выпуклой вниз функцией. Учтено, что в инновационную команду входит только часть коммуникантов. Учтено, что эффективность деятельности инновационного предприятия имеет максимум при определенном количестве работников. Выведено формулы для расчета времени на создание инновационного предприятия в зависимости от необходимого количества работников и эффективности коммуникации. Показано, что предположения метода соответствуют статистическим данным и современным результатам в области экономики и поведения человека. Обсуждены особенности использования времени на создание инновационного предприятия в задачах информационной безопасности.

METHOD FOR TIME DETERMINATION AT CREATION OF INNOVATIVE ENTERPRISES AS A FACTOR OF INFORMATION SECURITY

Liliya Nikiforova, Iurii Iaremchuk, Anatoliy Shiyan
Vinnitsia national technical university

The innovative enterprise is usually created as a result of collective action. Therefore, the presence of extensive information and communication space in its creation is a prerequisite. Communication between people, especially in the case where it is necessary to make a decision about their admission to the know-how, requires a sufficiently long time. In this paper we propose a new method for determination the time for creation an innovative enterprise, which takes into account both the need to create a team to accompany innovation and allowing to associate the appropriate time with the specific features of communication people for their joint activities. The number of communicants for the investor is modeled monotonically increasing convex function. It is taken into account that in an innovative team includes only part of the communicants. It is taken into account that the effectiveness of the innovative enterprise has a maximum at a certain number of employees. The formulas for calculating the time to create an innovative enterprise, which are dependent on the required number of employees and the effectiveness of communication, are obtained. It is shown that the assumptions of the method correspond to the statistical data and recent results in the field of economics and human behavior. The characteristic features of the use of time at creation of innovative enterprise in the problems of information security are discussed.

Literatura: ***1.*** *Andreyev V.I., Kozyura V.D., Skachek L.M., Xoroshko V.O. Strategiya upravlinnya informacijnoyu bezpekoyu. – K. : DUIKT, 2007. – 277 s.* ***2.*** *Shy`yan A.A. Metody` ta texnologiyi zaxy`stu lyudy`ny` vid negaty`vnogo informacijno-psy`xologichnogo vply`vu // Informacijna bezpeka. – 2013. – №3(11). – C.98-104.* ***3.*** *Illyashenko S.M. Innovacijny`j menedzhment. – Sumy` : VTD – Universy`tets`ka kny`ga, 2010. – 334 c.* ***4.*** *Brehm S. Lundin N. University–industry linkages and absorptive capacity: an empirical analysis of China's manufacturing industry // Economics of Innovation and New Technology. – 2012. – V. 21, N. 8. – P. 837–852.* ***5.*** *Shiyan A.A., Nikiforova L.O. Why Do Inefficient Innovation Institutions Exist in Russia and Ukraine? Mechanisms for Correcting Them, // Innovation & Organizational Behavior eJournal. – 2012. – V. 1, Issue 40.– 31 p. Available at SSRN: http://ssrn.com/abstract=1981199.* ***6.*** *Acemoglu D. Introduction to Modern Economic Growth. – Princeton : Princeton University Press, 2009. – 1072 p.* ***7.*** *Jackson M. Social and Economic Networks. – Princeton : Princeton University Press, 2010. – 520 p.* ***8.*** *Mas-Collel A., Whinston M. D., Green J. R. Microeconomic Theory. – Oxford : Oxford University Press, 1995. – 977 p.* ***9.*** *Shiyan A. A. Technologies for HR-Managers: Typology for Person's Economic Behavior, Applications and Mechanism Design / A. A. Shiyan // Labor: Personnel Economics eJournal. – 2011. – V.3, N70. – 373 p. Available at SSRN: http://ssrn.com/abstract=1827706. – 373 p.*

УДК 53.087.4:534.2

РОЗРОБКА МАТЕМАТИЧНОЇ МОДЕЛІ ВИЯВЛЕННЯ ТОНАЛЬНОГО СИГНАЛУ В УМОВАХ ДОМІНУЮЧИХ ПЕРЕШКОД

Михайло Дівізінюк, Юрій Столярчук*, Олександр Фаррахов
*Державна установа «Інститут геохімії навколишнього середовища НАН України», *Севастопольський національний університет ядерної енергії та промисловості*

Стаття: ***7 стор., 5 джерел.***

Розв'язок задачі виділення корисного сигналу на тлі домінуючих перешкод в телекомунікаційних та системах радіолокації здійснюється як оптимізаційне завдання, що підвищує вірогідність їх правильного виявлення, та мінімізує вірогідність хибної тривоги. У ряді прикладних завдань, таких як пошук людей, які зазнали лихо за допомогою аварійних буїв, виявлення маркерів пеленгацій при використанні самонавідної зброї, фіксації ядерного матеріалу, замаскованого під природний фон, оптимізація роботи систем екологічного моніторингу, необхідно виділяти тональний сигнал в умовах перешкод, що багаторазово його перевищують. Математичний опис домінуючого фону є системою двох і більшого числа випадкових величин, які повністю визначаються початковими моментами першого і другого порядку, а також змішаним (кореляційним) моментом. Оскільки усі випадкові параметри, що визначають фон, не корелюються, то всі

кореляційні матриці дорівнюватимуть константам. При появі низькоінтенсивного тонального джерела значення кореляційної матриці істотно росте, причому міра цього зростання буде пропорційна числу виконаних вимірювань.

Математичною моделлю виявлення тонального сигналу в умовах домінуючих перешкод є процес вузькосмугового стробування смуги вимірів, обчислення в кожній смузі кореляційної матриці по сімейству реалізацій, подальшого порівняння розрахованої матриці з нормативною і ухвалення рішення наявності джерела випромінювання при значній розбіжності матриць.

РАЗРАБОТКА МАТЕМАТИЧСЕКОЙ МОДЕЛИ ВЫЯВЛЕНИЯ ТОНАЛЬНОГО СИГНАЛА В УСЛОВИЯХ ДОМИНИРУЮЩИХ ПОМЕХ

Михаил Дивизинюк, Юрий Столярчук*, Александр Фаррахов

*Государственное учреждение «Институт геохимии окружающей среды НАН Украины», *Севастопольский университет ядерной промышленности и энергетики*

Решение задачи выделения полезного сигнала на фоне доминирующих помех в телекоммуникационных и радиолокационных системах осуществляется как оптимизационная задача, повышающая вероятность правильного обнаружения и минимизирующая вероятность ложной тревоги. В ряде прикладных задач, таких как поиск людей, потерпевших бедствие, с помощью аварийных буев, выявление пеленгационных маркеров при использовании самонаводящегося оружия, фиксации ядерного материала, замаскированного под естественный фон, оптимизация работы систем экологического мониторинга необходимо выделять тональный сигнал в условиях многократно превышающих помех. Математическое описание доминирующего фона является системой двух и большего числа случайных величин, которые полностью определяются начальными моментами первого и второго порядка, а также смешанным (корреляционным) моментом. Поскольку все случайные параметры, определяющие фон, не коррелируются, то все корреляционные матрицы будут равны константам. При появлении низкоинтенсивного тонального источника значение корреляционной матрицы существенно растет, причем степень этого роста будет пропорциональна числу выполненных измерений.

Математической моделью выявления тонального сигнала в условиях доминирующих помех есть процесс узкополосного стробирования полосы измерений, вычисления в каждой полосе корреляционной матрицы по семейству реализаций, последующего сравнения вычисленной матрицы с нормативной и принятия решения наличия источника излучения при значительном расхождении матриц.

DEVELOPMENT OF MATHEMATICAL MODEL OF DETECTION TONE UNDER DOMINANT INTERFERENCE

Mikhail Diviziniuk, Yurij Stolerchuk*, Oleksandr Farrakhov

*State Institution «Institute of Environmental Geochemistry of the NAS of Ukraine», *Sevaltopol National University of Nuclear Energy and Industryi*

The solution of the task of signal allocation at the prevailing background noise in telecommunication and radar systems is carried out as an optimization problem, which increases the probability of correct detection and minimizes the probability of false alarm. In some application tasks such as finding people who have experienced a disaster using emergency buoys, markers identify angular position measurement using homing weapons, nuclear material fixation disguised as natural background optimization of environmental monitoring systems, it is necessary to allocate a tone around the obstacles that exceeds the mentioned in many times. The mathematical description of the dominant background is a system of two and a greater number of random variables that are completely determined by the initial moments of the first and second order and mixed (correlation) point. As far as all random parameters determining the background is not correlated, the correlation matrix equals to a constant. When the source of low tone values of the correlation matrix has been growing, and the degree of this increase is proportional to the number of performed measurements.

Mathematical model of detection tone in terms of the dominant noise gating is the process of narrowband measurements, calculate each band correlation matrix for the family implementations, further comparison of the calculated matrix and regulatory decision presence of radiation sources with significant differences

Literatura: 1. Vanshteyn L. A. Vydeleniye signalov na fone sluchaynykh pomekh / L. A. Vanshteyn, V. D. Zubakov – M.: Gosenergoizdat, 1960. – 448 s. 2. Gol'dberg L. M. Tsifrovaya obrabotka signalov. / L. M. Gol'dberg, B. D. Matyushkin, M. N. Polyak – M.: Radiosvyaz', 1990. – 256 s. 3. Beletskiy Yu. S. Metody i algoritmy kontrastnogo obnaruzheniya signalov na fone pomekh s apriori neizvestnymi kharakteristikami / Yu. S. Beletskiy – M.: Radiotekhnika, 2011. – 436 s. 4. Zashchita radiolokatsionnykh sistem ot pomekh. Sostoyaniye i tendentsii razvitiya / Pod red. V. I. Merkulova. – M.: Radiotekhnika, 2003. – 416 s. 5. Levin B. R. Teoreticheskiye osnovy statisticheskoy radiotekhniki / B. R. Levin. – M.: Radio i svyaz', 1989. – 656 s.

УДК 004.321.3:621.327.8

СИНТЕЗ ОПТИМАЛЬНОЇ ТОПОЛОГІЇ МЕРЕЖІ ПЕРЕДАЧІ ДАНИХ

Володимир Хорошко, Юлія Хохлачова, Олена Скоробогатько, Микола Тимченко
Національний авіаційний університет

Стаття: ***9 стор., 13 джерел.***

Актуальною проблемою інформатизації державних структур є вирішення задачі інформаційної безпеки та незалежності інформаційних технологій від закордонних постачальників. Мережам властиві особливі вимоги до функціонування, а також обмеження з обробки та передачі даних, що частково визначаються нормативними та керівними документами. На жаль, більшість з цих вимог досить важко, а часом і неможливо, виконати на практиці.

Як часткові характеристики інформаційних потоків (ІП), переданих абонентам мережі, можуть бути використані функції розподілу інтервалів між моментами виникнення ІП, тривалості ІП з деталізацією за категоріями терміновості і конфіденційності, умовних ймовірностей появи ІП певної категорії терміновості тощо. На етапі рішення задачі синтезу оптимальних топологічних структур мереж спеціального зв'язку (ССС) використовується експоненціальна функція розподілу інтервалів між моментами появи ВП у потоці, переданому між заданою парою абонентів, і довжин ІП з їх параметрами, на підставі яких можуть бути визначені результуюча інтенсивність потоку і параметр розподілу їх довжин і задана матриця тяжінь. Розташування абонентів ССС задається у вигляді матриці модифікованих відстаней. При синтезі топологічної структури мережі вимоги до показників якості процесів доставки ВП у МСС задаються у вигляді сукупності ймовірнісно-часових характеристик.

Забезпечення виконання вимог при фіксованій топологічній структурі МСС і в умовах безвідмовної роботи всіх її елементів здійснюється за рахунок вибору відповідної швидкодії апаратури вузлів комутації (ВК) і ліній зв'язку (ЛЗ) мережі з урахуванням використаних згідно з рекомендаціями Міжнародної організації зі стандартизації методів підвищення достовірності передачі, державних стандартів і нормативних документів, які характеризують процеси, що спотворюють ІП при передачі по МСС, режими комутації та алгоритми обміну інформацією в МСС.

Як вихідні дані використовуються параметри, усереднені за категоріями терміновості, що призводить до істотного зниження математичних труднощів в описі процесів функціонування МСС і практично не позначається на результатах рішення задачі синтезу.

Складність завдання вибору оптимальної топології МСС визначається синтезом оптимальних топологічних структур абонентських та магістральних частин мережі, виключає можливість її вирішення на основі єдиної моделі мережі, в якій на базі складних математичних залежностей описується взаємозв'язок всіх розглянутих параметрів і змінних мережі. Тому запропонована методика вирішення поставленого завдання передбачає комбінацію аналітичних методів, методів імітаційного моделювання і включає в себе вибір місць розташування регіональних вузлів комутації (РВК); синтезу топологічних структур абонентської частини МСС, тобто абонентських мереж (АМ); синтезу топологічної структури магістральної мережі (ММ) МСС.

При синтезі оптимальної структури ММ слід мінімізувати витрати на її побудову, що досягається усуненням в структурі ММ надлишкових зв'язків; необхідно також враховувати, що порушення зв'язності ММ порушує функціонування МСС в цілому як єдиної системи. Для забезпечення високої структурної надійності ММ виявляється достатнім мати між будь-якою парою РВК не менше двох незалежних шляхів передачі ІП. Таким чином, структура ММ характеризується відсутністю висячих вершин, тобто досягається введенням до її складу дуг повного графа.

Принципи побудови найкоротшої зв'язуючої мережі такі: всяка ізольована вершина мережі з'єднується з найближчим сусідом; всякий ізольований фрагмент з'єднується з найближчим найкоротшою гілкою.

Реалізовану цим методом топологічну структуру МСС можна розглядати як деяку початкову мережу, яку в подальшому необхідно удосконалити.

Проведені дослідження показали, що існує вплив числа транзитних ділянок між абонентами мережі на пропускні спроможності абонентської мережі. Причому це дуже важливо при вирішенні задачі синтезу оптимальної топологічної структури мережі. Визначено показники якості у вигляді сукупності ймовірносно-часових характеристик щодо трафіків. Аналіз результатів показав, що існує область значень параметрів переданих потоків інформаційних пакетів і вимог до показників якості процесів їх доставки, для якої визначення пропускної здатності абонентської мережі необхідно проводити з урахуванням числа транзитних ділянок між вузлами мережі відповідно до отриманих виразів.

СИНТЕЗ ОПТИМАЛЬНОЙ ТОПОЛОГИИ СЕТИ ПЕРЕДАЧИ ДАННЫХ

Владимир Хорошко, Юлия Хохлачёва, Елена Скоробогатько, Николай Тимченко
Национальный авиационный университет

Актуальной проблемой информатизации государственных структур является решение задачи информационной безопасности и независимости информационных технологий от зарубежных поставщиков. Сетям свойственны особые требования к функционированию, а также ограничения по обработке и передаче данных, частично определяющиеся нормативными и руководящими документами. К сожалению, большинство из этих требований весьма трудно, а порой и невозможно выполнить на практике.

В качестве частичных характеристик информационных потоков (ИП), передаваемых абонентам сети, могут быть использованы функции распределения интервалов между моментами возникновения ИП, длительности ИП с детализацией по категориям срочности и конфиденциальности, условные вероятности появления ИП определенной категории срочности и т. п. На этапе решения задачи синтеза оптимальных топологических структур сетей специальной связи (ССС) используется экспоненциальная функции распределения интервалов между моментами появления ИП в потоке, передаваемом между заданной парой абонентов, и длин ИП с их параметрами, на основании которых могут быть определены результирующая интенсивность потока и параметр распределения их длин и задана матрица тяготений. Расположение абонентов ССС задается в виде матрицы модифицированных расстояний. При синтезе топологической структуры сети требования к показателям качества процессов доставки ИП в ССС задаются в виде совокупности вероятностно-временных характеристик.

Обеспечение выполнения требований при фиксированной топологической структуре ССС и в условиях безотказной работы всех ее элементов осуществляется за счет выбора соответствующего быстродействия аппаратуры узлов коммутации (УК) и линий связи (ЛС) сети с учетом используемых в соответствии с рекомендациями Международной организации по стандартизации методов повышения достоверности передачи, государственных стандартов и нормативных документов, которые характеризуют процессы, искажающие ИП при передаче по ССС, режимы коммутации и алгоритмы обмена информацией в ССС.

В качестве исходных данных используются параметры, усредненные по категориям срочности, что приводит к существенному снижению математических трудностей в описании процессов функционирования ССС и практически не сказывается на результатах решения задачи синтеза.

Сложность задачи выбора оптимальной топологии ССС определяется синтезом оптимальных топологических структур абонентских и магистральных частей сети, исключает возможность ее решения на основе единой модели сети, в которой на базе сложных математических зависимостей описывается взаимосвязь всех рассматриваемых параметров и переменных сети. Поэтому предложенная методика решения поставленной задачи предполагает комбинацию аналитических методов, методов имитационного моделирования и включает в себя выбор мест расположения региональных узлов коммутации (РУК); синтеза топологических структур абонентской части ССС, т. е. абонентских сетей (АС); синтеза топологической структуры магистральной сети (МС) ССС.

При синтезе оптимальной структуры МС следует минимизировать затраты на построение МС, что достигается устранением в структуре МС избыточных связей; необходимо также учитывать, что нарушение связности МС нарушает функционирование ССС в целом как единой системы. Для обеспечения высокой структурной надежности МС оказывается достаточным иметь между любой парой РУК не менее двух независимых путей передачи ИП. Таким образом, структура МС характеризуется отсутствием висячих вершин, то есть достигается введением в ее состав дуг полного графа.

Принципы построения кратчайшей связывающей сети таковы: всякая изолированная вершина сети соединяется с ближайшим соседом; всякий изолированный фрагмент соединяется с ближайшим кратчайшей ветвью. Реализованную этим методом топологическую структуру ССС можно рассматривать как некоторую начальную сеть, которую в дальнейшем необходимо усовершенствовать.

Проведенные исследования показали, что существует влияние числа транзитных участков между абонентами сети на пропускные способности абонентской сети. Причем это очень важно при решении задачи синтеза оптимальной топологической структуры сети. Определены показатели качества в виде совокупности вероятностно-временных характеристик относительно трафиков. Анализ результатов показал, что существует область значений параметров передаваемых потоков информационных пакетов и требований к показателям качества процессов их доставки, для которых определение пропускной способности абонентской сети необходимо проводить с учетом числа транзитных участков между узлами сети в соответствии с полученными выражениями.

THE OPTIMAL TOPOLOGY DATA NETWORK

Vladimir Khoroshko, Julia Hohlachova, Elena Skorobohatko, Nikolai Timchenko

National aviation university

Urgency of the problem of developing government structures is to solve the problem of information security and information technology independence from foreign suppliers. Network special requirements inherent in the operation, as well as restrictions on the processing and transfer of data, in part determined by regulations and policies. Unfortunately, most of these requirements is difficult, and sometimes impossible to perform in practice.

As partial information flow characteristics (IF) transferred subscribers can be used distribution functions intervals since the emergence of IF, IF duration of detail by Category urgency and confidentiality conditional probability of a certain category of IF urgency so on. At the stage of solving the problem of optimal synthesis Topological special communication networks (SCN) uses exponential distribution function intervals since the advent OP in this thread sent between a given pair of subscribers and the lengths of their IF parameters for which can be determined by the intensity of the resulting flow and parameter distribution of lengths and set attraction matrix. Location subscribers CAS is set in a matrix of modified distances. In the synthesis of topological structure of the network performance requirements of the quality of the delivery of IF in MCC set as a set of probabilistic and temporal characteristics.

Ensuring compliance with a fixed topological structure of SCN and conditions uptime of all its elements is performed by selecting the appropriate equipment performance switching units (SU) and lines (LS) based network used in accordance with the recommendations of the International Organization for Standardization methods improve the reliability of transmission, national standards and regulations that characterize the processes that distort IF transmission at SCN mode switching algorithms and information exchange in SCN.

As input data used parameters, averaged by category of urgency, which leads to a significant reduction of mathematical difficulties in describing the functioning of SCN and has virtually no effect on the results of solving the problem of synthesis.

The complexity of the task of selecting the optimal topology SCN determined the optimal topological structures of main parts of the user and the network eliminates the possibility of its solution based on a single model of a network that based on complex mathematical relationships described the relationship of the considered network parameters and variables. Therefore, the proposed method of solving this problem involves a combination of analytical methods by simulation and includes a range of locations regional switching units (RSU); Topological subscription synthesis of SCN, that subscriber networks (SN); synthesis of topological structure of the backbone network (BN) SCN.

At the optimal structure BN should minimize the cost of its construction, achieved in eliminating redundant structure BN relations; and be aware that abuse connectivity BN disrupt the SCN as a whole as a single system. To ensure high structural reliability BN is sufficient to have between any pair RSU least two independent IF transmission. Thus, the structure is characterized by the absence of BN hanging vertices is achieved by introducing its constituent arcs complete graph.

Principles shortest connecting networks include every vertex isolated network connects to the closest neighbor; all isolated fragment connects to the nearest shortest branch. Marketed by this method SCN topological structure can be regarded as some of the original network, which should be improved in the future.

Studies have shown that there is influence of the number of transit sites between network subscribers for carrying capacities subscriber network. And this is very important in solving the problem of the optimal topological structure of the network. Indexes quality as a set of probabilistic and temporal characteristics on traffic. Analysis of the results showed that there is a region of parameter values transmitted packets flow of information and requirements for the

quality of the performance of delivery for which the determination subscriber network bandwidth should be carried out taking into account the number of transit sites between network nodes according to the expressions.

Literatura: 1. Kudinov V. A. Optimizatsiya struktury informatsionnoy seti / Kudinov V. A., Parkhuts' L. T., Khoroshko V. A. // Zakhist informatsiï , №3, 2004. - S.44-49. 2. Andreyev V. I. Kolichestvennaya otsenka zashchishchennosti ob"yektov s uchetom ikh funktsionirovaniya / Andreyev V. I., Kozlov V. S., Khoroshko V. A. // Zakhist informatsiï , №1, 2004. - S.26-36. 3. Ivanchenko I. S. Upravlinnya paralel'noyu obrobkoyu informatsiï / Ivanchenko I. S., Khoroshko V. O. // Suchasna spetsial'na tekhnika, № 3, 2012. - S.14-20. 4. Kleynrok L. Kommutatsionnyye seti / Kleynrok L. - M.: Nauka, 1970. – 256 s. 5. Kapustyan M. V. Analiz metodiv skladannya optimal'nikh rozkladiv roboti skladnikh sistem / Kapustyan M. V., Parkhuts' L. T., Khoroshko V. O. // Informatika ta matematichni metodi v modelyuvanni, T.2, №1, 2012. - S.46-58. 6. YEgorov F. I. Matematicheskoye modelirovaniye protsessov peredachi i obrabotki informatsii v telekommunikatsionnykh setyakh / YEgorov F. I., Skorobogat'ko YE. A., Stepanenko V. I., Khoroshko V. A. // Informatika i matematicheskiye metody v modelirovanii T.2, №3, 2012. - C.210-221. 7. Kudinov V. A. Otsenka effektivnosti algoritmov kommutatsii paketov soobshcheniy v raspredelennoy informatsionnoy seti / Kudinov V. A., Parkhuts' L. T., Plus D .V., Khoroshko V. A. // Zakhist informatsiï, Spets.vipusk, 2004. – S.36-40. 8. Mesarovich M. Obshchaya teoriya sistem: matematicheskiye osnovy / Masarovich M., Takakhara Ya. - M: Mir, 1978. – 312 s. 9. Kazakova N. F. Issledovaniye informatsionnykh potokov v kompleksnykh sistemakh zashchity informatsii i metod rascheta propusknoy sposobnosti / Kazakova N. F., Tiskina YE. O., Khoroshko V. A. // Informatsiyna bezpeka, №2, 2009. - S. 5-17. 10. YEgorov F .I. Algoritmy nakhozhdeniya optimal'noy konfiguratsii seti s zadannym chislom abonentov / YEgorov F. I., Parkhuts' L. T., Khoroshko V. A. // Visnik DUIKT, T.7, №1, 2009. - S.40-50. 11. Ivanchenko I. S. Analiz trafikov informatsionnykh resursov / Ivanchenko I. S., Khoroshko V. A. // Informatsiyna bezpeka, №1(9), 2013. - S.63-68. 12. Khoroshko V. A. Osobennosti zashchity informatsii v setyakh svyazi / Khoroshko V. A., Khokhlacheva Yu. YE. // Visnik SNU im. V. Dalya , № 15(204), Ch.1, 2013. - S.219-222. 13. Brailovskiy N. N. Formirovaniye kompleksnykh programm po zashchite ob"yektov pri nalichii ugroz i riskov / Brailovskiy N. N., Orlenko V. S., Khoroshko V. A. // Suchasniy zakhist informatsiï, № 1, 2011. - S.10-15.

УДК 004.056.53(045)

КОРТЕЖНА МОДЕЛЬ ФОРМУВАННЯ НАБОРУ БАЗОВИХ КОМПОНЕНТ ДЛЯ ВИЯВЛЕННЯ КІБЕРАТАК

Анна Корченко
Національний авіаційний університет

Стаття: ***8 стор, 8 джерел.***

Несанкціоновані дії на ресурси інформаційних систем впливають і на середовище їх оточення, породжуючи в ньому певні аномалії. Таке середовище найчастіше складноформалізоване, нечітко визначене і для вирішення завдань виявлення кібератак, що породили аномалії в цьому середовищі, необхідні відповідні засоби, які дають можливість виявити вторгнення за низкою певних характерних ознак. Один з підходів до вирішення такого роду задач ґрунтується на використанні відповідних моделей, методів і систем виявлення вторгнень, які базуються на нечітких множинах, орієнтованих на обробку слабко структурованих даних з метою встановлення фактів несанкціонованого доступу до ресурсів інформаційних систем, наприклад, через комп'ютерні мережі. Виходячи з цього, створення моделей, що дозволяють формалізувати процес виявлення кібератак шляхом контролю поточного стану параметрів середовища оточення в нечітких умовах, є актуальною науковою задачею. Досить ефективними засобами, що використовуються для вирішення таких завдань, є базова модель параметрів, універсальна модель еталонів, модель евристичних правил, метод виявлення аномалій, низки відповідних систем та інші розробки. Зазначені дослідження показали ефективність відповідного застосування математичного апарату нечітких множин, а його використання для формалізації підходу до виявлення кібератак дозволить удосконалити процес розробки відповідних систем виявлення вторгнень. Слід зазначити, що у перелічених та інших джерелах не формалізований підхід до формування необхідної низки компонент, що використовуються для контролю в нечітких умовах стану параметрів середовища оточення в заданий момент часу, за допомогою якої можна виявити аномальний стан, породжений впливом відповідного класу кібератак. З метою компенсації цього недоліку пропонується математична модель формування величин, основу якої є кортеж, що складається з ідентифікатора кібератаки, підмножин можливих параметрів і лінгвістичних еталонів, а також підмножин поточних значень нечітких параметрів і детекційних правил. Запропонована кортежна модель за рахунок формалізації процесу створення m_i-мірних підсередовищ, а також атакуючих, еталонних, поточних та

детекційних середовищ, дозволяє сформувати набір окремих кортежів, що відображають процес виявлення аномального стану в m-мірному гетерогенному параметричному середовищі, породженого відповідним атакуючим середовищем в заданий часовий проміжок. Для практичного використання запропонованої кортежної моделі при вдосконаленні систем виявлення вторгнень необхідно створити відповідну модель детекційних правил. Для контролю за станом аномальності загального гетерогенного параметричного середовища протягом усіх часових проміжків слід розробити відповідну моніторингову модель кібератак.

КОРТЕЖНАЯ МОДЕЛЬ ФОРМИРОВАНИЯ НАБОРА БАЗОВЫХ КОМПОНЕНТ ДЛЯ ВЫЯВЛЕНИЯ КИБЕРАТАК

Анна Корченко
Национальный авиационный университет

Несанкционированные воздействия на ресурсы информационных систем оказывают влияние и на среду их окружения, порождая в ней определенные аномалии. Такая среда чаще всего сложноформализуема, нечетко определенная и для решения задач выявления кибератак, породивших аномалии в этой среде, необходимы соответствующие средства, которые дают возможность обнаружить вторжение по набору определенных характерных признаков. Один из подходов к решению такого рода задач основывается на использовании соответствующих моделей, методов и систем обнаружения вторжений, которые базируются на нечетких множествах, ориентированных на обработку слабоструктурированных данных с целью установления фактов несанкционированного доступа к ресурсам информационных систем, например, через компьютерные сети. Исходя из этого, создание моделей, позволяющих формализовать процесс выявления кибератак путем контроля текущего состояния параметров среды окружения в нечетких условиях есть актуальной научной задачей. Достаточно эффективными средствами, используемыми для решения таких задач, являются базовая модель параметров, универсальная модель эталонов, модель эвристических правил, метод выявления аномалий, набор соответствующих систем и другие разработки. Указанные исследования показали эффективность соответствующего применения математического аппарата нечетких множеств, а его использование для формализации подхода к выявлению кибератак позволит усовершенствовать процесс разработки соответствующих систем обнаружения вторжений. Следует отметить, что в указанных и других источниках не формализован подход к формированию необходимого набора компонент, используемого для контроля в нечетких условиях состояния параметров среды окружения в заданный момент времени, посредством которого можно выявить аномальное состояние, порожденное воздействием соответствующего класса кибератак. С целью компенсации этого недостатка предлагается математическая модель формирования величин, основу которой составляет кортеж, состоящий из идентификатора кибератаки, подмножеств возможных параметров и лингвистических эталонов, а также подмножеств текущих значений нечетких параметров и детекционных правил. Предложенная кортежная модель за счет формализации процесса создания m_i-мерных подсред, а также атакующих, эталонных, текущих и детектирующих сред, позволяет сформировать набор частных кортежей, отображающих процесс выявления аномального состояния в m-мерной гетерогенной параметрической среде, порожденного соответствующей атакующей средой в заданный временной промежуток. Для практического использования предложенной кортежной модели при совершенствовании систем обнаружения вторжений необходимо создать соответствующую модель детекционных правил. Для контроля за состоянием аномальности общей гетерогенной параметрический среды на протяжении всех временных промежутков следует разработать соответствующую мониторинговую модель кибератак.

THE TUPEL MODEL OF BASIC COMPONENTS' SET FORMATION FOR CYBER ATTACKS

Anna Korchenko
National aviation university

The unauthorized access on information systems resourses can also have an effect on the environment of its surroundings, causing the certain anomalies. This environment is not often clearly defined, and to detect the cyber attacks that have created the anomalies in this environment, there is a need for appropriate tools that make possible to detect intrusion by a set of specific features. The approach to solving this task is based on the use of corresponding

models, methods and intrusion detection systems based on fuzzy sets focused on processing of semistructured data with a purpose to establish the facts of unauthorized access to information systems resources, for example, through computer networks. On this basis, the creation of models allowing to formalize a process of cyber attacks detection by monitoring the current status of parameters in Fuzzy environment conditions is an actual scientific challenge. Quite effective means used to address these challenges are: the basic model of parameters, the universal model of standards, model of heuristic rules, anomaly detection method, a set of the relevant systems and other development. The specified studies have shown the effectiveness of appropriate use of mathematical apparatus of fuzzy sets, and it's use to formalize an approach for cyber attacks detection, will improve the development of intrusion detection systems. It should be mentioned that in specified and other sources there is no approach formalization to build up the necessary data set component used to control in Fuzzy environment the condition of environment parameters at any given time, by which you can detect an abnormal condition caused by the effects of the relevant class of cyber-attacks. In order to compensate for this lack there is given a mathematical model of the formation of values, which is based on a tuple, consisting of cyber attacks identifier, subsets of the possible parameters and linguistic standards, as well as subsets of the current values of fuzzy parameters and detection rules. The proposed tuple model of a set of basic components, which through the formalization of the process of creating a m_i-dimensional podsred, as well as attacking, reference, current and detecting environments, allows to create a set of private tuples that display the identification of abnormal state in m-dimensional heterogeneous parametric environment generated by the corresponding attacking environment within the specified time period. For the practical use of the proposed tuple model, while improving intrusion detection systems, it is necessary to create a proper model of detection rules. To control the state of anomaly heterogeneous parametric environment during all time periods it should be developed an appropriate monitoring model of cyber attacks.

Literatura: 1. Korchenko A. A. Model' evristicheskikh pravil na logiko-lingvisticheskikh svyazkakh dlya obnaruzheniya anomaliy v komp'yuternykh sistemakh / A. A. Korchenko // Zakhist informatsiї. – 2012. – № 4 (57). – S. 112-118. 2. 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. 3. Modeli etalonov lingvisticheskikh peremennykh dlya sistem vyyavleniya atak / M. G. Lutskiy, A. A. Korchenko, A. V. Gavrilenko, A. A Okhrimenko // Zakhist informatsiї. – 2012. – № 2 (55). – S. 71-78. 4. Stasyuk A. I. Metod vyyavleniya anomaliy porozhdennykh kiberatakami v komp'yuternykh setyakh / A. I. Stasyuk, A. A. Korchenko // Zakhist informatsiї. – 2012. – №4 (57). – S. 129-134. 5. Korchenko A. A. Sistema vyyavleniya anomal'nogo sostoyaniya v komp'yuternykh setyakh / A. A. Korchenko // Bezpeka informatsiї. – 2012. – № 2 (18). – S. 80-84. 6. Korchenko A. A. Sistema formirovaniya nechetkikh etalonov setevykh parametrov / A.A. Korchenko // Zakhist informatsiї. – 2013. – T.15, №3. – S. 240-246. 7. Korchenko A. A. Sistema formirovaniya evristicheskikh pravil dlya otsenivaniya setevoy aktivnosti / A. A. Korchenko // Zakhist informatsiї. – 2013. – №4. T.15. – S. 353-359. 8. Korchenko A. G. Postroyeniye sistem zashchity informatsii na nechetkikh mnozhestvakh [Tekst]: Teoriya i prakticheskiye resheniya / A. G. Korchenko. – K. : MK-Press, 2006. – 320 s.

УДК 004.056

ОЦІНКА ЕФЕКТИВНОСТІ ЗАШУМЛЕННЯ МОВНОГО СИГНАЛУ

Олександр Архипов, Катерина Безимянна
НТУУ «КПІ»

Стаття: ***5 стор., 7 джерел***

Серед робіт, які висвітлюють активні методи захисту мовної інформації – маскування мовного сигналу перешкодою, – особливе місце займають методи, в яких використовується так звана «мовоподібна» перешкода (МПП), що забезпечує високу ефективність захисту в поєднанні з достатнім рівнем комфортності сторін, що беруть участь у мовній комунікації. У низці публікацій, що стосуються найрізноманітніших аспектів застосування МПП, розглядаються методи їх генерації, способи застосування «мовоподібних» завад у конкретних (типових) умовах, оцінюються рівні перешкод, що гарантують надійний захист мовного сигналу і т. п. Ці відомості отримані в ході проведення серій окремих досліджень, виконуваних, як правило, індивідуально, поза рамками якої-небудь загальної системної методології, тому результати, що наводяться, в цілому носять фрагментарний, уривчастий характер, залишаючи нез'ясованими ряд питань, зокрема: чи

можна дати загальне визначення МПП, як оцінювати ефективність застосування МПП, який механізм реалізації захисної дії МПП.

Детальний розгляд цих питань дозволяє константувати наступне.

Застосовуваний нині підхід до визначення поняття «мовоподібних» перешкода – в основному описово-технологічний, що спирається на фіксацію способу формування та застосування МПП в кожному конкретному випадку.

Для оцінювання ефективності застосування МПП можна використовувати артикуляційні випробування. Зазвичай їх результати представляються показниками структурного (синтаксичного) характеру, що фіксують число неправильно прийнятих елементів при одноразовому відтворенні тестового завдання (наприклад, читання слів з артикуляційних таблиць), що цілком прийнятно в задачах акустики. Однак для задач захисту інформації основний показник захищеності мовного повідомлення має відображати рівень його семантичного сприйняття аудитором (приймати при цьому до уваги можливість багаторазового відтворення записаного повідомлення, можливість його попередньої шумоочистки), що тягне принципові зміни процедури оцінювання ступеня близькості переданої та сприйнятої аудитором інформації.

Нарешті, зазвичай пропоноване пояснення механізму дії МПП тільки впливом маскування мовного сигналу перешкодою, що приводить до загрублення рівня сприйняття біологічної мовоприймальної системи, має бути доповнене ефектом «упевненого» прийому аудитором перекручених аудіообраз, що утворюються внаслідок впливу МПП при відносно низькому (у зіставленні з мовним повідомленням) рівні МПП.

ОЦЕНКА ЭФФЕКТИВНОСТИ ЗАШУМЛЕНИЯ РЕЧЕВОГО СИГНАЛА

Александр Архипов, Екатерина Безымянная
НТУУ «КПИ»

Среди работ, освещающих активные методы защиты речевой информации – маскировки речевого сигнала помехой, – особое место занимают методы, в которых используется так называемая «речеподобная» помеха (РПП), обеспечивающая высокую эффективность защиты в сочетании с достаточным уровнем комфортности сторон, участвующих в речевой коммуникации. Во множестве публикаций, касающихся самых разных аспектов применения РПП, рассматриваются методы их генерации, способы применения «речеподобных» помех в конкретных (типовых) условиях, оцениваются уровни помех, гарантирующие надежную защиту речевого сигнала и т.п. Эти сведения получены в ходе проведения серий отдельных самостоятельных исследований, выполняемых, как правило, индивидуально, вне рамок какой-либо общей системной методологии, поэтому приводимые результаты в целом носят фрагментарный, отрывочный характер, оставляя невыясненными ряд вопросов, в частности: можно ли дать общее определение РПП, как оценивать эффективность применения РПП, каков механизм реализации защитного действия РПП.

Детальное рассмотрение этих вопросов позволяет константировать следующее.

Применяемый ныне подход к определению понятия «речеподобная» помеха – в основном описательно-технологический, опирающийся на фиксацию способа формирования и применения РПП в каждом конкретном случае.

Для оценивания эффективности применения РПП можно использовать артикуляционные испытания. Обычно их результаты представляются показателями структурного (синтаксического) характера, фиксирующими число неправильно принятых элементов при однократном воспроизведении тестового задания (например, чтения слов из артикуляционных таблиц), что вполне приемлемо в задачах акустики. Однако для задач защиты информации основной показатель защищенности речевого сообщения должен отражать уровень его семантического восприятия аудитором (принимать при этом во внимание возможность многократного воспроизведения записанного сообщения, возможность его предварительной шумоочистки), что влечет принципиальные изменение процедуры оценивания степени близости переданной и воспринятой аудитором информации.

Наконец, обычно предлагаемое объяснение механизма действия РПП только влиянием маскировки речевого сигнала помехой, приводящей к загрублению уровня восприятия биологической речеприемной системы, должно быть дополнено эффектом «уверенного» приема аудитором искаженных аудиообразов, образующихся вследствие воздействия РПП при относительно низком (в сопоставлении с речевым сообщением) уровне РПП.

EVALUATION OF EFFECTIVENESS NOISY SPEECH SIGNAL

Alexander Arkhipov, Katerina Bezymyannaya
NTUU "KPI"

Among the many works covering the active methods for protecting speech information – masking speech impediment – occupy a special place methods, which use the so-called "speech-like" interference (SLI), which provides high performance protection in combination with a sufficient level of comfort of the parties involved in speech communication. In a variety of publications relating to a variety of aspects of the application of SAR, deals with methods for their generation, methods of using the "speech-like" interference in specific (standard) conditions, interference levels are evaluated to ensure protection of the speech signal, etc. This information is obtained in the course of a series of separate independent research carried out, as a rule, individually, outside the framework of any general system methodology, so given the results in general are fragmentary, sketchy, leaving a number of outstanding issues, in particular: is it possible to give a general SLI definition of how to evaluate the effectiveness of the SAR, what is the mechanism of protective action of SLI implementation.

Detailed consideration of these issues allows approve following.

Now applied approach to the definition of "speech-like" interference – mostly descriptive and Technology, based on the fixation method of forming and applying SLI in each case.

For the evaluation of the effectiveness of the SLI can be used articulation test. They are usually the results are indicators of structural (syntactic) character, fixing the number of incorrectly received elements at play once the test task (for example, reading the words of the articulation tables), which is quite acceptable in the problems of acoustics. However, problems of information security protection key indicator of verbal communication should reflect the level of semantic perception of the audience (taking into account the possibility of multiple play a recorded message, the possibility of pre-noise reduction), which implies a fundamental change in the estimation procedure and the proximity of the transmitted information perceived by the auditor.

Finally, the usual explanation of how the proposed SLI only the influence of masking speech impediment, leading to desensitization level of perception of biological speech recived system must be supplemented by the effect of "confident" reception auditor distorted audio images formed as a result of exposure to SLI at a relatively low (in comparison with a voice message) SLI level.

Literatura: 1. http://www.confident.org.ua/index.php/stati-po-teme/198-zashchita-rechevoj-informatsii.html. 2. Zheleznyak V. K., Makarov Yu. K., Khorev A. A. Nekotoryye metodicheskiye podkhody k otsenke effektivnosti zashchity rechevoy informatsii // Spetsial'naya tekhnika. – 2000. – № 4.– S. 39-45. 3. http://www.bnti.ru/showart.asp?aid=867&lvl=04.03.01. 4. Khorev A. A., Makarov Yu. K.. Metody zashchity rechevoy informatsii i otsenki ikh effektivnosti // Zashchita informatsii. Konfident. – 2001. – № 4. – S. 22-33. 5. Radzishevskiy A. Yu. Osnovy analogovogo i tsifrovogo zvuka. – M.: Izdatel'skiy dom «Vil'yams», 2006 – 288s. 6. Kovalgin Yu. A., Vologdin E. I. Tsifrovoye kodirovaniye zvukovykh signalov. – SPb.: KORONA-print, 2004. – 240 s. 7. Arkhipov A. YE., Arkhipova YE. A. Analiz i modelirovaniye rezul'tatov artikulyatsionnykh ispytaniy // Pravove, normativne ta metrologichne zabezpechennya sistemi zakhistu informatsiї v Ukraïni. Kiïv – 2010r, vipusk 1(25).- s. 21-27.

УДК 002:651.928(083.73)

АЛГОРИТМ АСИМЕТРИЧНОГО ШИФРУВАННЯ, ЗАСНОВАНИЙ НА ЕЛІПТИЧНИХ КРИВИХ

Анатолій Кочубінський, Володимир Синявський, Олександр Шаталов
Інститут кібернетики імені В. М. Глушкова НАН України

Стаття: ***7 стор, 1 джерело.***

Наразі в України як ДСТУ існує усього один криптографічний алгоритм власної розробки. Це алгоритм електронного цифрового підпису ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння». Авторами цього алгоритму є вчені Інституту кібернетики імені В. М. Глушкова НАН України.

Натомість сучасні інформаційні технології часто вимагають створення структур типу цифрових конвертів.

На цей час не існує нормативно затвердженого алгоритму асиметричного шифрування власної розробки, але криптографічне перетворення, визначене в ДСТУ 4145-2002 дає можливість розробити такий алгоритм, що матиме високу стійкість і достатню швидкодію. Такий алгоритм розроблено і саме він використовується як складова частина цифрового конверту. Стійкість цього алгоритму перевершує стійкість алгоритму ДСТУ ГОСТ 28147:2009 і тому він забезпечує адекватну криптографічну стійкість цифрового конверту в цілому. Цей алгоритм пройшов широку апробацію в прикладних розробках і має позитивні відгуки.

В даній роботі запропоновано алгоритм асиметричного шифрування даних, що ґрунтується на криптографічному перетворенні, визначеному національним стандартом України ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевіряння» [1]. Цей алгоритм призначено для направленого шифрування невеликих за обсягом даних, головним чином, ключів та інших таємних параметрів криптографічних перетворень в системах розподілу ключової інформації в незахищених каналах зв'язку, системах управління доступом до ключових даних та розподілу повноважень користувачів в таких системах.

АЛГОРИТМ АСИММЕТРИЧНОГО ШИФРОВАНИЯ, ОСНОВАННЫЙ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Анатолий Кочубинский, Владимир Синявский, Александр Шаталов
Институт кибернетики имени В. М. Глушкова НАН Украины

На сегодняшний день в Украине в качестве ДСТУ существует всего один криптографический алгоритм собственной разработки. Это алгоритм электронной цифровой подписи ДСТУ 4145-2002 «Информационные технологии. Криптографическая защита информации. Цифровая подпись, которая основывается на эллиптических кривых. Формирование и проверка». Авторами этого алгоритма являются ученые Института кибернетики имени В. М. Глушкова НАН Украины. Современные информационные технологии часто требуют создания структур типа цифровых конвертов. На данный момент не существует нормативно утвержденного алгоритма асимметричного шифрования собственной разработки, но криптографическое преобразование, определенное в ДСТУ 4145-2002 дает возможность разработать такой алгоритм, который будет иметь высокую стойкость и достаточное быстродействие. Такой алгоритм разработан и именно он используется в качестве составной части цифрового конверта. Стойкость этого алгоритма превосходит стойкость алгоритма ДСТУ ГОСТ 28147:2009 и потому он обеспечивает адекватную криптографическую стойкость цифрового конверта в целом. Этот алгоритм прошел широкую апробацию в прикладных разработках и имеет позитивные отзывы. В данной работе предложен алгоритм асимметричного шифрования данных, который основывается на криптографическом преобразовании, определенным национальным стандартом Украины ДСТУ 4145-2002 «Информационные технологии. Криптографическая защита информации. Цифровая подпись, которая основывается на эллиптических кривых. Формирование и проверка». Этот алгоритм предназначен для направленного шифрования небольших по объему данных, главным образом, ключей и других секретных параметров криптографических преобразований в системах распределения ключевой информации в незащищенных каналах связи, системах управления доступом к ключевым данным и распределению полномочий пользователей в таких системах.

ALGORITHM OF ASYMMETRIC ENCRYPTION BASED ON ELLIPTIC CURVES

Anatoly Kochubinsky, Vladimir Sinyavskiy, Alexander Shatalov
V. M. Glushkov Institute of Cybernetics of theNational Academy of Sciences of Ukraine

Nowadays in Ukraine there is the only home-made cryptographic algorithm adopted as a Ukrainian national standard. This is an algorithm of electronic digital signature defined in DSTU 4145-2002 «Information technology. Cryptographic techniques. Digital signatures based on elliptic curves. Generation and verification». The authors of this algorithm are scientists of the V. M. Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine. Modern information technologies require creation of structures like digital envelopes. Up to date there is no officially adopted home-made algorithm of asymmetric encryption. However the cryptographic transformation defined in the DSTU 4145-2002 makes it possible to develop such an algorithm. This algorithm has a high strength and sufficient performance and fits seamlessly into the PKI developed for digital signature algorithm. The strength of this algorithm exceeds the strength of symmetric encryption algorithm

DSTU GOST 28147:2009 and thus it provides an adequate cryptographic wrapping of data encryption key within a digital envelope. This algorithm has passed a wide approbation and has positive reviews. This algorithm is intended for public key encryption of small data blocks, mainly, keys and other secret parameters of cryptographic transformations in key distribution systems, key management and shared access systems.

Literatura: 1. DSTU 4145-2002 «Informatsiyni tekhnologiï. Kriptografichniy zakhist informatsiï. Tsifroviy pidpis, shcho trunturєt'sya na yeliptichnikh krivikh. Formuvannya ta pereviryannya»// K.: Derzhstandart Ukraïni, 2003. 94 s.

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, *Віктор Бездітний
*ІСЗЗІ НТУУ "КПІ", *ФТІ НТУУ "КПІ"*

Стаття: ***6 стор, 5 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 оператора, що має блокову структуру, 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, *Виктор Бездетный
*ИССЗИ НТУУ "КПИ", *ФТИ 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 оператора с блочной структурой, 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, * Viktor Bezditnyi
*ISCIS of NNUU "KPI", *IPhT of NTUU "KPI"*

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 block-structured linear 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.

Literatura: 1. 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. 2. 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. 3. 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. 4. 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), C. 18 – 24. 5. Kuchinskaya N. V., Skrypnik L. V. Postroyeniye verkhnikh otsenok srednikh veroyatnostey tselochislennykh differentsialov dlya raundovykh funktsiy opredelennoy struktury // Zbirnik naukovikh prats' «Spetsial'ni telekomunikatsiyni sistemi ta zakhist informatsiï» – 2013, – №2 (24), C. 26 – 32.

УДК 681.3.06:519.248.681

ДОСЛІДЖЕННЯ КУБІЧНИХ АТАК З МАЛИМИ СТЕПЕНЯМИ МАКСТЕРМІВ

Людмила Завадська, Віталій Сергієнко
ФТІ НТУУ «КПІ»

Стаття: ***7 стор., 6 джерел***

Кубічні атаки – один з нових перспективних методів криптоаналізу, який нині успішно застосовується до різних типів сучасних криптосистем, таких як потокові і блокові системи шифрування та хеш-функції.

Кубічні атаки є різновидом алгебраїчних атак, де кожен біт вихідної послідовності шифру інтерпретується як значення деякої булевої функції (поліному) *f*, що залежить від бітів секретного ключа та деяких відкритих змінних (бітів відкритого тексту, вектора ініціалізації тощо). Ключовими поняттями для кубічної атаки є поняття макстерму та суперполіному. Макстерм – така підмножина множини відкритих змінних функції *f*, що просумувавши виходи даної функції по всіх значеннях змінних, які входять у макстерм (по двійковому кубу), можна отримати лінійний поліном від секретних змінних. Цей поліном в такому випадку називається суперполіномом. На заключній стадії атаки розв'язується система лінійних рівнянь, отриманих на основі знайдених на попередній стадії лінійно незалежних суперполіномів. Праві частини

рівнянь системи отримуються як сума виходів функції за всіма значеннями змінних, що входять у відповідний макстерм.

Перебір макстермів (кубів) для перевірки відповідних суперполіномів на лінійність є тривалою операцією і тому потребує ефективних підходів для її здійснення. Одним із таких підходів є обмеження степеня макстермів, що беруться до розгляду. Таке обмеження можна робити як знизу, так і зверху, джерелом обмежень може виступати просто уявлення про можливий степінь функції, що описує вихід шифру, або, при більш строгому підході, знаходження степеня нелінійної функції за допомогою відповідних тестів, які, однак, є досить складними і важкими для реалізації. Тому використання макстермів невеликого степеня значно підвищило б ефективність атаки. Проте при цьому постає питання ймовірності успіху, тобто ймовірності знайти необхідну кількість лінійно незалежних суперполіномів.

У роботі розглядається питання застосовності кубічних атак за умови використання лише макстермів малого степеня і, як пеший крок у цьому напрямі, – лише макстермів першого степеня. Вводиться поняття сприятливої функції – функції, до якої можливе успішне застосування кубічної атаки з макстермами тільки першого степеня. В результаті досліджень отримано математичний вираз для кількості сприятливих функцій залежно від кількості відкритих і секретних змінних. Розраховані за цими формулами значення перевірено шляхом порівняння із результатами безпосереднього комп'ютерного перебору для невеликих значень кількості аргументів функції *f*.

Також розраховані імовірності успіху кубічної атаки з макстермами першого степеня для різних комбінацій кількостей відкритих і секретних змінних. При цьому всі булеві функції з заданою кількістю аргументів вважаються рівноймовірними, що є природним припущенням з огляду на складність функцій, які описують криптографічні системи. Звісно, за умови використання макстермів малих степенів імовірність успішної атаки є дуже малою за реальних значень кількості відкритих та секретних змінних. Проте, знаючи величину цієї імовірності, можна оцінити максимальний степінь макстермів, що забезпечує прийнятний рівень імовірності успіху кубічної атаки.

Подальший розвиток досліджень можливий у різних напрямках, пов'язаних як із розглядом більших степенів макстермів, так і узагальненням поняття суперполінома (наприклад, пошук суперполіномів другого степеня). Слід зазначити, що розглядувана задача також представляє самостійний інтерес з точки зору теорії булевих функцій та комбінаторики.

ИССЛЕДОВАНИЕ КУБИЧЕСКИХ АТАК С МАЛЫМИ СТЕПЕНЯМИ МАКСТЕРМОВ

Людмила Завадская, Виталий Сергиенко
ФТИ НТУУ «КПИ»

Кубические атаки – один из новых перспективных методов криптоанализа, ныне успешно применяемый к разным типам современных криптосистем, таким как поточные и блочные системы шифрования и хеш-функции.

Кубические атаки являются разновидностью алгебраических атак, где каждый бит выходной последовательности шифра интерпретируется как значение некоторой булевой функции (полинома) f, который зависит от битов секретного ключа и некоторых открытых переменных (битов открытого текста, вектора инициализации и т. п.). Ключевыми понятиями для кубической атаки являются понятия макстерма и суперполинома. Макстерм – такое подмножество множества открытых переменных функции f, что просуммировав выходы данной функции по всем значениям переменных, которые входят в макстерм (по двоичному «кубу»), можно получить линейный полином от секретных переменных. Этот полином в таком случае называется суперполиномом. На заключительной стадии атаки решается система линейных уравнений, полученных на основе найденных на предыдущей стадии линейно независимых суперполиномов. Правые части уравнений системы получаются как сумма выходов функции по всем значениям переменных, которые входят в соответствующий макстерм.

Перебор макстермов (кубов) для проверки соответствующих суперполиномов на линейность является длительной операцией и посему требует эффективных подходов для её выполнения. Один из таких подходов – ограничение степени рассматриваемых макстермов. Такое ограничение можно делать как снизу, так и сверху, источником ограничений может выступать просто представление о возможной степени функции, описывающей выход шифра, либо, при более строгом подходе, нахождение степени нелинейной функции с помощью соответствующих тестов, которые, однако, являются очень сложными и трудными в реализации. Поэтому использование макстермов небольшой степени значительно повысило бы эффективность атаки.

Однако при этом возникает вопрос вероятности успеха, то есть вероятности найти необходимое количество линейно независимых суперполиномов.

В работе рассматривается вопрос применимости кубических атак при условии использования только макстермов малой степени и, как первый шаг в этом направлении, – только макстермов первой степени. Вводится понятие благоприятной функции – функции, к которой возможно успешное применение кубической атаки с макстермами только первой степени. В результате исследований получено математическое выражение для количества благоприятных функций в зависимости от количества открытых и секретных переменных. Рассчитанные по этим формулам значения проверены путем сравнения с результатами непосредственного компьютерного перебора для небольших значений количества аргументов функции f.

Также были рассчитаны вероятности успеха кубической атаки с макстермами первой степени для разных комбинаций количеств открытых и секретных переменных. При этом все булевы функции с заданным количеством аргументов считались равновероятными, что является естественным допущением, учитывая сложность функций, описывающих криптографические системы. Разумеется, при условии использования макстермов малых степеней вероятность успешной атаки очень мала при реальных значениях количества открытых и секретных переменных. Однако, зная величину этой вероятности, можно оценить максимальную степень макстермов, обеспечивающую приемлемый уровень вероятности успеха кубической атаки.

Дальнейшее развитие исследований возможно в разных направлениях, связанных как с рассмотрением больших степеней макстермов, так и с обобщением понятия суперполинома (например, поиск суперполиномов второй степени). Следует отметить, что рассматриваемая задача также представляет самостоятельный интерес с точки зрения теории булевых функций и комбинаторики.

RESEARCH OF CUBE ATTACKS WITH LOW DEGREE MAXTERMS

Lyudmyla Zavadska, Vitaliy Sergienko
NTUU «KPI», PTI

Cube attack is one of new promising cryptanalysis methods, which is now successfully applied to various types of modern cryptosystems, such as stream, block ciphers and hash functions.

Cube attack is a kind of algebraic attack, where every bit of the cipher output sequence is interpreted as a value of some Boolean function (polynomial) f, that depends on bits of secret key and some public variables (bits of plaintext or initialization vector etc.). Key notions for the Cube attack are notion of maxterm and superpoly. Maxterm is such subset of the function f public variables set, that sum of f output values over all possible values of variables that belong to maxterm (over a binary "cube") can result in a linear polynomial of secret variables. This polynomial in such case is called superpoly. On the final stage of the attack, system of linear equations is solved. This system is based on the linearly independent superpolies acquired on the previous attack stage. Right parts of equations can be calculated by summing function output values over all variables presented in a corresponding maxterm.

Maxterm (cube) search for the linearity checking of corresponding superpolies is a time-consuming operation, so it requires effective implementation approach. One of such approaches is a degree limitation of maxterms under consideration. This limitation can be both upper and lower. As a limitation source, possible function degree assumption can be used. Alternatively, in more strict approach, function degree can be acquired using some appropriate tests, which are, however, more complex and hard to implement. Therefore, usage of low degree maxterms can significantly increase attack effectiveness. However, in such case a question of attack success rate can be raised, i.e. the probability of getting required quantity of linearly independent superpolies.

In this paper, we consider question of Cube attack applicability using only low degree maxterms and, as a first step, only maxterms of degree 1. We introduce a notion of auspicious function – function, to which Cube attack can be applied successfully, using maxterms of degree 1 only. As a result of our research, we acquired a mathematical expression (formula) for the number of auspicious functions. It depends on the number of public and secret variables of the function. Values calculated using this formula were verified by comparison with the results of direct computer exhaustive search for some small numbers of arguments of function f.

Additionally, success rates for the Cube attack with maxterms of degree 1 were calculated for various combinations of numbers of public and secret variables. Here all Boolean functions with specified numbers of arguments were considered equally probable, which is a natural assumption, taking into account complexity of functions representing real cryptographic systems. Of course, given that we used only low degree maxterms, attack

success rate is very low for real numbers of public and secret variables. However, knowing this probability, one can evaluate maximal degree of maxterms that provides acceptable Cube attack success rate.

Further development of our research is possible in lots of directions, related to consideration of bigger maxterm degrees, as well as to generalization of the superpoly notion (e.g. search of quadratic superpolies). It should be noted that studied problem is also of independent interest from the Boolean functions theory and combinatorics point of view.

Literatura: 1. Dinur I. Cube attacks on tweakable black box polynomials / Dinur I., Shamir A. – Cryptology ePrint Archive, 2008/385. [Online] Available at: http://eprint.iacr.org/2008/385.pdf. 2. Dinur I. Cube attacks on tweakable black box polynomials / Dinur I., Shamir A. // EUROCRYPT, vol. 5479 of Lecture Notes in Computer Science ¬ Springer, 2009. – P. 278-299. 3. Dinur I. Side Channel Cube Attacks on Block Ciphers / Dinur I., Shamir A. – Cryptology ePrint Archive, 2009/127. [Online] Available at: http://eprint.iacr.org/2009/127.pdf. 4. Aumasson J-P. Cube Testers and Key Recovery Attacks on Reduced Round MD6 and Trivium / Aumasson J-P., Meier W., Dinur I., Shamir A. // Fast Software Encryption 2009, LNCS, vol 5665 – Springer, 2009. – P. 1-22. 5. Dinur I. Cube Attacks and Cube-attack-like Cryptanalysis on the Round-reduced Keccak Sponge Function / Dinur I., Morawiecki P., Pieprzyk J., Srebrny M., Straus M. – Cryptology ePrint Archive, 2014/736. [Online] Available at: http://eprint.iacr.org/2014/736.pdf. 6. Meier W. Cube Testers and Key Recovery in Symmetric Cryptography / Meier W. – 2009. [Online] Available at: http://indocrypt09.inria.fr/slides_cube_ind09.pdf.

УДК 002:651.928(083.73)

АЛГОРИТМ ВСТАНОВЛЕННЯ СПІЛЬНОГО СЕКРЕТНОГО ЗНАЧЕННЯ, ЩО ҐРУНТУЄТЬСЯ НА ЕЛІПТИЧНИХ КРИВИХ

Анатолій Кочубінський, Володимир Синявський, Олександр Шаталов
Інститут кібернетики імені В. М. Глушкова НАН України

Стаття: ***8 стор, 5джерел.***

Конфіденційність повідомлення забезпечується шифруванням повідомлення за допомогою алгоритму шифрування даних. При великому розмірі документа таким алгоритмом може бути тільки алгоритм симетричного шифрування. Використання симетричного алгоритму шифрування пов'язано з необхідністю вирішення проблеми розподілу секретних ключів шифрування. Одним з можливих рішень є використання алгоритму асиметричного шифрування, яким шифрується разовий ключ симетричного шифрування, однак в системах передачі даних в реальному часі потрібне інше рішення, яке дозволить швидко з'єднатися з будь яким абонентом, встановити спільний секретний ключ та за певним розкладом або у разі потреби сформувати новий спільний ключ та перейти на використання нового спільного ключа. Під час встановлення спільного секретного ключа обов'язково повинна забезпечуватися автентичність сторін інформаційного обміну. Алгоритми цього типу є необхідною складовою частиною основних на цей час методів захисту трафіку в мережі Інтернет, а саме протоколів SSL/TSL та IPSec.

Найбільше поширення як алгоритм встановлення спільного секретного значення мають алгоритми, що базуються на алгоритмі Діффі-Хеллмана. В своєму стандартному вигляді цей алгоритм не забезпечує автентифікації сторін і тому не може протистояти засобам криптоаналізу, що використовують можливість порушення автентичності. Алгоритм встановлення спільного секретного значення має також гарантувати стійкість обчисленого спільного секретного значення, не меншу за стійкість симетричного алгоритму шифрування даних. Реально це можливо тільки за умови застосування криптографічних перетворень у групі точок належно обраних еліптичних кривих. З практичної точки зору важливо уніфікувати обчислювальні засоби, що використовуються для реалізації криптографічних перетворень різного типу.

В роботі пропонується алгоритм встановлення спільного секретного значення з використанням криптографічного перетворення, визначеного національним стандартом України ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, заснований на еліптичних кривих. Формування і перевіряння» та криптографічних стандартів, що діють в Україні. Цей алгоритм забезпечує автентичність сторін інформаційного обміну.

Алгоритм призначено для обчислення в режимі реального часу двома учасниками інформаційного обміну спільного секретного значення, розмір якого визначається функцією гешування, що використовується. Це секретне значення використовується для ініціалізації алгоритму симетричного шифрування але не визначає

його спосіб ініціалізації та спосіб шифрування потоку даних. Алгоритм встановлення спільного секретного значення можна використовувати для захисту даних в інформаційних системах загального призначення.

АЛГОРИТМ УСТАНОВЛЕНИЯ ОБЩЕГО СЕКРЕТНОГО ЗНАЧЕНИЯ, ОСНОВАННЫЙ НА ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Анатолий Кочубинский, Владимир Синявский, Александр Шаталов
Институт кибернетики имени В. М. Глушкова НАН Украины

Конфиденциальность сообщения обеспечивается шифрованием сообщения с помощью алгоритма шифрования данных. При большом размере документа таким алгоритмом может быть только алгоритм симметричного шифрования. Использование симметричного алгоритма шифрования связано с необходимостью решения проблемы распределения секретных ключей шифрования. Одним из возможных решений есть использование алгоритма асимметричного шифрования, которым шифруется разовый ключ симметричного шифрования, однако в системах передачи данных в реальном времени нужно другое решение, которое позволит быстро соединиться с любым абонентом, установить общий секретный ключ и по определенному расписанию или в случае необходимости сформировать новый общий ключ и перейти на использование нового общего ключа. Во время установления общего секретного ключа обязательно должна обеспечиваться подлинность сторон информационного обмена. Алгоритмы этого типа являются необходимой составной частью основных на это время методов защиты траффика в сети Интернет, а именно протоколов Ssl/tsl и Ipsec.

Наибольшее распространение как алгоритм установления общего секретного значения имеют алгоритмы, которые базируются на алгоритме Диффи-Хеллмана. В своем стандартном виде этот алгоритм не обеспечивает аутентификации сторон и потому не может противостоять средствам криптоанализа, которые используют возможность нарушения подлинности. Алгоритм установления общего секретного значения должен также гарантировать стойкость вычисленного общего секретного значения, не меньше стойкости симметричного алгоритма шифрования данных. Реально это возможно только при условии применения криптографических преобразований в группе точек должным образом выбранных эллиптических кривых. С практической точки зрения важно унифицировать вычислительные средства, которые используются для реализации криптографических преобразований разного типа.

В работе предлагается алгоритм установления общего секретного значения с использованием криптографического преобразования, определенного национальным стандартом Украины ДСТУ 4145-2002 «Информационные технологии. Криптографическая защита информации. Цифровая подпись, основанная на эллиптических кривых. Формирование и проверка», и криптографических стандартов, которые действуют в Украине. Этот алгоритм обеспечивает подлинность сторон информационного обмена.

Алгоритм предназначен для вычисления в режиме реального времени двумя участниками информационного обмена общего секретного значения, размер которого определяется используемой функцией хеширования. Это секретное значение используется для инициализации алгоритма симметричного шифрования но не определяет его способ инициализации и способ шифрования потока данных. Алгоритм установления общего секретного значения можно использовать для защиты данных в информационных системах общего назначения.

ALGORITHM OF ESTABLISHMENT OF GENERAL SECRET VALUE, BASED ON ELLIPTIC CURVES

Anatoly Kochubinsky, Vladimir Sinyavskiy , Alexander Shatalov
V. M. Glushkov Institute of Cybernetics of the National Academy of Sciences of Ukraine

To ensure confidentiality a document is usually encrypted by a symmetric key encryption algorithm. The use of a symmetric key encryption algorithm makes it necessary to distribute the used common encryption/decryption key. A possible decision is to use an asymmetric encryption algorithm to hide a session symmetric encryption key. However in many cases another decision is more appropriate consisting in the establishment of a shared secret key as needed by performing a set of cryptographic operations in a dialogue. A secure establishment of a shared secret key requires a mutual authentication of communicating parties. Algorithms of this type are basic components of network security tools including Internet protocols Ssl/tsl and Ipsec.

Most shared key establishment algorithms are based on the Diffie-Hellmann algorithm. In its original design this algorithm does not provide the authentication of parties and thus is vulnerable to cryptanalytic attacks using the violation of authenticity. The shared key establishment algorithm should also guarantee the strength exceeding that of the symmetric encryption algorithm in use. A natural approach is to design such an algorithm on cryptographic transformations in the group of points of the properly chosen elliptic curves.

The presented algorithm of shared secret key establishment is based on the cryptographic transformation defined in the national standard of Ukraine DSTU 4145-2002 «Information technology. Cryptographic techniques. Digital signatures based on elliptic curves. Generation and verification», and cryptographic standards which operate in Ukraine. This algorithm provides the mutual authenticity of information exchange parties and fits smoothly within the framework of the PKI developed for DSTU 4145 digital signature.

The algorithm is intended for a real time computation of a shared secret key by two parties of information exchange the size of which is determined the hash function in use. The computed secret key is used to initialize an algorithm of symmetric encryption.

Literatura: 1. L. Law, A. Menezes, M. Qu, J. Solinas and S. Vanstone. An efficient protocol for authenticated key agreement. //Technical report CORR 98-05, University of Waterloo,1998. 2. DSTU 4145-2002 «Informatsiyni tekhnologiï. Kriptografichniy zakhist informatsiï. Tsifroviy pidpis, shcho ґruntuєt'sya na yeliptichnikh krivikh. Formuvannya ta pereviryannya»// K.: Derzhstandart Ukraïni, 2003. 94 s. 3. Blake I., Seroussi G., Smart N. Elliptic Curves in Cryptography. Cambridge University Press, 1999. p.204. 4. U. Maurer and S. Wolf, The Diffie-Hellman protocol, //Designs, Codes and Cryptography, 19 (2000), 147-171. 5. A.Muzereau, N.P.Smart, F.Vercauteren. The Equivalence between the DHP and DLP for Elliptic Curves Used in Practical Applications. //LMS J. Comput. Math. 7 (2004), p.- 50-72.

УДК 621.391:519.2:519.7

ПОРІВНЯННЯ ОПЕРАЦІЙ МОДУЛЬНОГО ТА ПОКОМПОНЕНТНОГО ДОДАВАННЯ І ВІДНІМАННЯ НА МНОЖИНІ N-МІРНИХ ВЕКТОРІВ НАД ПРОСТИМ СКІНЧЕННИМ ПОЛЕМ

Людмила Ковальчук, Наталія Лисенко*, Сергій Красніков*
*ІСЗЗІ НТУУ «КПІ», *ДержНДІ Спецзв'язку*

Стаття: ***8 стор., 10 джерел.***

У роботі отримано результати, які характеризують імовірності збігу результатів операцій покомпонентного та модульного додавання (віднімання) на множині *n*-мірних векторів над простим скінченним полем. Показано, що імовірність збігу результатів операцій модульного та покомпонентного додавання (віднімання) тим менша, чим більшою є довжина векторів. Вона прямує до нуля з зростанням довжини векторів. Тому використання для обґрунтування стійкості такої модифікації блокового шифру, в якій модульне додавання (віднімання) замінюється на покомпонентне, є некоректним.

СРАВНЕНИЕ ОПЕРАЦИЙ МОДУЛЬНОГО И ПОКОМПОНЕНТНОГО СЛОЖЕНИЯ И ВЫЧИТАНИЯ НА МНОЖЕСТВЕ N-МЕРНЫХ ВЕКТОРОВ НАД ПРОСТЫМ КОНЕЧНЫМ ПОЛЕМ

Людмила Ковальчук, Наталия Лисенко*, Сергей Красников*
*ИССЗИ НТУУ «КПИ», *ГосНИИ Спецсвязи*

В работе получены результаты, характеризирующие вероятности совпадения результатов операций покомпонентного и модульного сложения (вычитания) на множестве *n*-мерних векторов над простым конечным полем. Показано, что вероятность совпадения результатов операций покомпонентного та модульного сложения (вычитания) тем меньше, чем длиннее вектора. Она стремится к нулю при возрастании

длины векторов. Поэтому использование для обоснования стойкости такой модификации блочного шифра, в которой модульное сложение (вычитание) заменяется на покомпонентное, является некорректным.

THE COMPARISON OF THE COMPONENT-WISE AND MODULAR ADDITION (SUBTRACTION) OF N-DIMENSIONAL VECTOR SPACE OVER A PRIME FINITE FIELD

Kovalchuk Ludmila, Lysenko Natalija*, Krasnikov Sergej*
*ISCDI NTUU «KPI», *SRI for STIP*

The results are obtained that characterize the results coincidence probability of the component-wise and modular addition (subtraction) of *N*-dimensional vector space over a prime finite field. It is shown that the results coincidence probability of the component-wise and modular addition (subtraction) decreases when the space dimension increaces. This probability tends to zero when the length of vectors increaces. So it's incorrect to use for security estimation such modification of block cipher, where modular addition (subtraction) is replaced by the component-wise.

Literatura: 1. Shennon K. Teoriya svyazi v sekretnykh sistemakh //Raboty po teorii informatsii i kibernetike. – M.: Izdatel'stvo inostrannoy literatury, 1963. – S. 333-402. 2. Gorchinskiy Yu. N. O gomomorfizmakh mnogoosnovnykh universal'nykh algebr vsvyazi s kriptograficheskimi primeneniyami // Trudy po diskretnoy matematike. T. 1. – M.: TVP, 1997. – s. 67– 84. 3. O. V. Shemyakina. O peremeshivayushchikh svoystvakh operatsiy v konechnom pole. // Trudy Vos'moy Obshcherossiyskoy nauchnoy Konferentsii «Matematika i bezopasnost' informatsionnykh tekhnologiy» – (MaBIT-09), 30 oktyabrya – 2 noyabrya 2009. 4. L. V. Koval'chuk, O. A. Sirenko. Analiz peremeshivayushchikh svoystv operatsiy modul'nogo i pobitovogo slozheniya, opredelennykh na odnom nositele. // Kibernetika i sistemnyy analiz. – 2011. – № 5. – s. 83 – 97. 5. L. V. Koval'chuk, O. A. Sirenko. Analiz peremeshivayushchikh svoystv operatsiy v konechnom kol'tse. // Sbornik tezisov KhIV Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Bezopasnost' informatsii v informatsionno-telekommunikatsionnykh sistemakh», 17-20 maya 2011, Kiyev, s. 45 – 46. 6. Koval'chuk L. V., Lysenko N. V., Skrypnyk L. V. Peremeshivayushchiye svoystva operatsiy, opredelennykh na mnozhestve N-mernykh vektorov nad prostym konechnym polem // Kibernetika i sistemnyy analiz. – 2014. – № 4. – S.135 – 145. 7. GOST 28147-89. Sistemy obrabotki informatsii. Zashchita kriptograficheskaya. Algoritm kriptograficheskogo preobrazovaniya. – M.: Gosstandart SSSR, 1989. – 28 str. 8. 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. 9. 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. 10. Galinskiy V. A. Veroyatnostnyye svoystva perenosov pri slozhenii po modulyu 2n // Obozreniye prikladnoy i promyshlennoy matematiki. 2003. T. 10, vyp. 1. s. 129 – 130.

УДК 502.3:502.36

РОЗРОБКА ОДИНИЧНОГО ЕЛЕМЕНТУ (ПОСТУ) ДЛЯ ВИМІРЮВАННЯ ПОКАЗНИКІВ АТМОСФЕРНОГО ПОВІТРЯ

Михайло Дівізінюк, Валерія Ковач
ДУ «Інститут геохімії навколишнього середовища НАН України», м. Київ

Стаття: ***5 стор., 7 джерел.***

Система моніторингу – це вимірювальна система або система перетворення інформації про фактичний стан навколишнього природного середовища в вид і в форму, які дозволяють її досить швидко передавати і обробляти. Оптимізації цього процесу сприяє впровадженню засобів цифрової обчислювальної техніки. Існуючі на сьогоднішній день вимірювальні радіаційні пристрої в своїй основі є аналоговими вимірювачами (датчиками). Транслювати аналоговий сигнал на великі відстані досить складна задача. Вона обумовлена, з одного боку, впливом безлічі перешкод на канал трансляції даних. З іншого – обробка аналогових сигналів вимагає досить габаритного і дорогого устаткування. Вирішують цю задачу так звані гібридні перетворювачі інформації.

В сучасних гібридних системах, незалежно від їх призначення, великого поширення набули аналого-цифрові канали. Для правильної організації процесу аналого-цифрового перетворення принципове значення

має питання про те, за яких умов виходять коди аналого-цифрового перетворювача, які, в свою чергу, можуть вважатися еквівалентними вхідному аналоговому сигналу.

Основним завдання системи радіоекологічного моніторингу є контроль за радіаційною та екологічною ситуацією.

Тому, виходячи з цього, в статті описано, що одиничний елемент (автоматизований пост) повинен забезпечити збір (вимірювання) первинної інформації про стан навколишнього природного середовища: в повітрі, в ґрунтах та його поверхні, в підземних водах. Передача первинних даних відбувається на головний (базовий) пост, де на основі отриманої первинної інформації формується оцінка радіаційної обстановки, аналізується поточна екологічна ситуація та прогнозується динаміка її розвитку та можливих наслідків. Крім цього, пост повинен забезпечувати безперервний радіаційній контроль, а на головному (основному) пості повинна реалізовуватися система баз даних про всі необхідні елементи навколишнього природного середовища. Пост також має забезпечувати періодичний відбір проб для їх подальшого лабораторного аналізу.

РАЗРАБОТКА ЕДИНИЧНОГО ЭЛЕМЕНТА (ПОСТА) ДЛЯ ИЗМЕРЕНИЯ ПОКАЗАТЕЛЕЙ АТМОСФЕРНОГО ВОЗДУХА

Михаил Дивизинюк, Валерия Ковач

ГУ «Институт геохимии окружающей среды НАН Украины», г. Киев

Система мониторинга – это измерительная система или система преобразования информации о фактическом состоянии окружающей природной среды в вид и в форму, которые позволяют ее достаточно быстро передавать и обрабатывать. Оптимизации этого процесса способствует внедрение средств цифровой вычислительной техники. Существующие на сегодняшний день измерительные радиационные устройства в своей основе являются аналоговыми измерителями (датчиками). Транслировать аналоговый сигнал на большие расстояния достаточно сложная задача. Она обусловлена, с одной стороны, влиянием множества препятствий на канал трансляции данных. С другой – обработка аналоговых сигналов требует достаточно габаритного и дорогостоящего оборудования. Решают эту задачу так называемые гибридные преобразователи информации.

В современных гибридных системах, независимо от их назначения, большое распространение получили аналого-цифровые каналы. Для правильной организации процесса аналого-цифрового преобразования принципиальное значение имеет вопрос о том, при каких условиях выходят коды аналого-цифрового преобразователя, которые, в свою очередь, могут считаться эквивалентными входным аналоговым сигналам.

Основной задачей системы радиоэкологического мониторинга является контроль за радиационной и экологической ситуацией.

В статье описано, что единичный элемент (автоматизированный пост) должен обеспечить сбор (измерение) первичной информации о состоянии окружающей природной среды: в воздухе, в почвах и его поверхности, в подземных водах. Передача первичных данных происходит на главный (базовый) пост, где на основе полученной первичной информации формируется оценка радиационной обстановки, анализируется текущая экологическая ситуация и прогнозируется динамика ее развития и возможных последствий. Кроме этого пост должен обеспечивать непрерывный радиационной контроль, а на главном (базовом) посте должна реализовываться система баз данных о всех необходимых элементах окружающей природной среды. Пост также должен обеспечивать периодический отбор проб для их дальнейшего лабораторного анализа.

DEVELOPMENT OF A SINGLE ELEMENT (STATION) FOR MEASUREMENT OF ATMOSPHERIC AIR PARAMETERS

Mikhail Diviziniuk, Valeriia Kovach

SI "Institute of Environmental Geochemistry of the NAS of Ukraine", Kiev

The monitoring system - a measuring system or system of information conversion about the actual state of the environment in the form that allows its quick transfer and process. Optimization of the process facilitates the introduction of digital computing. Existing radiation measuring devices by origin - analog meters (sensors). Cast analog signal over long distances is quite a difficult task. It is due, on the one hand, the influence of many obstacles on the broadcast channel data. On the other - processing of analog signals requires marker and expensive equipment. Solves the problem so-called hybrid information converters.

In modern hybrid systems, regardless of their purpose, large widely analog - digital channels. For proper organization of analog - digital conversion of fundamental importance to the question of under what conditions the codes go through analog - digital converter, which in turn may be considered equivalent to the input analog signal.

The main task of radiological monitoring system is to control the radiation and ecological situation.

Therefore, based on this, the article explains that a single element (automated satation) should provide constant (measurement) of primary information about the environment: in the air, soil and its surface, in groundwater. Transfer of raw data goes to the main (basic) station, where on the bases of received initial information emerging radiation situation assessment, analyzes the current environmental situation and projected dynamics of its development and the possible consequences. This post should provide continuous radiation monitoring, and at the base station should be implemented database system on all the elements of the environment. Station should also provide periodic sampling for subsequent laboratory analysis.

Literatura: 1. Kovalko, M. P. YEnergetichna bezpeka – skladova natsional'noï bezpeki Ukraïni [Tekst] / M. P. Kovalko, S. P. Denisyuk. – K. : UYEZ, 1997. – 197 s. 2. Dopovid' pro stan yadernoï ta radiatsiynoï bezpeki v Ukraïni u 2013 rotsi [YElektronniy resurs] / Rezhim dostupu: http://www.snrc.gov.ua. 3. The Ux Consulting Company [Electronic resource] / Available at: http://www.uxc.com. 4. Lisichenko, G. V. Uranovi rudi Ukraïni [Tekst] / G. V. Lisichenko, Yu. P. Mel'nik ta in. – Kiïv: Naukova dumka, 2010. – 221 s. 5. Yaderne zakonodavstvo Ukraïni: Zbirnik normativno – pravovikh aktiv. V 2 t. T. 1. [Tekst] / za red. Yu. S. Shamshuchenka; vid. 2-ge pererob. i dopov. – K.: Vid. Dim «In Yure», 1999. – 648 s. 6. Ukrainian Centre for Economic & Political Studies Named after Olexander Razumkov [Text] / Nuclear energy in the world and in Ukraine: state and prospects of development. – 2008. – Vol. 3. – P. 60.

УДК 531/534(075.8)

СТІЙКІСТЬ РАДІОЕЛЕКТРОННОЇ АПАРАТУРИ ЗАХИСТУ ІНФОРМАЦІЇ ЩОДО ДЕСТАБІЛІЗУЮЧИХ МЕХАНІЧНИХ ВПЛИВІВ

Юрій Зіньковський, Борис Уваров
НТУУ ”КПІ”

Стаття: ***9 стор., 4 джерела.***

У методах проектування високонадійної радіоелектронної апаратури (РЕА) захисту інформації мають бути використані всі можливості підвищення показників надійності конструкції радіоелектронних засобів (РЕЗ) у її складі.

Істотний вплив на роботу РЕЗ мають зовнішні дестабілізуючі впливи - вібрації і удари. Для оцінки працездатності в цих умовах необхідно перш за все визначити власні частоти механічних коливань апарату. При збігу цих частот з частотами зовнішніх впливів виникають резонансні явища - амплітуди коливань можуть стати неприпустимо великими, призвести до порушення цілісності елементів конструкції і відмов РЕА.

У процесі проектування поведінку реальної апаратури при експлуатації може бути оцінено моделюванням на фізичних моделях, які повинні адекватно представляти конструкцію РЕЗ. Наступним кроком проектування має бути розробка математичних моделей - систем диференціальних рівнянь, рішення яких дозволить визначити параметри коливальних процесів при дії вібрацій і ударів.

У статті описані фізичні та математичні моделі, що представляють конструкції дво- і трьохмасових систем - еквіваленти блоків РЕЗ з встановленими в них шасі і чарунками, на яких кріпляться функціональні вузли (ФВ) і елементи електронної структури (ЕЕС).

Отримані рішення показують, що раціональним вибором інерційних характеристик блоку, чарунок та характеристик віброізоляторів можна домогтися практично повного захисту ФВ і ЕЕС від дії дестабілізуючих механічних факторів.

Наведено також результати оптимізації системи віброізоляції для тривимірної моделі реального блоку РЕА, що враховує можливість появи лінійних і крутних коливань відносно всіх трьох осей.

УСТОЙЧИВОСТЬ РАДИОЭЛЕКТРОННОЙ АППАРАТУРЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ДЕСТАБИЛИЗИРУЩИХ МЕХАНИЧЕСКИХ ВОЗДЕЙСТВИЯХ

Юрий Зиньковский, Борис Уваров
НТУУ «КПИ»

В методах проектирования высоконадежной радиоэлектронной аппаратуры (РЭА) защиты информации должны быть использованы все возможности повышения показателей надежности конструкции радиоэлектронных средств (РЭС) в ее составе.

Существенное влияние на работу РЭС оказывают внешние дестабилизирущие воздействия – вибрации и удары. Для оценки работоспособности в этих условиях необходимо прежде всего определить собственные частоты механических колебаний аппарата. При совпадении этих частот с частотами внешних воздействий возникают резонансные явления – амплитуды колебаний могут стать недопустимо большими, привести к нарушению целостности элементов конструкции и отказам РЭА.

В процессе проектирования поведение реальной аппаратуры при эксплуатации может быть оценено моделированием на физических моделях, которые должны адекватно представлять конструкцию РЭС. Следующим шагом проектирования должна быть разработка математических моделей – систем дифференциальных уравнений, решение которых позволит определить параметры колебательных процессов при воздействии вибраций и ударов.

В статье описаны физические и математические модели, представляющие конструкции двух- и трехмассовых систем – эквиваленты блоков РЭС с установленными в них шасси и ячейками, на которых крепятся функциональные узлы (ФУ) и элементы электронной структуры (ЭЭС).

Полученные решения показывают, что рациональным выбором инерционных характеристик блока, ячеек и виброизоляторов можно добиться практически полной защиты ФУ и ЭЭС от действия дестабилизирующих механических факторов.

Приведены также результаты оптимизации системы виброизоляции для трехмерной модели реального блока РЭА, учитывающей возможность появления линейных и крутильных колебаний относительно всех трех осей.

STABILITY OF INFORMATION PROTECTION RADIO EQUIPMENT AGAINST DESTABILIZING MECHANICAL EFFECTS

Juriy Zinkovsky, Boris Uvarov
NTUU “KPI”

In the methods of designing highly reliable electronic equipment (REE) data protection should be used all the possibilities of improving the reliability design of radio-electronic means (REM) in its composition.

Significant impact on the work of REE’s have external destabilizers impact - vibration and shock. To assess the performance under these conditions, it is first necessary to determine the frequency of mechanical oscillation device. The coincidence of these frequencies with the frequencies of external influences there are resonant phenomena - amplitude oscillations may become unacceptably large, lead to the violation of the integrity of structural members and failures REE.

In the process of designing the behavior of the actual equipment in operation can be estimated by modeling the physical models should adequately represent the design of REM’s. The next step of the design should be the development of mathematical models - differential equations, the solution of which will determine the parameters of oscillatory processes when exposed to vibrations and shocks.

This article describes the physical and mathematical models representing the design of two- and trehmetrovyh systems - equivalent blocks of the system from the installed chassis and the cells, which are attached to the functional units (FU) and the elements of the electronic structure (EES).

The obtained solutions show that the rational choice of the inertial characteristics of the unit cells and the characteristics of vibration isolators can achieve almost complete protection FU and EES from destabilizing mechanical factors.

Given the results of the optimization of the vibration isolation system for three dimensional models of real unit REA, taking into account the possibility of linear and torsional vibrations with respect to all three axes.

Literatura: 1. Timoshenko S. P., Yang D. Kh., Uiver U. Kolebaniya v inzhenernom dele/Per. s angl. L. G. Korneychuka; pod red. E. I. Grigolyuka. – M.: Mashinostroyeniye, 1985. – 472 s. 2. G. Korn, T. Korn. Spravochnik po matema-tike dlya nauchnykh rabotnikov i inzhenerov. M.: Nauka, 1968. – 720 s. 3. Tokarev M. F., Talitskiy YE. N., Frolov V. A. Mekhanicheskiye vozdeystviya i zashchita radio-elektronnoy apparatury: Ucheb. posobiye dlya vuzov/Pod red. V. A. Frolova. – M.: Radio i svyaz', 1984. – 224 s. 4. Uvarov B. M., Zin'kovs'kiy Yu. F. Proyektu-vannya ta optimizatsiya mekhanostiykikh konst-ruktsiy radioyelektronnikh zasobiv z imovirnisnimi kharakteristikami. – K.: "Korniychuk", 2011. – 248 s.

УДК 681.35

ЗАСТОСУВАННЯ МЕТОДІВ ФОРСОВАНИХ ВИПРОБУВАНЬ ДЛЯ ОТРИМАННЯ ЗАЛЕЖНОСТІ ДІАГНОСТИЧНОГО ПАРАМЕТРА ВІД ЧАСУ НАПРАЦЮВАННЯ ЦИФРОВИХ РАДІОЕЛЕКТРОННИХ КОМПОНЕНТІВ

Василь Кузавков, Євген Редзюк

Військовий інститут телекомунікацій та інформатизації Державного університету телекомунікацій

Стаття: ***5 стор., 12 джерел***

При використанні методів форсованих випробувань для отримання залежності діагностичного параметру (ДП) від часу напрацювання цифрових радіоелектронних компонентів (РЕК) в безконтактному індукційному методі діагностування потрібно мати на увазі, що існує певна межа, за якою набувають чинності фактори, відсутні в реальних умовах експлуатації. Через вплив цих факторів дані, отримані при форсованих випробуваннях, можуть виявитися спотвореними або помилковими.

За наявності принципової та технічної можливості форсування того або іншого фактора зовнішніх впливів в обов'язковому порядку потрібно оцінити припустиму межу його форсування, встановлену з урахуванням збереження якісної картини фізико-хімічних процесів, що визначають накопичення ушкоджень та настання відмови в умовах експлуатації.

Аналізом методів форсованих випробувань було встановлено, що для РЕК цифрових блоків доцільно застосовувати форсований метод "збільшення режимів роботи виробу", що дозволяє виявити відмови інтегральних схем (ІС), пов'язані з фізико-хімічними процесами та конструктивно-технологічними факторами, такими як: помилки літографії, дефекти окисла, металізації, контактів; короткі замикання або обриви в провідних шинах а також між полікремнієм і металом і т. д.

Аналіз режимів роботи цифрового блоку радіоелектронного озброєння та експлуатаційних параметрів РЕК показав технічну можливість введення в модель випробувань коефіцієнта прискорення при підвищеному омічному навантаженні K_n^R та коефіцієнта прискорення при підвищеній частоті вхідного сигналу K_n^f.

Введення в комплексні форсовані випробування додаткових факторів, що активують, дозволило:

- охопити весь період безвідмовної роботи $T(t) = (10^7 - 10^8)_{\text{Г}}$ РЕК за час випробувань $t_в = 10^3{}_{\text{Г}}$;

- знизити значення частинних коефіцієнтів прискорень ($K_n^T, K_n^R, K_n^f, K_n^U$) та підвищити вірогідність процесу форсованих випробувань, наблизивши ідентичність процесів, що відбуваються в РЕК (фізико-хімічних процесів), до звичайних умов експлуатації.

ПРИМЕНЕНИЕ МЕТОДОВ ФОРСИРОВАННЫХ ИСПЫТАНИЙ ДЛЯ ПОЛУЧЕНИЯ ЗАВИСИМОСТИ ДИАГНОСТИЧЕСКОГО ПАРАМЕТРА ОТ ВРЕМЕНИ НАРАБОТКИ ЦИФРОВЫХ РАДИОЭЛЕКТРОННЫХ КОМПОНЕНТОВ

Василий Кузавков, Евгений Редзюк
Военный институт телекоммуникаций и информатизации Государственного университета телекоммуникаций

При использовании методов форсированных испытаний для получения зависимости диагностического параметра (ДП) от времени наработки цифровых радиоэлектронных компонентов (РЕК) в бесконтактном индукционном методе диагностирования нужно иметь в виду, существование определенной границы, за которой приобретают силу факторы, отсутствующие в реальных условиях эксплуатации. Вследствие влияния этих факторов данные, полученные при форсированных испытаниях, могут оказаться искаженными или ошибочными.

При наличии принципиальной и технической возможности форсирования того или иного фактора внешних влияний в обязательном порядке необходимо провести оценку допустимых границ его форсирования, установленную с учетом сохранения качественной картины физико-химических процессов, определяющих накопление повреждений и наступление отказа в условиях эксплуатации.

Анализ методов форсированных испытаний позволил установить, что для РЕК цифровых блоков целесообразно применять форсированный метод "увеличение режимов работы изделия", что позволяет выявить отказы интегральных схем связанные с физико-химическими процессами и конструктивно-технологическими факторами, такими как: ошибки литографии, дефекты окисла, металлизации, контактов, короткие замыкания или обрывы в ведущих шинах а также между поликремнием и металлом и т. д.

Анализ режимов работы цифрового блока радиоэлектронного вооружения и эксплуатационных параметров РЕК показал наличие технической возможности введения в модель испытаний коэффициента ускорения, связанного с повышенной омической нагрузкой K_y^R, и коэффициента ускорения, связанного с повышенной частотой входного сигнала K_y^f.

Введение в комплексные форсированные испытания дополнительных активирующих факторов позволило:

- охватить весь период безотказной работы РЕК $T(t) = (10^7 - 10^8)_{\text{ч}}$ за время испытаний $t_u = 10^3{}_{\text{ч}}$;

- снизить значение частных коэффициентов ускорения ($K_y^T, K_y^R, K_y^f, K_y^U$) и повысить достоверность процесса форсированных испытаний, приблизив идентичность процессов, происходящих в РЕК (физико-химических процессов), к обычным условиям эксплуатации.

THE APPLICATION OF METHODS OF FORCED TESTING TO OBTAIN THE DEPENDENCE OF DIAGNOSTIC PARAMETER OF RUN TIMES OF DIGITAL RADIO ELECTRONIC COMPONENTS

Vasil Kuzctvkov, Evgen Redzuk
Military Institute Of Telecommunication And Informatization Of State Telecommunication University

By using the methods of forced testing to obtain the dependence of DP of run times of digital radio electronic components (REC) in non-contact induction method of diagnosing necessary to mean that there is a certain limit beyond which become effective factors that absent in real operating conditions. Because of influence of these factors data that was obtained by forced testing may be distorted or erroneous.

If there are principled and technical possibility of forcing one or another external influences compulsorily it is necessary to assess the permissible limits of its forcing that established with a view to preserving the qualitative picture of physical and chemical processes that determined the accumulation of damage and the onset of failure in service.

Analysis techniques augmented tests revealed that the rivers of digital blocks appropriate to apply the method of forced "increase the product to function" that allows you to identify the failures of integrated circuits associated with the physical and chemical processes and structural and technological factors, such as lithography errors, defects in the oxide, metallization contacts, short circuit or open circuit in the leading tire and between polysilicon and metal, and so on.

Analysis of the processes of the unit electronic equipment and operational parameters REC showed the presence of technical possibility of introducing a model test acceleration factor associated with increased ohmic load K_y^R and acceleration factor associated with an increased frequency of the input signal K_y^f.

Introduction to complex forced testing additional activating factors allowed:

- cover the entire uptime REK $T(t) = (10^7 - 10^8)_{\text{ч}}$ during the test $t_u = 10^3{}_{\text{ч}}$;

- reduce the value of the partial factors of acceleration ($K_y^T, K_y^R, K_y^f, K_y^U$), and increase the reliability of the process of forced testing, bringing identity processes in REC (physical and chemical processes) to the normal conditions of use.

Literatura: 1. Vishnivs'kiy V. V., Kuzavkov V. V., Redzyuk Є. V. Analiz metodiv forsovanikh viprobuvan' dlya otrimannya zalezhnosti zmini diagnostichnogo parametra vid chasu napratsyuvannya napivprovidnikovikh REK // Zbirnik naukovikh prats' Viys'kovogo institutu Kiïvs'kogo natsional'nogo universitetu imeni Tarasa Shevchenka. – K.: VIKNU, 2013. – Vip. №43. 2. Volkov A N. Rol' uskorennykh ispytaniy v opredelenii nadezhnosti integral'nykh skhem [Tekst] / A. N. Volkov // Molodoy uchenyy. — 2012. — №10. — S. 41-52. 3. Strogonov A V. «Dolgovechnost' integral'nykh skhem i proizvodstvennyye metody yeye prognozirovaniya»: http://www.chipinfo.ru/literature/chipnews/200206/8.html. 4. Gorlov M. I., YEmel'yanov V. A., Stroganov A. V. Gerontologiya kremniyevykh integral'nykh skhem. M: Nauka. 2004. 5. Stojadinovic N. D. Failure physics of integrated circuits-a review // Microelectron. Reliab. 1983. Vol. 23. N4. P. 609-707. 6. Stojadinovic N. D., Ristic S. D. Failure physics of integrated circuits and relationship to reliability // Phys. Stat. Sol. (a). 1983. Vol. 75. P. 11-47. 7. Wurnik F., Pelloth W. Zuver lassigkeit von integrierton schaltungenll nachrichtennische zeltschrift//1984.Vol.37.N U.S.710-712,714-716. 8. ADI Reliability Handbook 2001. www.analoQ.com 9. Atmel corporation. Quality & reliability handbook 2001-2002. Rev. 09/01// www.atmel.com 10. RD 11 0755-90. Mikroskhemy integral'nyye. Metody uskorennykh ispytaniy na bezotkaznost' i dolgovechnost'. RNII «Elektronstandart». 1990. 11. Vowles J. V. A survey of reliability prediction procedures for microelectronics devices // IEEE Trans. Reliab. 1992. Vol. 41. N 1. P. 2-12. 12. Gorlov M. I., Korolev S. Yu., Kulakov A. V., Strogonov A. V. Raschet nadezhnosti integral'nykh skhem po konstruktivno-tekhnologicheskim dannym. Voronezh: Izd-vo Voronezhskogo universiteta. 1996.

УДК 004.62

СПОСІБ ПІДВИЩЕННЯ ШВИДКОДІЇ СИСТЕМИ КОНТРОЛЮ ДОСТУПУ ЗА РАЙДУЖНОЮ ОБОЛОНКОЮ ОКА

Євгеній Подгорний, Любов Рябова, Володимир Темніков
Національний авіаційний університет

Стаття: ***5 стор, 9 джерел.***

Одними із складових частин систем технічного захисту інформації на об'єктах інформаційної діяльності є автоматизовані системи контролю доступу на ці об'єкти, робота яких заснована на скануванні, обробці та аналізі біометричних ознак людини. Системи контролю доступу будуються за типовою схемою розпізнавання образів, що включає в себе підсистеми попередньої обробки зображень або сигналів, параметризації, класифікації та прийняття рішення, а також бази даних (БД) зареєстрованих користувачів. Швидкодія системи, що є найважливішим показником ефективності її роботи, істотно залежить від швидкодії підсистеми класифікації, яка значною мірою визначається часом взаємодії з БД і, в першу чергу, – тривалістю пошуку еталонів в них. Це обумовлює високу актуальність вирішення проблеми прискорення цього процесу.

Авторами за результатами проведених досліджень розроблено спосіб підвищення швидкодії систем контролю доступу, заснований на мінімізації часу пошуку еталонів в БД. У статті зазначений спосіб представлений для випадку розпізнавання людини біометричними системами, побудованими на основі

сканування, обробки та аналізу зображень райдужної оболонки ока (РОО) людини. Вибір РОО обумовлений тим, що розпізнавання за цією біометричною ознакою є одним з найбільш точних.

Мінімізувати тривалість пошуку еталона в БД авторами пропонується шляхом кластеризації усієї множини еталонів РОО, що зберігаються в БД, з подальшим проведенням пошуку тільки в деякій підмножині еталонів (в одному з кластерів). Кластери утворюються за таким правилом: об'єкт буде приєднаний до вже існуючого кластеру, якщо, принаймні, один з його елементів знаходиться на тому ж рівні подібності, що і об'єкт, який претендує на включення в цей кластер. Для визначення відстані між кластерами за результатами експериментальних досліджень була обрана метрика «за далеким сусідом», застосування якої дозволяє отримати більш збалансований розподіл об'єктів по кластерах порівняно з іншими підходами.

Наведені в статті результати аналізу показали, що використання розробленого способу дозволяє істотно скоротити час пошуку відповідного еталону в базі даних.

СПОСОБ ПОВЫШЕНИЯ БЫСТРОДЕЙСТВИЯ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА ПО РАДУЖНОЙ ОБОЛОЧКЕ ГЛАЗА

Евгений Подгорный, Любовь Рябова, Владимир Темников
Национальный авиационный университет

Одними из составных частей систем технической защиты информации на объектах информационной деятельности являются автоматизированные системы контроля доступа на эти объекты, работа которых основана на сканировании, обработке и анализе биометрических признаков человека. Системы контроля доступа строятся по типовой схеме распознавания образов, включающей в себя подсистемы предварительной обработки изображений или сигналов, параметризации, классификации и принятия решения, а также базы данных (БД) зарегистрированных пользователей. Быстродействие системы, являющееся важнейшим показателем эффективности ее работы, существенно зависит от быстродействия подсистемы классификации, которое в значительной степени определяется временем взаимодействия с БД и, в первую очередь, – продолжительностью поиска эталонов в них. Это обусловливает высокую актуальность решения проблемы ускорения этого процесса.

Авторами по результатам проведенных исследований разработан способ повышения быстродействия систем контроля доступа, основанный на минимизации времени поиска эталонов в БД. В статье указанный способ представлен для случая распознавания человека биометрическими системами, построенными на основе сканирования, обработки и анализа изображений радужной оболочки глаза (РОГ) человека. Выбор РОГ обусловлен тем, что распознавание по этому биометрическому признаку является одним из наиболее точных.

Минимизировать продолжительность поиска эталона в БД авторами предлагается путем кластеризации всего множества эталонов РОГ, хранящихся в БД, с последующим проведением поиска только в некотором подмножестве эталонов (в одном из кластеров). Кластеры образуются по следующему правилу: объект будет присоединен к уже существующему кластеру, если, по крайней мере, один из его элементов находится на том же уровне сходства, что и объект, претендующий на включение в этот кластер. Для определения расстояния между кластерами по результатам экспериментальных исследований была выбрана метрика «по дальнему соседу», применение которой позволяет получить более сбалансированное распределение объектов по кластерам по сравнению с другими подходами.

Приведенные в статье результаты анализа показали, что использование разработанного способа позволяет существенно сократить время поиска соответствующего эталона в базе данных.

THE METHOD OF INCREASING A SPEED OF A CONTROL SYSTEM OF ACCESS BY IRIS

Yevgeny Podgorny, Lyubov Ryabova, Volodymyr Temnikov
National aviation university

One of the components of technical information security systems on the objects of information activity are automated access control systems for these objects, which are based on scanning, processing and analysis of biometric human features. Access control systems are based on the template pattern recognition, including subsystems of pretreatment of images or signals, parameterization, classification and decision making, and a registered users databases. Speed of the system is an important indicator of its effectiveness, essentially depends on

the speed of classification subsystem, which is largely determined by the time of interaction with the database and, in the first place, the duration of the search standards in them. This causes the high relevance of solving the problem of acceleration of this process.

The authors by results of the research developed a method for increasing the speed of access control systems based on minimizing time of searching standards in the database. In this paper, the method is presented for the case of human recognition by biometric systems based on scanning, image processing and analysis of the iris. Selection of iris is caused by that this kind of recognition is one of the most accurate.

The authors propose to minimize the duration of the searching standard in the databases, by clustering the entire set of standards iris stored in the database, followed by search only in a subset of standards (in one of the clusters). Clusters are formed according to the rule: the object will be attached to an already existing cluster, if at least one of its elements is at the same level of similarity as the subject, pretending to be included in this cluster. To determine the distance between the clusters by results of experimental studies was chosen metric "for distant neighbors", application which allows you to get a more balanced distribution of objects in clusters compared with other approaches.

Presented in the paper the results of the analysis showed that the use of the developed method can significantly reduce the search time of the corresponding standard in the database.

Literatura: 1. Vorona V. A., Tikhonov V. A. Sistemy kontrolya i upravleniya dostupom. – M.: Goryachaya liniya-Telekom, 2010. – 272 s. 2. Gonchar V. K. Biometricheskiye sistemy i ikh primeneniye // Biznes i bezopasnost'. – 2002. – № 6. – S. 30-31. 3. Daugman J. How Iris Recognition Works // IEEE Trans. – 1993. – CSVT 14(1). – P.21–30. 4. Hao F., Daugman J., Zielinski P. A Fast Search Algorithm for a Large Fuzzy Database // IEEE Trans. Information Forensics and Security. – 1994. – №3(2). – P.203–212. 5. Berikov V.S., Lbov G.S. Sovremennyye tendentsii v klasternom analize // Vserossiyskiy konkursnyy otbor obzorno-analiticheskikh statey po prioritetnomu napravleniyu «Informatsionno-telekommunikatsionnyye sistemy», 2008. – 26 s. 6. Pavel'yeva YE. A., Krylov A. S. Algoritmy predobrabotki raduzhnoy obolochki glaza // Trudy konferentsii «GraphiCon». – M., 2008. – S.314. 7. Pavel'yeva YE. A, Krylov A. S., Ushmayev O.S. Razvitiye informatsionnoy tekhnologii identifikatsii cheloveka po raduzhnoy obolochke glaza na osnove preobrazovaniya Ermita // Sistemy vysokoy dostupnosti. – 2009. – № 1. – S.36–42. 8. Faktornyy, diskriminantnyy i klasternyy analiz / Dzh.-O. Kim, Ch. U. M'yuller, U. R. Klekka, M. S. Oldenderfer, R. K. Bleshfild; pod red. I. S. YEnyukova. – M.: Finansy i statistika, 1989. – 215 s. 9. Baza dannykh CASIA-IrisV3; http://www.cbsr.ia.ac.cn / IrisDatabase.htm.