4 Реферати

УДК 351.86:004.056

КІБЕРТЕРОРИЗМ І ІНФОРМАЦІЙНА БЕЗПЕКА

Володимир Хорошко, Михайло Шелест
Національний Авіаційний Університет

Стаття: ***5 стор., 7 джерел.***

Розвиток людства послідовно призводить до нових форм поширення інформації, найбільш популярними з яких є телекомунікаційні мережі. Використання цих мереж у різних галузях діяльності людського суспільства природно приваблює різного роду злочинців.

Виходячи з цього можна виділити наступні аспекти привабливості телекомунікаційних мереж для кібертероризму:

- більшість серверів мереж дозволяють користувачам працювати відносно конфіденційно і анонімно;
- існує можливість використання спеціальних роботів для зниження часу витрат на терористичну діяльність;
- кіберзлочини складно відстежити і зібрати докази;
- менший ризик порівняно із звичайними видами злочинів і більш висока ефективність;
- можливість здійснювати кіберзлочини через кордони країн і континентів;
- не потрібно фізичної присутності.

Отже, розгляд стану і розвитку інформаційних технологій та кібертероризму дозволяє прогнозувати майбутнє. Однією з найбільш небезпечних загроз безпеки є все більш широке використання кібертерористами можливостей відкритих телекомунікаційних мереж на світову громадськість і координації своєї діяльності.

Існує значне число проблем у протидії злочинності. Осторонь від числа технічних, правових та фінансових аспектів, що визначають захист інформаційного простору та інфраструктури, стоїть різна кількість неврегульованих елементів між комерційними структурами та державними організаціями щодо того, які компоненти інформаційного простору та інфраструктури вимагають захисту і методи дій стосовно кібертерористів.

У роботі сформульовані і приведені негативні наслідки, до яких призводить суперечливість і нерозвиненість правового регулювання суспільних відносин в інформаційному просторі; пропозиції щодо вдосконалення формування інформаційної інфраструктури України з метою підтримки питань національної безпеки; спрогнозовані тенденції розвитку засобів захисту від кібертероризму.

КИБЕРТЕРРОРИЗМ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Владимир Хорошко, Михаил Шелест
Национальный Авиационный Университет

Развитие человечества последовательно приводит к новым формам распространения информации, наиболее популярными из которых являются телекоммуникационные сети. Использование этих сетей в различных отраслях деятельности человеческого общества естественно привлекает различного рода преступников.

Исходя из этого можно выделить следующие аспекты привлекательности телекоммуникационных сетей для кибертерроризма:

- большинство серверов сетей позволяют пользователям работать относительно конфиденциально и анонимно;
- существует возможность использования специальных роботов для снижения времени затрат на террористическую деятельность;
- киберпреступления сложно отследить и собрать доказательства;
- меньший риск в сравнении с обычными видами преступлений и более высокая эффективность;
- возможность совершать киберпреступления через границы стран и континентов;
- не требуется физического присутствия.

Следовательно, рассматрение состояния и развития информационных технологий и кибертерроризма позволяется прогнозировать будущее. Одной из наиболее опасных угроз безопасности является все более

широкое использование кибертеррористами возможностей открытых телекоммуникационных сетей на мировую общественность и координации своей деятельности.

Существует значительное число проблем в противодействии преступности. В стороне от числа технических, правовых и финансовых аспектов, определяющих защиту информационного пространства и инфраструктуры, стоит различное количество неурегулированных элементов между коммерческими структурами и государственными организациями относительно того, какие компоненты информационного пространства и инфраструктуры требуют защиты и методы действий по отношению к кибертеррористам.

В работе сформулированы и приведены негативные последствия к которым приводит противоречивость и неразвитость правового регулирования общественных отношений в информационном пространстве; предложения по совершенствованию формирования информационной инфраструктуры Украины с целью поддержания вопросов национальной безопасности; спрогнозированы тенденции развития средств защиты от кибертерроризма.

CYBERTERRORISM AND INFORMATION SECURITY

Vladimir Khoroshko, Michael Shelest
National Aviation University

Development of mankind consistently leads to new forms of information dissemination, the most popular of which are telecommunications networks. The use of these networks in different fields of activity of human society naturally attracts different kinds of criminals.

From this we can identify the following aspects of telecommunications networks for the attractiveness of cyberterrorism:

- Most servers networks allow users to respect confidential and anonymous;
- There is the possibility of using special robots to reduce the time cost of terrorist activity;
- Cybercrime is difficult to track and collect evidence;
- Less risk in comparison to conventional forms of crime and higher efficiency;
- The ability to commit cybercrimes across borders and continents;
- Does not require a physical presence.

Therefore, considering the status and development of information technology and cyber-terrorism is allowed to predict the future. One of the most dangerous security threats is the increasing use of cyber-terrorists opportunities open telecommunication networks on the world community and coordinate their activities.

There is a significant number of problems in combating crime. In the mapping of the number of technical, legal and financial aspects that determine the protection of information space and infrastructure, there is also a different number of outstanding elements between businesses and government organizations on what components of the information space and infrastructure require protection methods and actions in relation to cyber-terrorists.

In work and given the negative consequences which leads contradictory and inadequate legal regulation of social relations in the information space, proposals for improvement of information infrastructure of Ukraine in order to maintain national security, development trends predicted protection against cyberterrorism.

УДК 621.321

СТВОРЕННЯ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ МАТРИЦ НЕБЕЗПЕЧНИХ ФАКТОРІВ, ЩО ХАРАКТЕРИЗУЮТЬ ТЕХНІЧНІ КАНАЛИ ВИТОКУ

Сергій Довбня, Андрій Нікірін, Іван Четверіков
Київський Національний університет імені Тараса Шевченка

Статья: ***8 стор., 10 джерел***.

Забезпечення захисту інформації спрямовується зокрема на те, щоб не допустити збитків від утрати конфіденційної інформації. Усі шкідливі дії можуть бути здійснені тільки за наявності будь-яких слабких місць (уразливостей). Для одного об'єкту може бути декілька можливих технічних каналів витоку інформації. Загальним критерієм для усіх типів каналів є рівень загрози застосування технічних засобів розвідки. Захист інформації не існує сам по собі, у відриві від людини. Він забезпечується для людини і ним же оцінюється. Тому, поняття технічного захисту інформації має не лише об'єктивну, але і суб'єктивну сторону, оскільки оцінка його рівня проводиться людиною. При цьому оцінка рівня захисту інформації (РЗІ) завжди відносна. Спроби безпосередньо надати цій оцінці чисельне значення у більшості випадків

безперспективні в плані подальшої інтерпретації результатів. Це призводить до слабкої формалізованості завдання оцінки технічної захищеності інформації і до необхідності оперування лінгвістичними змінними і, як наслідок, до застосування апарату нечіткої логіки. Для вирішення завдань, пов'язаних з моделюванням нечітко формалізованих процесів, їх прогнозуванням і підтримкою ухвалення рішень часто використовуються нечітки когнітивні моделі. При побудові нечіткої когнітивної моделі (НКМ) об'єкт дослідження представляють у вигляді знакового орієнтованого графа, що дає можливість формалізації чисельно незмірних чинників, використання неповної, нечіткої і навіть суперечливої інформації.

Рішення такої задачі необхідно проводити з урахуванням інформації, яка циркулює на об'єкті та її співвідношення з типом технічного каналу. Для отримання множини небезпечних факторів на основі отриманих таблиц $\{X_j\}_{НФ}$ необхідно сформувати алгоритм оцінки захищеності. Алгоритм являє собою сукупність послідовних "тестових" дій щодо об'єкта:

- збір інформації про об'єкт захисту, вибір критеріїв, що характеризують стан різних технічних каналів витоку інформації, визначення їх прийнятного рівня (можливо у вигляді інтервальних оцінок або лінгвістичних термінів);
- побудова когнітивної моделі у вигляді знакового орієнтованого графа з накладеною системою стосунків переваги типу;
- обчислення вагів Фішберна на підставі модифікованого методу нестрого ранжування;
- аналіз рівня захисту інформації.

Якщо РЗІ не знаходиться в прийнятному діапазоні значень, то робляться зміни у складі концептів, які приймають участь в побудові когнітивної моделі, у складі зв'язків між концептами, змінюються їх ваги за допомогою введення захисних заходів. Ці зміни відповідають різним стратегіям побудови системи ТЗІ: зменшення ризиків, ухилення від ризиків, прийняття ризиків.

Таким чином, процес створення системи ТЗІ має на увазі рішення двох взаємозв'язаних завдань: прямого (аналіз стану системи) і зворотного завдання управління (дія на систему).

При рішенні першої задачі вимагається визначити значення критеріїв просочування інформації K_i і інтегрального критерію K при заданих значеннях усіх концептів, що впливають на них. Якщо отримані значення знаходяться поза діапазоном прийнятності, то при рішенні зворотної задачі необхідно підібрати такі дії Z_i і L, що управляють, які забезпечать повернення цільових критеріїв у безпечний діапазон.

Якщо існує не єдиний набір необхідних управляючих дій, то на цьому етапі може виникнути завдання оптимізації, що полягає в знаходженні такої комбінації Zi і L, яка забезпечує максимальну дію на негативні чинники при заданих або мінімальних витратах на реалізацію способів і засобів захисту.

СОЗДАНИЕ СИСТЕМЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ МАТРИЦ ОПАСНЫХ ФАКТОРОВ, КОТОРЫЕ ХАРАКТЕРИЗУЮТ ТЕХНИЧЕСКИЕ КАНАЛЫ УТЕЧКИ

Сергей Довбня, Андрей Никирин, Иван Четвериков
Киевский Национальный университет имени Тараса Шевченко

Обеспечение защиты информации направляется, в частности, на то, чтобы не допустить убытков от потери конфиденциальной информации. Все вредные действия могут быть осуществлены только при наличии любых слабых мест (уязвимостей). Для одного объекта может быть несколько возможных технических каналов утечки информации (ТКУИ). Общим критерием для всех типов каналов является уровень угрозы применения технических средств разведки (ТСР). Защита информации не существует сама по себе, в отрыве от человека. Она обеспечивается для человека и им же оценивается. Поэтому понятие технической защиты информации имеет не только объективную, но и субъективную сторону, поскольку оценка его уровня проводится человеком. При этом оценка уровня защищенности информации всегда относительна. Попытки непосредственно придать этой оценке численное значение в большинстве случаев бесперспективны в плане дальнейшей интерпретации результатов. Это приводит к слабой формализованности задания оценки технической защищенности информации и к необходимости. Это приводит к слабой формализованности задачи оценки технической защищенности информации и к необходимости оперирования лингвистическими переменными и, как следствие, к применению аппарата нечеткой логики. Для решения заданий, связанных с моделированием нечетко формализированных процессов, их прогнозированием и поддержкой принятия решений, часто используются нечеткие

когнитивные модели. При построении нечеткой когнитивной модели (НКМ) объект исследования представляют в виде знакового ориентированного графа, который дает возможность формализации численно неизмеримых факторов, использования неполной, нечеткой и даже противоречивой информации.

Решение такой задачи необходимо проводить с учетом информации, которая циркулирует на объекте и ее соотношение с типом технического канала. Для получения множества опасных факторов на основе полученных таблиц $\{Xj\}_{НФ}$ необходимо сформировать алгоритм оценки защищенности. Алгоритм являет собой совокупность последовательных "тестовых" действий относительно объекта:

- сбор информации об объекте защиты, выборе критериев, которые характеризуют состояние разных ТКУИ, определение их приемлемого уровня (возможно в виде интервальных оценок или лингвистических сроков);
- построение когнитивной модели в виде знакового ориентированного графа с наложенной системой отношений преимущества типа;
- вычисление весов Фишберна на основании модифицированного метода нестрого ранжирования;
- анализ уровня защиты информации (УЗИ).

Если УЗИ не находится в приемлемом диапазоне значений, то делаются изменения в составе концептов, которые принимают участие в построении когнитивной модели, в составе связей между концептами, изменяются их весы с помощью введения защитных средств. Эти изменения отвечают разным стратегиям построения системы ТЗИ: уменьшение рисков, уклонения от рисков, принятия рисков.

Таким образом, процесс создания системы ТЗИ имеет в виду решение двух взаимосвязанных заданий : прямого (анализ состояния системы) и обратного задания управления (действия на систему).

При решении первой задачи требуется определить значение критериев утечки информации K_i и интегрального критерия K при заданных значениях всех концептов, которые влияют на них. Если полученные значения находятся вне диапазона приемлемости, то при решении обратной задачи необходимо подобрать такие действия Z_i и L, что управляют, какие обеспечат возвращение целевых критериев в безопасный диапазон.

Если существует не единственный набор необходимых управляющих действий, то на этом этапе может возникнуть задание оптимизации, которая заключается в нахождении такой комбинации Z_i и L, которая обеспечивает максимальное действие на негативные факторы при заданных или минимальных расходах на реализацию способов и средств защиты.

CREATION OF TECHNICAL DEFENCE INFORMATION SYSTEM WITH THE DANGEROUS FACTORS MATRICES USAGE THAT CHARACTERIZE TECHNICAL LOSS CHANNELS

Serhij Dovbnia, Andrii Nicirin, Ivan Chetverikov
Kyiv National university of the name of Taras Shevchenko

Providing of defence of information in particular heads for that, to shut out losses from the loss of confidential information. All harmful actions can be carried out only at presence of any weak points. For one object there can be a few possible technical channels of source of information. A general criterion for all types of channels is a level of threat of application of technical equipments of secret service. Defence of information does not exist in itself, in tearing away from a man. He is provided for a man and estimated them. Volume, concept of technical defence of information has not only objective but also subjective side, as an estimation of his level is conducted by a man. Thus estimation of level of security Attempts directly to give this estimation a numeral value in most cases having no prospects in the plan of further interpretation of results. It results in weak formalization of task of estimation of technical security of information and to the необходимости operating by linguistic variables and, as a result, to application of vehicle of fuzzy logic. For the decision of the tasks, related to the design of the unclearly formalized processes, their prognostication and support of making decision, нечітки is often used verbal - logical models. At the construction of unclear verbal - logical model a research object is presented as the sign oriented count, that gives an opportunity formalizations numeral of immeasurable factors, uses of incomplete, unclear and even contradictory information.

The decision of such task must be conducted taking into account information that circulates on an object and her correlation with the type of technical channel. For the receipt of great number of dangerous factors on the basis of got tables of dangerous factors {Xj} must be formed algorithm of estimation of security. An algorithm shows a soba totality of successive "test" actions in relation to an object:

it is collection of information about the object of defence, choice of criteria that characterize the state of different TCSI, determination of them acceptable level (maybe as interval estimations or linguistic terms);

it is a construction of verbal - logical model as the sign oriented count with the imposed system of relations of advantage as;

it is a calculation of scales of Fichberna on the basis of the modified method unstrict ranging;

it is an analysis of level of defence of information (LDI).

If LDI is not in the acceptable range of values, then changes in composition concepts, that take part in the construction of verbal - logical model, are done, in composition connections between concepts, their scales change by means of introduction These changes answer different strategies of construction of the system TDI : reduction of risks, avoiding risks, acceptance of risks.

Thus, process of creation of the system technical defence of information means decision of two associate tasks : direct (analysis of the state of the system) and reverse task of management (operating is on the system).

At the decision of the first task it is required to define the value of criteria of loss of information of Ki and integral criterion of K at the set values of all concepts that influence on them. If the got values are out of range of acceptability, then at the decision of reverse task it is necessary to pick up such actions of Zi and L, that manage, what will provide the return of having a special purpose criteria in a safe range.

If there is a not only set of necessary managers of actions, then on this stage there can be a task to optimization that consists in being of such combination of Zi and L, that provides the maximal operating on negative factors at the set or minimum charges on realization of methods and facilities of defence.

УДК 621.372

ОЦІНЮВАННЯ ЙМОВІРНОСТІ ПРАВИЛЬНОГО РОЗПІЗНАВАННЯ ІНФОРМАЦІЇ ПРИ ПРИЙМАННІ ПОБІЧНИХ ЕЛЕКТРОМАГНІТНИХ ВИПРОМІНЮВАНЬ ПІД ЧАС ПАРАЛЕЛЬНОГО ПЕРЕДАВАННЯ СИГНАЛІВ

Михайло Прокофьєв, Василь Стеченко
НДЦ «ТЕЗІС» НТУУ КПІ

Стаття ***4 стор., 4 джерел***

У засобах обчислювальної техніки часто застосовується паралельна передача сигналів по багатопровідним лініям. При цьому в навколишній простір випромінюється сумарний сигнал, рівень якого пропорційний кількості переданих сигналів високого рівня. За рівнем цього сумарного сигналу неможливо однозначно визначити, в яких лініях передавався сигнал високого рівня, а в яких - сигнал низького рівня. У точці прийому рівень прийнятого сигналу сумірний з рівнем навколишнього шуму, тому на ймовірність правильного розпізнавання впливає ще й шум. У найпростішому випадку це сума корисного сигналу та адитивної завади у вигляді стаціонарного гауссового шуму з нормальним законом розподілу амплітуди.

У статті досліджується залежність ймовірності правильного приймання біта інформації залежно від кількості ліній і відносини сигнал/шум на вході оптимального приймального пристрою. Наведено результати аналізу в припущенні, що рівні випроміненого сигналу кожної лінії багатопровідного кабелю однакові, і оцінено вплив відмінності сигналів в окремих лініях.

Показано, що при малому відношенні сигнал/шум ймовірність правильного приймання біта інформації при паралельній передачі наближається до ймовірності послідовної передачі. У цьому випадку неоднозначність визначення номера лінії з сигналом високого рівня компенсується збільшенням середньої енергії сумарного сигналу в порівнянні з енергією сигналу однієї послідовної лінії. У міру збільшення відносини сигнал/шум ймовірність правильного прийому інформації при паралельному її передаванні збільшується повільніше, ніж у послідовній передачі і значення цієї ймовірності завжди менше одиниці. Таким чином, паралельна передача сигналів характеризується певним рівнем захищеності. Граничне значення ймовірності правильного прийому при паралельній передачі сигналів знаходиться в зворотній залежності від числа передавальних ліній.

ОЦЕНКА ВЕРОЯТНОСТИ ПРАВИЛЬНОГО РАСПОЗНАВАНИЯ ИНФОРМАЦИИ ПРИ ПРИЕМЕ ПОБОЧНОГО ИЗЛУЧЕНИЯ ОТ ПАРАЛЛЕЛЬНО ПЕРЕДАВАЕМЫХ СИГНАЛОВ

Михаило Прокофьев, Василий Стеченко
НДЦ «ТЕЗИС» НТУУ КПИ

В средствах вычислительной техники часто применяется параллельная передача сигналов по многопроводным линиям. При этом в окружающее пространство излучается суммарный сигнал, уровень которого пропорционален количеству передаваемых сигналов высокого уровня. По уровню этого суммарного сигнала невозможно однозначно определить, в каких линиях передавался сигнал высокого уровня, а в каких – сигнал низкого уровня. В точке приема уровень принимаемого сигнала обычно соизмерим с уровнем окружающего шума, поэтому на вероятность правильного распознавания влияет еще и шум. В простейшем случае это сумма полезного сигнала и аддитивной помехи в виде стационарного гауссова шума с нормальным законом распределения амплитуды.

В статье исследуется зависимость вероятности правильного приема бита информации в зависимости от количества линий и отношения сигнал/шум на входе оптимального приемного устройства. Приведены результаты анализа в предположении, что уровни излученного сигнала каждой линии многопроводного кабеля одинаковы, и оценено влияние отличия сигналов в отдельных линиях.

Показано, что при малом отношении сигнал/шум вероятность правильного приема бита информации для параллельной передачи приближается к вероятности последовательной передачи. В этом случае неоднозначность определения номера линии с сигналом высокого уровня компенсируется увеличением средней энергии суммарного сигнала по сравнению с энергией сигнала одной последовательной линии. По мере увеличения отношения сигнал/шум вероятность правильного приема информации при параллельной передаче увеличивается медленнее, чем у последовательной и значение этой вероятности всегда меньше единицы. Таким образом, параллельная передача сигналов характеризуется определенным уровнем защищенности. Предельное значение вероятности правильного приема при параллельной передаче сигналов находится в обратной зависимости от числа передающих линий.

EVALUATION PROBABILITY OF RECOGNITION INFORMATION RECEPTION SPURIOUS EMISSIONS FROM THE PARALLEL TRANSMIT SIGNALS

Mikhail Prokofiev, Basil Stechenko
Research Centre "TESIS" NTUU " KPI "

In computing machinery is often used parallel transmission of information signals on multiwire lines. In the surrounding space is emitted total signal whose level is proportional to the number of transmitted signal of high level. According to the level of the total signal can not determine if any lines in the transmitted signal is high level, and in which - a low level signal . At the point of receiving the received signal level is usually commensurate with the level of ambient noise, so the probability of correct recognition and affects more noise. In the simplest case, the programming signal and additive noise in the form of a stationary Gaussian noise with a normal law of distribution of the amplitude.

The paper investigates the dependence of the probability of correctly receiving bits of information depending on the number of lines and the signal/noise ratio at the input of the optimal receiver. Results of the analysis on the assumption that the transmitted signal levels of each line are the same multi-wire cable, and evaluated the impact of differences in individual signal lines.

It is shown that at low signal/noise ratio probability of correct reception of bits of information in parallel transmission probability is close to the serial transmission. In this case, the ambiguity of the definition of the line room with high-level signal is compensated by the increase in the average total energy of the signal compared to the signal energy of one serial line. With increasing parameter signal / noise ratio probability of correct reception of information in parallel to its transmission increases slower than the sequential transmission and the value of this probability is always less than unity. Thus, the parallel transmission of signals characterized by a certain level of

protection. The limit value for the probability of correct reception of the parallel transmission signals is inversely proportional to the number of transmission lines.

УДК 621.373

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПОБІЧНОГО ЕЛЕКТРОМАГНІТНОГО ВИПРОМІНЮВАННЯ SSD ТА HDD НАКОПИЧУВАЧІВ

Микола Романюков
ГУМВС України в Одеській області

Стаття: ***6 стор., 7 джерел.***

З появою на сучасних ринках твердотілих накопичувачів SSD (solid-state drive) при аналізі методів обробки інформації, що містить державну таємницю, виникає потреба провести дослідження та порівняльну характеристику вимірювання побічного електромагнітного випромінювання та наводів від HDD накопичувачів та твердотілих аналогів, що можна зробити за допомогою комплексу АКОР-2ПК.

Цифровий багатофункціональний пошуково-вимірювальний комплекс реалізовано на основі виявлення радіовипромінювань. АКОР-2ПК являє собою аналізатор спектру та високочутливий селективний вимірювальний приймач для частотного діапазону від 10 Гц до 3000 МГц. Згідно з експлуатаційною документацією комплекс забезпечує:

– вимірювання напруги, створюваної ПЕМВН від різних пристроїв низькострумової техніки (персональних ЕОМ, оргтехніки, апаратури зв'язку);

– вимірювання напруженості електричного (Е) і магнітного (Н) поля (при підключенні вимірювальних антен);

– вимірювання струму (при підключенні вимірювального струмознімача).

Проводячи вимірювання електричної складової поля із застосуванням методу примусової активізації, який полягає в активізації каналу еталонним сигналом, проведено порівняльну характеристику вимірювання побічних електромагнітних випромінювань від SSD та HDD накопичувачів та отримано наступні результати:

• швидкість читання-запису SSD накопичувачів в декілька разів перевищує швидкість читання-запису HDD;

• HDD накопичувачі в режимі роботи споживають майже в 2 рази більше енергії ніж SSD;

• ударостійкість SSD накопичувачів перевищує ударостійкість HDD в 23 рази в режимі роботи та в 4 рази в режимі зберігання інформації;

• відсутність будь-якого шуму під час роботи твердотілих накопичувачів пояснюється відсутністю рухомих частин конструкції (на відміну від HDD);

• фізичні розміри та вага HDD значно перевищують твердотілий аналог;

• більше значення тактової частоти та зниження тривалості імпульсу SSD свідчить про досить швидкий обмін даними накопичувача;

• отримання інформативних частот під час вимірювання HDD свідчить про реальну загрозу витоку інформації каналом ПЕМВН;

• на сьогоднішній день вартість твердотілих накопичувачів порівняно з HDD залишається досить високою.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОБОЧНОГО ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ SSD И HDD НАКОПИТЕЛЕЙ

Николай Романюков
ГУМВД Украины в Одесской области

С появлением на современных рынках твердотельных накопителей SSD (solid-state drive) при анализе методов обработки информации, содержащей государственную тайну, возникает необходимость провести исследования и сравнительную характеристику измерений побочного электромагнитного излучения и

наводок от HDD накопителей и твердотельных аналогов, что можно сделать с помощью комплекса АКОР- 2ПК.

Цифровой многофункциональный поисково-измерительный комплекс реализован на основе выявления радиоизлучений. АКОР-2ПК представляет собой анализатор спектра и высокочувствительный селективный измерительный приемник для частотного диапазона от 10 Гц до 3000 МГц. В соответствии с эксплуатационной документацией комплекс обеспечивает:

- измерение напряжения, создаваемого ПЭМИН от различных устройств низкотоковой техники (персональных ЭВМ, оргтехники, аппаратуры связи);
- измерение напряженности электрического (Е) и магнитного (Н) поля (при подключении измерительных антенн);
- измерение тока (при подключении измерительного токосъемника).

Проведены измерения электрической составляющей поля по методу принудительной активизации. Приведена сравнительная характеристика измерения побочных электромагнитных излучений от SSD и HDD накопителей и получены следующие результаты :

- скорость чтения-записи SSD накопителей в несколько раз превышает скорость чтения-записи HDD;
- HDD накопители в режиме работы потребляют почти в 2 раза больше энергии, чем SSD ;
- ударопрочность SSD накопителей превышает ударопрочность HDD в 23 раза в режиме работы и в 4 раза в режиме хранения информации ;
- отсутствие какого-либо шума во время работы твердотельных накопителей объясняется отсутствием подвижных частей конструкции (в отличие от HDD);
- физические размеры и вес HDD значительно превышает твердотельный аналог;
- большее значение в данных тактовой частоты и снижение длительности импульса SSD свидетельствует о достаточно быстром обмене данными накопителя;
- получение информативных частот при измерении HDD свидетельствует о реальной угрозе утечки информации по каналу ПЭМИН;
- на сегодняшний день стоимость твердотельных накопителей остается достаточно высокой по сравнению с HDD.

COMPARATIVE ANALYSIS BY ELECTROMAGNETIC RADIATION AND HDD SSD DRIVES

Nikolay Romanyukov

The main thing Management Ministry of Internal Affairs of Ukraine in Odessa region

With the advent of modern markets SSD (solid-state drive) and analyzing methods of processing information containing state secrets, there is a need to conduct a study and comparative description of the measurement side electromagnetic radiation and leads from HDD drives and solid-state analogues that can be done with complex AKOR-2PK.

Digital multi-function search- measuring system implemented by identifying radio emission . AKOR - 2PK is a spectrum analyzer and measurement receiver is highly selective for the frequency range from 10 Hz to 3000 MHz. According to a set of operational documentation provides:

- measure the voltage generated by different devices PEMVN low current technology (personal computers , office equipment, communications equipment);
- measurement of the electric (E) and magnetic (H) fields (for connecting the measuring antenna);
- measurement of current (for connecting the measuring current collector).

Through measuring the electric field component using the method of forced activation , which is the activation of the channel reference signal conducted comparative description of the measurement of electromagnetic radiation from the side SSD and HDD storage and obtained the following results:

- read-write speed of SSD drives several times the speed read-write HDD;
- HDD drives in operation consumes almost 2 times more energy than the SSD;
- shockproof SSD drives HDD shockproof than 23 times when working 4 times using storage media;
- the absence of any noise during the SSD due to the lack of moving parts design, in contrast to the HDD;
- physical size and weight significantly higher than HDD solid state analog;
- very significant advantage in the data and reduce the clock frequency pulse width SSD show a fast exchange of data storage;
- receive informative frequencies while measuring HDD constitutes a real threat of information leakage channel PEMVN;

- today cost solid state drive is quite high compared to HDD.

УДК 681.350

АЛГОРИТМ АНАЛІЗУ ФІЗИЧНИХ ПРОЦЕСІВ ТА ДІАГНОСТИЧНА МОДЕЛЬ ТРАНЗИСТОРА В КЛЮЧОВОМУ РЕЖИМІ

Микола Жердев, Василь Кузавков
ВІТІ ДУТ

Стаття: ***6 стор., 4 джерела.***

Формальний опис об'єкту діагностування (ОД), що дає можливість розрахунку діагностичного параметру ОД на етапі проектування, називається діагностичною моделлю. Цифрові блоки, які складають основу радіоелектронної техніки (РЕТ) систем захисту інформації, віднесено до категорії складних систем, які представляються основними групами діагностичних моделей: безперервні, дискретні, гібридні, спеціальні.

За видами представлення взаємозв'язків між станом ОД, його елементами і параметрами вихідних сигналів методи синтезу моделей поділяються на аналітичні, графоаналітичні, функціонально-логічні і інформаційні.

Математичні і інформаційні моделі використовуються головним чином при проектуванні засобів і систем технічного діагностування складних об'єктів. Виходячи з розглянутого та враховуючи особливості побудови радіоелектронного компоненту (РЕК) цифрового блоку РЕТ для визначення його технічного стану (ТС) запропоновано використовувати математичну модель.

Цифрові блоки РЕТ складаються з напівпровідникових РЕК, основою яких е активні елементи. Тому розглянута модель транзистора, що працює в ключовому режимі.

Для визначення діагностичних параметрів транзистора, його діагностичну модель (ДМ) розроблено з урахуванням процесів, що в ньому відбуваються. Дані процеси можуть бути проаналізовані за допомогою моделей, які враховують електрофізичні та фізико-хімічні властивості транзистора залежно від часу напрацювання. Знання цих властивостей дозволяє використовувати безконтактний індукційний метод для діагностування та прогнозування ТС цифрових блоків.

Для побудови ДМ транзистора в активному режимі роботи використано класичні моделі Еберса-Мола, Бьюфойя-Спаркса, Лінвілла та розроблено відповідний алгоритм.

Аналіз процесів в транзисторі проведено при наступних припущеннях:

- тип транзистора n-p-n;
- в області бази створено поле що прискорює;
- домішки в базі вздовж вісі X (вісь, перпендикулярна переходам) розподілені за експонентним законом;
- колекторний перехід характеризується дифузійним механізмом переносу носіїв;
- емітерний перехід вважається різким, а колекторний плавним;
- модель транзистора в активному режимі одновимірна.

Розглянуто дві складові одновимірної моделі транзистора в активному режимі:

а) стаціонарна складова;

б) складова, що описує процес старіння.

Алгоритм надає змогу визначити ДМ транзистора в ключовому режимі роботи у вигляді залежностей струму $I_к$ від його електрико-фізичних та фізико-хімічних параметрів.

В ключовому режимі колекторний та емітерний переходи зміщені в прямому напрямку. При інжекції носіїв в базу їх надлишкова концентрація викликає збільшення базового струму. Падіння напруги на опорі бази, що створене за рахунок протікання струму бази, приводить до перерозподілу густини струму по поверхні переходу.

Аналіз процесів проведено наступним чином:

- отримано двовимірну функцію розподілу концентрації носіїв в базі;
- визначено густини струмів;
- проведено перехід до струму насиченого транзистора.

АЛГОРИТМ АНАЛИЗА ФИЗИЧЕСКИХ ПРОЦЕСОВ И ДИАГНОСТИЧЕСКАЯ МОДЕЛЬ ТРАНЗИСТОРА В КЛЮЧЕВОМ РЕЖИМЕ

Николай Жердев, Василий Кузавков
ВИТИ ГУТ

Формальное описание объекта диагностирования (ОД), дающее возможности расчета диагностического параметра ОД на этапе проектирования, называется диагностической моделью. Цифровые блоки, являющиеся основой радиоэлектронной техники (РЕТ) систем защиты информации, отнесены в категорию сложных систем, которые в свою очередь представляются основными группами диагностических моделей: непрерывные, дискретные, гибридные, специальные.

По видами представления взаимосвязей между состоянием ОД, его элементами и параметрами выходных сигналов методы синтеза моделей разделяются на аналитические, графоаналитические, функционально - логические и информационные.

Математические и информационные модели используются главным образом при проектировании средств и систем технического диагностирования сложных объектов. Исходя из рассмотренного и с учетом особенностей построения радиоэлектронного компонента (РЕК) цифрового блока РЕТ для определения его технического состояния (ТС) предложено использовать математическую модель.

Цифровые блоки РЕТ состоят из полупроводниковых РЕК, основой которых есть активные элементы. Поэтому рассматривается модель транзистора работающего в ключевом режиме.

Для определения диагностических параметров, разработана диагностическая модель транзистора (ДМ) учитывающая протекающие в нем процессы. Эти процессы могут быть проанализированы с помощью моделей, учитывающих электрофизические и физико-химические особенности транзистора в зависимости от времени наработки. Знание этих особенностей позволяет использовать бесконтактный индукционный метод для диагностирования и прогнозирования ТС цифровых блоков.

Для построения ДМ транзистора в активном режиме работы использованы классические модели Еберса-Мола, Бьюфойя-Спаркса, Линвилла и разработан соответствующий алгоритм.

Анализ процессов в транзисторе проведен при следующих допущениях:

- тип транзистора n-p-n;
- в области базы создано ускоряющее поле;
- примеси в базе вдоль оси X (ось, перпендикулярная переходам) распределены по экспоненциальному закону;
- коллекторный переход характеризуется диффузионным механизмом переносу носителей;
- эмиттерный переход считается резким, а коллекторный плавным;
- модель транзистора в активном режиме одномерна.

Рассмотрены две составляющие одномерной модели транзистора в активном режиме:

а) стационарная составляющая;

б) составляющая, описывающая процесс старения.

Алгоритм дает возможность определить ДМ транзистора в ключевом режиме роботы в виде зависимостей тока $I_к$ от его электрофизических и физико-химических параметров.

В ключевом режиме коллекторный и эмиттерный переходы смещены в прямом направлении. При инжекции носителей в базу их излишняя концентрация вызывает увеличение базового тока. Падение напряжения на сопротивлении базы, вызванное протеканием тока базы, приводить к перераспределению плотности тока по поверхности перехода.

Анализ процессов проведен следующим образом:

- получена двухмерная функция распределения концентрации носителей в базе;
- определена плотность тока;
- осуществлен переход к току насыщенного транзистора.

ANALYSIS ALGORITHM PHYSICS PROCESS AND DIAGNOSTIC TRANSISTOR MODEL IN KEYING MODE

Nikolai Zherdev, Vasily Kuzavkov
VITI GUT

Formal description diagnosis (DD), which gives the possibility to calculate the diagnostic parameter DD at the design stage, called the diagnostic model. Digital blocks, which are the basis of radioelectronic technology (RET), categorized as complex systems, which in turn represent the main groups of diagnostic models : continuous, discrete, hybrid, special.

By species representing relationships between the state of DD, its elements and parameters of the output signals of the synthesis methods are divided into analytical models, Graphic analytical, functional - and logical information.

Mathematical and information models are mainly used in the design of tools and systems for technical diagnostics of complex objects. From a consideration and taking into account peculiarities of constructing electronic component (CEC) digital PET unit to determine whether it is proposed to use the TC mathematical model.

Digital RET blocks consist of semiconductor rivers, the basis of which there are active elements. Therefore, a model of the transistor operates in key mode.

To determine the diagnostic parameters, developed diagnostic transistor model (TM) takes into account the processes taking place in it. These processes can be analyzed using models that take into account electrical and physico - chemical characteristics of the transistor according to the time of use. Knowledge of these characteristics enables contactless inductive method for diagnosing and predicting TS digital blocks.

To construct DM transistor in active mode of operation used classical models Ebersa Mola, Byufoyya -Sparks , Linville and developed appropriate algorithm.

Analysis of the processes carried out in the transistor with the following assumptions:

• type of transistor n-p-n;
• in the field of database created by the accelerating field;
• impurities in the base along the axis X (axis perpendicular transitions) is exponentially distributed;
• collector junction characterized by the diffusion mechanism of transport vehicles;
• emitter junction is considered to be sharp and smooth manifold;
• model of the transistor in the active mode is one-dimensional .

We consider two -dimensional model of the components of a transistor in the active mode:

a) stationary component;

b) component, describing the aging process.

Algorithm makes it possible to determine the DM transistor in key mode robots as dependencies of its current electricity - physical and physical - chemical parameters.

In key mode collector and emitter junction is shifted forward. Injection of carriers into the base of their excessive concentration causes an increase in the base current. The voltage drop across the base resistance caused by the flow of base current drive to the redistribution of current density at the junction surface.

Analysis of the processes carried out as follows:

- received a two-dimensional distribution function of the carrier concentration in the database;
- determined the current density;
- the transition to the saturation current of the transistor.

УДК 681.3.067

ДОСЛІДЖЕННЯ СТАТИСТИЧНОЇ БЕЗПЕКИ МЕТОДУ АВТЕНТИФІКАЦІЇ СТОРІН ВЗАЄМОДІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Юрій Яремчук
Вінницькій національний технічний університет

Стаття: ***9 стр., 12 джерел.***

Існуючи на сьогодні методи автентифікації сторін взаємодії Фіата-Шаміра, Фейге-Фіата-Шаміра, Гіллоу-Куіскуотера, Шнорра та інші базуються на операції піднесенні до степеня, яка вимагає виконання досить складних обчислень, що впливає на швидкість роботи методу при його практичній реалізації, окрім того

актуальним залишається підвищення стійкості схем автентифікації. В зв'язку з цим певний інтерес викликають методи автентифікації сторін взаємодії, що базуються на математичному апараті рекурентних U_k та V_k –послідовностей, які забезпечують спрощення обчислень. Серед цих методів особливий інтерес викликає метод автентифікації на основі математичного апарату V_k –послідовностей, який, порівняно з іншими методами, що базуються на рекурентних U_k та V_k –послідовностях, забезпечує підвищення стійкості за рахунок введення в схему автентифікації додаткового сеансового ключа з боку претендента. Проведено дослідження статистичної безпеки методу автентифікації сторін взаємодії на основі рекурентних V_k –послідовностей та здійснено його порівняння з відомими методами Шнорра, Фіата-Шаміра та Фейге-Фіата-Шаміра. Для дослідження статистичної безпеки використано пакет NIST STS, який на сьогодні є одним з кращих пакетів для статистичного тестування криптографічних схем та протоколів. Тестування проводилось для різних довжин ключів, а саме 512, 768 та 1024 бітів. Результати аналізу показали, що в цілому метод на основі V_k –послідовностей має стабільно високі показники, характеризуючи його з кращого боку щодо статистичної безпеки. Особливо це стосуються малих довжин ключів, що, в першу чергу, рекомендує його застосування в системах автентифікації, для яких використання великих ключів не є важливим.

ИССЛЕДОВАНИЕ СТАТИСТИЧЕСКОЙ БЕЗОПАСНОСТИ МЕТОДА АУТЕНТИФИКАЦИИ СТОРОН ВЗАИМОДЕЙСВТИЯ НА ОСНОВЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Юрий Яремчук
Винницкий национальный технический университет

Существующие на сегодня методы аутентификации сторон взаимодействия Фиата-Шамира, Фейге-Фиата-Шамира, Гиллоу-Куискуотера, Шнорра и другие базируются на операции возведения в степень, которая требует выполнения достаточно сложных вычислений, что влияет на скорость работы метода при его практической реализации, кроме того актуальным остаётся повышение стойкости схем аутентификации. В связи с этим определённый интерес вызывают методы аутентификации сторон взаимодействия, базирующиеся на математическом аппарате рекуррентных U_k и V_k –последовательностей, которые обеспечивают упрощение вычислений. Среди этих методов особый интерес вызывает метод аутентификации на основе математического аппарата V_k –последовательностей, который, по сравнению с другими методами, базирующимися на рекуррентных U_k и V_k –последовательностях, обеспечивает повышение стойкости за счёт введения в схему аутентификации дополнительного сеансового ключа со стороны претендента. Проведено исследование статистической безопасности метода аутентификации сторон взаимодействия на основе рекуррентных V_k –последовательностей и осуществлено его сравнение с известными методами Шнорра, Фиата-Шамира и Фейге-Фиата-Шамира. Для исследования статистической безопасности использовано пакет NIST STS, который на сегодня является одним из лучших пакетов для статистического тестирования криптографических схем и протоколов. Тестирование проводилось для разных длин ключей, а именно 512, 768 и 1024 бит. Результаты анализа показали, что в целом метод на основе V_k – последовательностей имеет стабильно высокие показатели, характеризующие его с лучшей стороны в отношении статистической безопасности. Особенно это касается малых длин ключей, что, в первую очередь, рекомендует его применение в системах аутентификации, для которых использование больших ключей не является важным.

RESEARCH A STATISTICAL SECURITY OF METHOD OF AUTHENTICATION THE PARTIES INTERACTION BASED ON RECURRENT SEQUENCES

Iurii Iaremchuk
Vinnytsia national technical university

Existing methods of authentication of the parties interact, in particular Fiat-Shamir, Feige-Fiat-Shamir, Guillou-

Quisquater, Schnorr and others are based on exponentiation operation which requires performing complex calculations that affect the speed of the method in its practical implementation also remains relevant increase in the durability of authentication schemes. Therefore, a certain interest is the methods of authentication the parties interaction, based on the mathematical apparatus of recurrent U_k and V_k sequences that allow for simplification of the calculations. Among these methods of particular interest is the authentication method based on the mathematical apparatus V_k sequences, which, compared to other methods based on recurrent U_k and V_k sequences, provides increased resistance due by introducing of the additional session key to the authentication scheme on the part of the applicant. The research are conducted for statistical security of the method of authentication the parties interaction based on recurrent V_k sequences and made his comparison with well-known Schnorr, Fiat-Shamir and Feige-Fiat-Shamir methods. To investigate the statistical package used security NIST STS, which today is one of the best packages for statistical testing of cryptographic schemes and protocols. Testing was conducted for different key lengths, namely 512, 768 and 1024 bits. Results of analysis showed that the overall method based on V_k sequences has consistently high scores, characterizing his best side on the statistical security. This is especially concerning for small lengths of keys that, first and foremost, recommends its use in authentication systems, which use large keys is not important.

УДК 004.056

АНАЛІЗ МІЖНАРОДНОГО ДОСВІДУ ЩОДО ВИЗНАЧЕННЯ КЛЮЧОВИХ СИСТЕМ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

Юрій Васильєв
ДержНДІ Спецзв'язку

Стаття: ***5 стор., 3 джерела.***

У кожному суспільстві можливо виділити сектори, системи або мережі, від яких життєво залежить суспільство і порушення функціонування яких може привести до колапсу на загальнодержавному, регіональному або місцевому рівні. Комплекс цих секторів, систем або мереж почали називати ключовими або критичними системами інформаційної інфраструктури (далі - КСІІ).

Багато держав, а також терористичних та кримінальних структур інтенсивно вдосконалюють методи і способи використання інформаційних технологій та засобів для деструктивних інформаційних впливів на інформаційні ресурси інформаційно-телекомунікаційних систем і мереж державних та недержавних організацій. Таке застосування інформаційних технологій та засобів надає їм властивості так званої інформаційної зброї. Для нанесення значного збитку інтересам держави і суспільства інформаційна зброя може бути застосована і в мирний час, особливо терористичними організаціями. При цьому порушення функціонування КСІІ може призвести до розвитку надзвичайних ситуацій, пов'язаних із загибеллю людей, екологічними катастрофами, нанесенням великої матеріальної, фінансової, економічної шкоди або великомасштабними порушеннями життєдіяльності міст та населених пунктів і т. п. У цих умовах важливу роль відіграє державне регулювання діяльності щодо забезпечення безпеки інформації в КСІІ.

АНАЛИЗ МЕЖДУНАРОДНОГО ОПЫТА ПО ОПРЕДЕЛЕНИЮ КЛЮЧЕВЫХ СИСТЕМ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Юрий Васильев
ГосНИИ Спецсвязи

В каждом обществе можно выделить сектора, системы или сети, от которых жизненно зависит общество и нарушение функционирования которых может привести к коллапсу на общегосударственном, региональном и местном уровнях. Комплекс этих секторов, систем или сетей стали называть ключевыми или критическими системами информационной инфраструктуры (далее - КСИИ). Многие зарубежные государства, а также террористические и криминальные структуры интенсивно совершенствуют методы и способы использования информационных технологий и средств для деструктивных информационных воздействий на информационные ресурсы информационно-телекоммуникационных систем и сетей государственных и негосударственных организаций. Такое применение информационных технологий и

средств придает им свойства так называемого информационного оружия. Для нанесения значительного ущерба интересам государства и общества информационное оружие может быть применено и в мирное время, особенно террористическими организациями. При этом нарушения функционирования КСИИ может привести к развитию чрезвычайных ситуаций, связанных с гибелью людей, экологическими катастрофами, нанесением большого материального, финансового, экономического ущерба или крупномасштабными нарушениями жизнедеятельности городов и населенных пунктов и т.п. В этих условиях важную роль играет государственное регулирование деятельности по обеспечению безопасности информации в КСИИ.

ANALYSIS OF INTERNATIONAL EXPERIENCE TO IDENTIFY KEY SYSTEMS OF INFORMATION INFRASTRUCTURE

Iurii Vasyliev
SRI for STIP

In every society can be identified sector, system or network on which life depends on society and the malfunction of which may lead to a collapse at the national, regional and local levels. The complex of these sectors, systems or networks began calling key or critical systems of infrastructure information (hereinafter - KSII). Many foreign countries, as well as terrorist and criminal organizations intensively improve their methods and how to use information technology and information for the destructive impacts on information resources of information technology systems and networks of governmental and nongovernmental organizations. Such use of information technology and gives them the properties of so-called information warfare. Significant damage to the interests of the state and society, information weapons may be used in peacetime, especially terrorist organizations. At the same malfunctions KSII can lead to emergencies involving loss of life, environmental disasters, causing great material, financial, economic damage or large-scale violations of the life of cities and towns, etc. In these circumstances, an important role is played by state regulation of information security in the KSII.

УДК 621.396

ОСОБЛИВОСТІ ПРОЕКТУВАННЯ РАЦІОНАЛЬНОЇ СТРУКТУРИ ЦИФРОВИХ МЕРЕЖ ЗВ'ЯЗКУ

Дмитро Могилевич, Микола Фомін
ВІТІ ДУТ

Стаття: ***7 стор., 10 джерел.***

В останні роки зросла кількість системних розробок, мета яких полягає у визначенні раціональної (оптимальної) структури мережі зв'язку. З'явилася необхідність у налагодженні комплексу технічних засобів, алгоритмів функціонування, програмного забезпечення мереж зв'язку на високому науково-технічному рівні. Досвід показує, що вирішення цих складних задач за допомогою інтуїції або шляхом проведення простих розрахунків потрібного результату не дає. При такому підході на завершальному етапі проектування, як правило, витрачається багато засобів і часу на переробку, доопрацювання, налагодження та проведення інших зайвих операцій. У зв'язку з цим постає питання про розробку математичного апарату, алгоритмів, програм для проведення необхідних розрахунків і проектування мереж зв'язку за допомогою ПЕОМ. Можливі наступні варіанти при проектуванні мереж зв'язку – за допомогою аналітичних чи імітаційних моделей. Мережа зв'язку відноситься до класу складних технічних систем, тому їм притаманні всі особливості і труднощі теоретичних досліджень такого класу систем. Мережа зв'язку є багатопараметричною системою. Важкість постановки та вирішення задачі раціонального (оптимального) проектування мережі обумовили розробку низки математичних моделей, кожна з яких дозволяє вирішити яку-небудь конкретну задачу оптимізації за обраним критерієм.

Тому під час практичного застосування задачі оптимізації структури (топології) відносяться до підкласу таких екстремальних пошукових задач, для яких не доказано існування методів пошуку рішень, що забезпечують отримання оптимуму за час, обмежений поліномом від розмірності N задач. Більш того, отримання хоча б одного такого методу для будь-якої задачі із даного підкласу означало би можливість отримання оптимуму будь-якій задачі із даного підкласу за поліноміальний (від N) час.

ОСОБЕННОСТИ ПРОЕКТИРОВАНИЯ РАЦИОНАЛЬНОЙ СТРУКТУРЫ ЦИФРОВЫХ СЕТЕЙ СВЯЗИ

Дмитрий Могилевич, Николай Фомин
ВИТИ ГУТ

В последние годы возросло количество системных разработок, цель которых заключается в определении рациональной (оптимальной) структуры сети связи. Появилась необходимость в налаживании комплекса технических средств, алгоритмов функционирования, программного обеспечения сетей связи на высоком научно - техническом уровне. Опыт показывает, что решение этих сложных задач с помощью интуиции или путем проведения простых расчетов нужного результата не дает. При таком подходе на завершающем этапе проектирования, как правило, тратится много средств и времени на переработку, доработку, настройку и проведение других лишних операций. В связи с этим встает вопрос о разработке математического аппарата, алгоритмов, программ для проведения необходимых расчетов и проектирования сетей связи с помощью ЭВМ. Возможны следующие варианты при проектировании сетей связи – с помощью аналитических или имитационных моделей. Сеть связи относится к классу сложных технических систем, поэтому им присущи все особенности и трудности теоретических исследований такого класса систем. Сеть связи является многопараметрической системой. Сложность постановки и решения задачи рационального (оптимального) проектирования сети обусловили разработку целого ряда математических моделей, каждая из которых позволяет решить какую-либо частную задачу оптимизации по выбранному критерию.

Поэтому во время практического применения задачи оптимизации структуры (топологии) относятся к подклассу таких экстремальных поисковых задач, для которых не доказано существование методов поиска решений, обеспечивающих получение оптимума за время, ограниченное полиномом от размерности N задач. Более того, получение хотя бы одного такого метода для любой задачи из данного подкласса означало бы возможность получения оптимума любой задачи из данного подкласса за полиномиальное (от N) время.

DESIGN FEATURES RATIONAL STRUCTURE OF DIGITAL COMMUNICATION NETWORKS

Dmitro Mogilevich, Mykola Fomin
MITI SUT

In recent years an increasing number of system development, the aim of which is to determine the rational (optimal) network structure. Now you need to establish a set of technical means, functioning algorithms, software networks based on high scientific - technical level. Experience shows that the solution to these challenges through intuition or by simple calculation does not give the desired result. With this approach, the final design stage usually spent a lot of money and time for processing, handling, setting and carrying out other unnecessary operations. In this regard, the question arises about the development of the mathematical apparatus, algorithms, programs for the necessary calculations using a computer for analysis and design of communication networks. The following options for the design of communication networks - using analytical or simulation models. The communication network is a class of complex technical systems , so it has all the features and difficulties of theoretical studies of this class of systems . Communication network is a multi-parameter system. Complexity of formulating and solving the problem of rational (optimal) network design led to the development of a number of mathematical models, each of which allows you to solve any particular problem of optimization of the selected criteria.

Therefore, during the practical application of the optimization problem of structure (topology) belong to a subclass of such extreme search tasks that do not prove the existence of methods to search for solutions that provide optimum receive in time bounded by a polynomial in N-dimensional problems. Moreover, obtaining at least one such method for any problem of this subclass would mean the possibility of obtaining the optimum any problem of this subclass in polynomial (as N) time.

УДК 621.396.4

НЕКОТОРЫЕ РЕЗУЛЬТАТЫ НАТУРНЫХ ИССЛЕДОВАНИЙ МАКЕТА ПРИЕМНОГО МОДУЛЯ СТАНЦИИ ТРОПОСФЕРНОЙ СВЯЗИ НОВОГО ПОКОЛЕНИЯ

Андрей Демаш, Андрей Паламарчук, Сергей Усенко, Алексей Юдин, Сергей Мазор*
*ГосНИИ Спецсвязи, *ИССЗИ НТУУ «КПІ»*

Стаття: ***6 стор., 3 джерела.***

Среди всех видов связи тропосферная связь является одной из наиболее сложной для технической реализации. Эта сложность обусловлена природой распространения радиоволн, которая характеризуется своими случайными параметрам и значительными энергетическими потерями на трассе распространения.

Одним из основных параметров, определяющим энергетическую эффективность сигнала, является минимальное возможное отношение энергии сигнала к спектральной плотности мощности шума (h^2) при заданной вероятности ошибки. Проведенные лабораторные исследования показали, что минимизация h^2 возможна при использовании составных многопозиционных шумоподобных сигналов (СМПШПС) и их двухступенчатой обработке. В первой ступени производится когерентная обработка сигнала в целом на радиочастоте с последующей его обработкой по алгоритму Витерби с перемежением. Следует отметить, что расчеты радиолинии тропосферной связи с использованием шумоподобных сигналов (ШПС) или СМПШПС в литературе отсутствуют.

Натурные исследования проводились с целью:

- определения эффективности предложенного способа обработки сигнала и подтверждения результатов лабораторных исследований, проведенных в канале с постоянными параметрами;
- проверки возможности использования модемов спутниковой связи, работающих со сверточным кодированием по алгоритму Витерби с перемежением, как составной части модема станции тропосферной связи нового поколения;
- получения результатов измерений h^2, необходимых для расчета радиолинии тропосферной связи при использовании СМПШПС и минимизации базы ШПС.

По результатам исследований сделаны выводы о том, что:

- полученные экспериментальным путем результаты хорошо совпадают с расчетными значениями h^2, что в свою очередь подтверждает возможность использования современных модемов спутниковой связи как составной части для обработки сигналов в станциях тропосферной связи нового поколения;
- предложенный способ обработки СМПШПС дает положительный эффект.

ДЕЯКІ РЕЗУЛЬТАТИ НАТУРНИХ ДОСЛІДЖЕНЬ МАКЕТУ ПРИЙМАЛЬНОГО МОДУЛЮ СТАНЦІЇ ТРОПОСФЕРНОГО ЗВ'ЯЗКУ НОВОГО ПОКОЛІННЯ

Андрій Демаш, Андрій Паламарчук, Сергій Усенко, Олексій Юдін, Сергей Мазор*
*ДержНДІ Спецзв'язку, *ІСЗЗІ НТУУ «КПІ»*

Серед усіх видів зв'язку тропосферний зв'язок є одним з найбільш складних для технічної реалізації. Ця складність обумовлена природою поширення радіохвиль, яка характеризується своїми випадковими параметрами та значними енергетичними втратами на трасі поширення.

Одним із основних параметрів, який визначає енергетичну ефективність сигналу, є мінімально можливе відношення енергії сигналу до спектральної щільності потужності шуму (h^2) при заданій ймовірності похибки. Проведені лабораторні дослідження показали, що мінімізація h^2 можлива при використанні складових багатопозиційних шумоподібних сигналів (СБПШПС) та їх двохступеневої обробці. В першій ступені здійснюється когерентна обробка сигналу в цілому на радіохвилі з наступною його обробкою за алгоритмом Вітербі з перемежуванням. Необхідно відмітити, що розрахунки радіолінії тропосферного зв'язку з використанням шумоподібних сигналів (ШПС) чи СБПШПС в літературі відсутні.

Натурні дослідження проводились з метою:

- визначення ефективності запропонованого способу обробки сигналу та підтвердження результатів лабораторних випробувань, які були проведені в каналі з постійними параметрами;

- перевірки можливості використання модемів супутникового зв'язку, які працюють зі згортковим кодуванням за алгоритмом Вітербі з перемежуванням як складової частини модему станції тропосферного зв'язку нового покоління;

- отримання результатів вимірювань h^2, необхідних для розрахунку радіолінії тропосферного зв'язку при використанні СБПШПС та мінімізації бази ШПС.

За результатами досліджень зроблені висновки про те, що:

- отриманні експериментальним шляхом результати добре збігаються з розрахунковими значеннями h^2, що в свою чергу підтверджує можливість використання сучасних модемів супутникового зв'язку як складової частини для обробки сигналів в станції тропосферного зв'язку нового покоління;

- запропонований спосіб обробки СБПШПС дає позитивний ефект.

SOME INFORMATION ABOUT FIELD RESEARCH STATION RECEIVER MODULE LAYOUT TROPOSPHERIC COMMUNICATION OF NEW GENERATION

Andriy Demash, Andriy Palamarchuk, Sergiy Usenko, Oleksii Yudin, Sergiy Mazor*
*SRI for STIP, *ISCDI NTUU «KPI»*

Among all types of communications, tropospheric communication is one of the most difficult for the technical realization. This complexity is due to the nature of radio wave propagation, which is characterized by its random parameters and significant energy losses in the propagation path.

One of the main parameters determining the energy efficiency of the signal is the minimum possible ratio of signal energy to noise power spectral density (h2) for a given probability of error. The laboratory studies have shown that minimizing h2 possible using composite multiposition noise-like signals (CMNLS) and their two-stage processing. In the first stage of the coherent signal processing is performed on the radio frequency as a whole with its subsequent processing Viterbi interleaved. It should be noted that the calculation of tropospheric radio connection with the use of noise-like signals (NLS) or CMNLS in the literature.

Field investigations were carried out in order to:

- Determine the effectiveness of the proposed signal processing method and confirm the results of laboratory studies conducted in a channel with constant parameters;

- Test the feasibility of using satellite communications modems working Convolutional Codes Viterbi interleaved as part of modem tropospheric communication station of the new generation;

- Obtain measurements h2, needed to calculate the tropospheric radio communications using CMNLS and minimize database NLS.

According to the research conclusions that:

- Obtained by experimental results agree well with the calculated values of h2, which in turn confirms the possibility of using modern modems satellite communications as an integral part , for processing signals in tropospheric communication stations of the new generation;

- The proposed method for processing CMNLS a positive effect.

УДК 004.056.5

СТРУКТУРА МОДЕЛИ ИНТЕЛЛЕКТУАЛЬНЫХ ЭЛЕКТРОЭНЕРГЕТИЧЕСКИХ СИСТЕМ, УЧИТЫВАЮЩАЯ НЕОБХОДИМОСТЬ ОБЕСПЕЧЕНИЯ ИХ КИБЕРБЕЗОПАСНОСТИ

Алексей Юдин, Геннадий Леоненко, Сергей Гончар
ГосНИИ Спецсвязи

Стаття: ***9 стор., 8 джерел.***

В статье рассматривается общая структура интеллектуальных электроэнергетических систем на примере моделей предложенных Национальным институтом стандартов и технологий США и Украинским центром экономических и политических исследований имени Александра Разумкова. Также рассматриваются

вопросы возможности реализации эталонных моделей на базе действующей объединенной энергосистемы Украины.

Предложено взять за базовую структуру модели NIST, которая состоит из 49 объектов. Как объекты предлагается рассматривать группы устройств, системы, процессы, организации и учреждения, потребителей. Схематично представлено взаимодействие между объектами посредством 137 логических интерфейсов информационного обмена. Указанные интерфейсы сгруппированы по 22 категориям. В материалах изложено краткое описание объектов интеллектуальных электроэнергетических систем.

По результатам описания структуры модели интеллектуальных электроэнергетических систем сделаны следующие выводы

1. Описанная структура модели базируется на общих и доменно-ориентированных требованиях по снижению рисков и обеспечению совместимости решений в различных элементах инфраструктуры и позволяет создавать сложные системы с функциями предупреждения, выявления, реагирования и восстановления.

2. Использование таких понятий как “домен”, “объект домена”, “логический интерфейс” позволяют более четко провести декомпозицию энергосистемы и описать требования к обеспечению кибербезопасности ее составляющих в критериях, нормативно закрепленных в Украине, а именно “конфиденциальности”, “целостности”, “доступности” и “наблюдаемости”.

3. Достоинством предложенной структуры является то, что она позволяет выделить объекты электроэнергетической системы, к которым предъявляются повышенные требования по тем или иным критериям.

4. Представленная структура вполне реализуема посредством трансформации существующих элементов объединенной энергетической системы Украины.

СТРУКТУРА МОДЕЛІ ІНТЕЛЕКТУАЛЬНИХ ЕЛЕКТРОЕНЕРГЕТИЧНИХ СИСТЕМ, ЯКА ВРАХОВУЄ НЕОБХІДНІСТЬ ЗАБЕЗПЕЧЕННЯ ЇХ КІБЕРБЕЗПЕКИ

Олексій Юдін, Геннадій Леоненко, Сергій Гончар

ДержНДІ Спецзв’язку

В статті розглядається загальна структура інтелектуальних електроенергетичних систем на прикладі моделей, запропонованих Національним інститутом стандартів і технологій США та Українським центром економічних і політичних досліджень імені Олександра Разумкова. Також розглядаються питання можливості реалізації еталонних моделей на базі діючої об’єднаної енергосистеми України.

Запропоновано взяти за базову структуру моделі NIST, яка складається з 49 об’єктів. Як об’єкти пропонується розглядати групи пристроїв, системи, процеси, організації та заклади, споживачів. Схематично наведена взаємодія між об’єктами через 137 логічних інтерфейсів інформаційного обміну. Зазначені інтерфейси згруповані за 22 категоріями. В матеріалах викладений скорочений опис об’єктів інтелектуальних електроенергетичних систем.

За результатами опису структури моделі інтелектуальних електроенергетичних систем зроблені наступні висновки

1. Описана структура моделі базується на загальних та доменно-орієнтованих вимогах до зниження ризиків і забезпечення сумісності рішень в різних елементах інфраструктури та дозволяє утворювати складні системи з функціями попередження, виявлення, реагування та відновлення.

2. Використання таких понять як “домен”, “об’єкт домену”, “логічний інтерфейс” дозволяє чіткіше провести декомпозицію енергосистеми та зробити опис вимог щодо забезпечення кібербезпеки її складових в критеріях, нормативно закріплених на Україні, а саме: “конфіденційності”, “цілісності”, “доступності” і “спостереженості”.

3. Перевагою запропонованої структури є те, що вона дозволяє виділити об’єкти електроенергетичної системи, до яких висуваються підвищені вимоги за тими чи іншими критеріями.

4. Наведена структура придатна до реалізації шляхом трансформації існуючих елементів об’єднаної енергетичної системи України.

STRUCTURE OF THE MODEL OF INTELLIGENCE POWER INDUSTRY SYSTEMS CONSIDERING NECESSITY TO SAFEGUARD THEIR CYBERSECURITY

Oleksii Yudin, Gennadii Leonenko, Sergii Gonchar
SRI for STIP

The article deals with the general structure of intelligent electricity systems on the example models proposed by the National Institute of Standards and Technology and the Ukrainian Centre for Economic and Political Studies named Alexander Razumkov. Also addresses the feasibility of reference models based on the existing unified energy system of Ukraine.

Asked to take over the base, NIST model structure which consists of 49 objects. As objects proposed to consider a group of devices, systems, processes, organizations and institutions, consumers. Schematic representation of the interaction between objects by 137 logical interfaces for information exchange. These interfaces are grouped into 22 categories. The materials set forth a brief description of the objects of intellectual power systems.

According to the results describe the structure model of intelligent electricity systems to the following conclusions:

1. Described structure of the model is based on general and domain-specific requirements to reduce risks and ensure the compatibility of solutions in various infrastructure elements and allows you to create complex systems with functions of prevention, detection, response and recovery.

2. The use of such concepts as "domain", "domain object", "logical interface" allow to spend more clearly describe the decomposition of the power system and cyber security requirements of its components in the regulatory criteria set forth in Ukraine, namely "confidentiality", "integrity", "accessibility" and "observability".

3. The advantage of the proposed structure is that it allows you to select objects of electric power systems to which the increased requirements on certain criteria.

4. The framework presented is quite realistic by transforming existing elements united energy system of Ukraine.

УДК 621.396.67

ФУНКЦІЯ УСПІШНОСТІ ЗАХИСТУ ЕЛЕКТРОННОЇ АПАРАТУРИ ВІД ЗОВНІШНІХ ФАКТОРІВ

Борис Уваров, Юрій Зіньковський
Національний технічний університет України "КПІ"

Стаття: ***8 стор., 12 джерел***

Актуальна задача створення сучасних конструкцій радіоелектронних апаратів (РЕА) – розробка методів проектування, заснованих на використанні математичного апарату теорії ймовірності, що давало б можливість прогнозувати межі розсіювання функціональних характеристик реального РЕА, отриманих в результаті проектування.

Радіоелектронна апаратура завжди працює під дією різних зовнішніх впливів - електромагнітних, механічних, теплових, які можуть порушити нормальне її функціонування або призвести до відмов. Серед таких впливів можуть бути і навмисні (вжиті конкуруючою стороною), з метою вивести РЕА з ладу.

Створення таких складних технічних об'єктів, якими є РЕА, неможливо без використання систем автоматизованого проектування (САПР), що представляють собою комплекс взаємодії продуктів відповідних комп'ютерних програм. Кожна САПР має власні об'єктно-орієнтовані бази даних і часто взаємодіє з зовнішніми інформаційними масивами. Тому при створенні комплексів САПР необхідно мати у їх складі також і системи захисту інформації.

Стійкість функціонування РЕА в умовах зовнішніх впливів можна оцінити за допомогою функції успішності захисту, що враховує імовірнісну природу всіх фізичних процесів, в тому числі і функціональних характеристик, і впливаючих чинників, яка запропонована такою:

$$\Phi_P^{st} = \frac{Y_{\text{ном}}^{st}\left(Q^{st}\right)}{Y_{\text{доп}}^{st}}\left(1+\delta Y_m^{st}\right),$$

де $Y^{st}_{ном}$ – номінальне значення функціональної характеристики Y; $Y^{st}_{доп}$ – допустиме її значення; Q^{st} – значення зовнішнього фактора; δY^{st}_{m} – допуск на відхилення характеристики Y від номінального значення;

верхній індекс "*st*" позначає стохастичность всіх фізичних величин та процесів.

На основі рівнянь Лагранжа другого роду, записаних з урахуванням стохастичних характеристик фізичних величин, отримано вирази для функціональних характеристик, що описують електромагнітні, механічні і теплові процеси в РЕА.

ФУНКЦИЯ УСПЕШНОСТИ ЗАЩИТЫ ЭЛЕКТРОННОЙ АППАРАТУРЫ ОТ ВНЕШНИХ ФАКТОРОВ

Борис Уваров, Юрий Зиньковский

Национальный технический университет Украины "КПИ"

Актуальная задача создания современных конструкций радиоэлектронных аппаратов (РЭА) – разработка методов проектирования, основанных на использовании математического аппарата теории вероятности, что давало бы возможность прогнозировать границы рассеяния функциональных характеристик реального РЭА, полученных в результате проектирования.

Радиоэлектронная апаратура всегда подвержена различным внешним воздействиям – электромагнитным, механическим, тепловым, которые могут нарушить нормальное её функционирование или привести к отказам. Среди таких воздействий могут быть и преднамеренные (предпринятые конкурирующей стороной), с целью вывести РЭА из строя.

Создание таких сложных технических объектов, какими являются РЭА, невозможно без использования систем автоматизированного проектирования (САПР), представляющих собой комплекс взаимодействующих компьютерных программ. Каждая САПР имеет собственные объектно-ориентированные базы данных и часто взаимодействует с внешними информационными массивами. Поэтому при создании комплексов САПР необходимо иметь в их составе также и системы защиты информации.

Устойчивость функционирования РЭА в в условиях внешних воздействий можно оценить с помощью функции успешности защиты, учитывающей вероятностную природу всех физических процессов, в том числе и функциональных характеристик, и воздействующих факторов, которая предложена такой:

$$\Phi_P^{st} = \frac{Y_{\text{ном}}^{st}\left(Q^{st}\right)}{Y_{\text{доп}}^{st}}\left(1+\delta Y_m^{st}\right),$$

где $Y^{st}_{ном}$ – номинальное значение функциональной характеристики Y; $Y^{st}_{доп}$ – допустимое ее значение; Q^{st} – значение внешнего фактора; δY^{st}_m – допуск на отклонение характеристики Y от номинального значения; верхний индекс "*st*" обозначает стохастичность всех физических величин и процессов.

На основе уравнений Лагранжа второго рода, записанных с учетом стохастических характеристик физических величин, получены выражения для функциональных характеристик, описывающих электромагнитные, механические и тепловые процессы в РЭА.

SUCCESSION PROTECTION FUNCTION OF ELECTRONIC EQUIPMENT FROM EXTERNAL FACTORS

Borys Uvarov, Yurij Zincovsky

National Technical University of Ukraine "KPI"

The current task of creating up-to-date radioelectronic devices constructions (the RED) is development of design methods based on a usage of the probability theory mathematical algorithms, which would make it possible to predict the boundary scattering functional characteristics of real RED achieved as a result design.

Radioelectronic devices always are a subject of external influences - electromagnetic, mechanical, thermal, which can disrupt the normal functionality or lead to failures. Some of these impacts may be intentional (made by an enemies or competitors) with the purpose of destroying the functionality of RED.

The creation of such complex technical objects, what are the RED, is impossible without usage of computer-aided design (the CAD), including complex interacting software. Each has its own CAD object-oriented databases and often interacts with external information arrays. Therefore, when creating the CAD systems it is necessary to have in their composition an information security systems.

Stable functionality of the RED with external influences can be estimated using the success protection function, taking into account the probabilistic nature of all physical processes, including the functional characteristics and

influencing factors, which is offered as follows:

$$\Phi_P^{st} = \frac{Y_{\text{ном}}^{st}\left(Q^{st}\right)}{Y_{\text{доп}}^{st}}\left(1+\delta Y_m^{st}\right),$$

which $Y^{st}_{ном}$ - nominal value of the Y functional characteristics; $Y^{st}_{доп}$ - its allowed value; Q^{st} - external factors importance; δY^{st}_m - tolerance deviation Y characteristics of the nominal value; superscript "*st*" means the stochastic nature of all physical values and processes. On the second kind Lagrange equations basis, recorded considering physical quantities stochastic characteristics, were obtained the expressions for the functional characteristics describing electromagnetic, mechanical and thermal processes in the RED.