4 Реферати

УДК 354:007

ІНФОРМАЦІЙНА БЕЗПЕКА: НОВІ ВИКЛИКИ УКРАЇНСЬКОМУ СУСПІЛЬСТВУ

Євген Скулиш
Національна Академія Служби безпеки України

Стаття: ***4 стор., 7 джерел.***

Інформаційна революція, що триває протягом останніх десятиріч, зумовлює кардинальні зміни в суспільстві: зароджуються нові культурні та економічні тенденції, з'являється інформаційне виробництво продукування інформації як самостійного виду товару, формуються нові види соціальної комунікації. Така сфера життя, як національна безпека, не могла залишитися поза впливом інформаційного фактору.

В умовах інформаційного суспільства всі без винятку об'єкти національної безпеки (людина, суспільство, держава) стають чутливими до інформації, яка їх оточує, що дозволяє впливати на діяльність об’єктів національної безпеки за допомогою зміни інформації, способів її обробки та передачі. На сьогодні низка факторів свідчить про зміну середовища безпеки в Україні та навколо нього, коли виникає реальна небезпека втрати керованості процесами в інформаційному протистоянні, коли майбутнє країни визначається не діями окремих особистостей, а внутрішньою логікою конфронтації. Відповідно, поглиблюється політичне усвідомлення проблем інформаційної безпеки та розширення сфери наукового інтересу до них.

Особливе місце в інформаційній сфері суспільства посідають індивідуальна, групова й масова свідомість людей, які все більшою мірою піддаються агресивним інформаційним впливам, що нерідко завдає шкоди моральному здоров'ю громадян, руйнує духовні норми життя суспільства, призводить до дестабілізації соціально-політичної обстановки. Отже, антропоцентричний підхід стає одним із пріоритетних у забезпеченні національної безпеки, а безпека людини утворює комплексну систему, яка входить як складова до метасистеми національної безпеки, і має визначати підхід до вироблення стратегії забезпечення національної безпеки.

Результати проведеного дослідження дозволяють дійти висновку, що в сучасних умовах інформаційна безпека стає органічним елементом національної безпеки, оскільки інформація перетворюється на ресурс не лише національного стратегічного, але й світового значення. Відповідно, при розробці концепцій, стратегій, цільових програм і планів дій щодо забезпечення національної безпеки України слід враховувати зміни у просторі загроз і викликів, зумовлені розширенням впливу інформаційного фактору в умовах глобалізації.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: НОВЫЕ ВЫЗОВЫ УКРАИНСКОМУ ОБЩЕСТВУ

Евгений Скулиш
Национальная Академия Службы безопасности Украины

Информационная революция, которая длится на протяжении последних десятилетий, приводит к кардинальным изменениям в обществе: зарождаются новые культурные и экономические тенденции, появляется информационное производство продуцирования информации как самостоятельного вида товара, формируются новые виды социальной коммуникации. Такая сфера жизни, как национальная безопасность, не могла остаться вне влияния информационного фактора.

В условиях информационного общества все без исключения объекты национальной безопасности (человек, общество, государство) становятся чувствительными к информации, которая их окружает, что позволяет влиять на деятельность объектов национальной безопасности с помощью изменения информации, способов ее обработки и передачи. На сегодня ряд факторов свидетельствует об изменении среды безопасности в Украине и вокруг нее, когда возникает реальная опасность потери управляемости процессами в информационном противостоянии, когда будущее страны определяется не действиями отдельных личностей, а внутренней логикой конфронтации. Соответственно, углубляется политическое осознание проблем информационной безопасности и расширения сферы научного интереса к ним.

Особое место в информационной сфере общества занимают индивидуальное, групповое и массовое сознание людей, которые всё больше подвергаются агрессивным информационным воздействиям, что нередко наносит ущерб моральному здоровью граждан, разрушает духовные нормы жизни общества, приводит к дестабилизации социально-политической обстановки. Таким образом, антропоцентрический подход становится одним из приоритетных в обеспечении национальной безопасности, а безопасность человека образовывает комплексную систему, которая входит как составляющая в метасистему национальной безопасности, и должна определять подход к разработке стратегии обеспечения национальной безопасности.

Результаты проведенного исследования позволяют прийти к выводу, что в современных условиях информационная безопасность становится органическим элементом национальной безопасности, поскольку информация превращается в ресурс не только национального стратегического, но и мирового значения. Соответственно, при разработке концепций, стратегий, целевых программ и планов действий относительно обеспечения национальной безопасности Украины нужно учитывать изменения в пространстве угроз и вызовов, обусловленные расширениям влияния информационного фактора в условиях глобализации.

INFORMATIONAL SECURITY: NEW CHALLENGES TO THE UKRAINIAN SOCIETY

Eugene Skulish
The National Academy Security Service of Ukraine

Information revolution which take place throughout last decades, predetermines cardinal changes in a society: new cultural and economic tendencies arise, there is the news production of the producing information as an independent product, new kinds of social communications form. Such sphere of life as national safety could not remain out of influence of the information factor.

In the conditions of an information society all without an exception objects of national safety (the person, the society, the state) become sensitive to the information which surrounds them that allows to influence activity of objects of national safety by means of change of the information, ways of its processing and transfer. Today a number of factors testifies to change of the environment of safety in Ukraine and round it when there is a real danger of loss of controllability processes in information opposition when the country future is defined not by actions of separate persons, and internal logic of confrontation. Accordingly, political comprehension of problems of information safety and expansion of sphere of scientific interest to them goes deep.

Special place in information sphere of society occupies individual, group and mass consciousness of people which are exposed to aggressive information influences which quite often cause a damage to moral health of citizens more and more, destroy spiritual norms of life of society, lead to destabilizations of sociopolitical conditions. Thus, the anthropocentric approach becomes one of priority in maintenance of national safety, and safety of the person forms the complex system which is included as a component into metasystem of the national safety, and should define the approach to working out of the strategy of maintenance of the national safety.

Results of the research allow to come to the conclusion, that in modern conditions information safety becomes an organic element of the national safety as the information turns to a resource not only national strategic, but also world value. Accordingly, by working out of concepts, strategies, target programs and plans of action concerning maintenance of national safety of Ukraine it is necessary to consider changes in space of threats and the calls, the influences of the information factor caused to expansions in the conditions of globalisation.

УДК 351.9; 621.321

ПРОБЛЕМНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ПОВНОВАЖЕНЬ ДЕРЖСПЕЦЗВ'ЯЗКУ УКРАЇНИ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ ПРО ПЕРСОНАЛЬНІ ДАНІ

Михайло Косіцин, Едуард Плешко
Управління Держспецзв'язку в Одеській області

Стаття: ***4 стор., 15 джерел***

Створення Держспецзв'язку України, як окремого спеціально уповноваженого центрального органу виконавчої влади, співпало з оформленням нової концепції побудови інформаційного простору держави, що

знайшло відображення у законі «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». У звя'зку з цим потребують суттєвих змін питання правового регулювання щодо надання органами державної влади та місцевого самоврядування інформаційних послуг юридичним та фізичним особам з використанням мережі Інтернет, запровадження електронного документообігу та електронного цифрового підпису, дистанційного навчання, телемедицини, електронних платіжних систем, електронного бізнесу, електронних бірж, аукціонів і депозитаріїв. Конституційний Суд України вже визнав недосконаліть вітчизняного законодавства в сфері регулювання інформаційних правовідносин і його невідповідність європейським стандартам в частині захисту персональних даних. У системі національного права України досі відсутні єдина правова термінологія та понятійний апарат інформації про особу.

Прийнятий Закон України «Про захист персональних даних» тягне за собою необхідність удосконалення окремих діючих правових норм, що безпосередньо регулюють діяльність Держспецзв'язку України, бо передбачена законодавством для службових осіб Держспецзв'язку можливість складання лише протоколів значно погіршує оперативність усунення виявлених недоліків та фактично надає змогу порушникам тривалий час порушувати права громадян та інтереси держави, що охороняються законом. Більш поширеним засобом державного контролю має бути відповідний атестат Держспецзв'язку, відсутність якого є підставою для відповідальності.

Безпосередньо перед Держспецзв'язком постають питання термінового удосконалення нормативно-правової бази з організації власної діяльності та визначення невирішених питань серед її пріоритетів, упорядкування структури підрозділів державного контролю з метою забезпечення реального захисту персональних даних.

ПРОБЛЕМНЫЕ ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПОЛНОМОЧИЙ ГОССПЕЦСВЯЗИ УКРАИНЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ О ПЕРСОНАЛЬНЫХ ДАННЫХ

Михаил Косицын, Эдуард Плешко
Управление Госспецсвязи в Одесской области

Создание Госспецсвязи Украины, как отдельного специально уполномоченного центрального органа исполнительной власти, совпало с оформлением новой концепции построения информационного пространства государства, что нашло отражение в законе «Об основных принципах развития информационного общества в Украине на 2007-2015 годы». В связки с этим требуют существенных изменений вопросы правового регулирования относительно предоставления органами государственной власти и местного самоуправления информационных услуг юридическим и физическим лицам с использованием сети Интернет, внедрение электронного документооборота и электронной цифровой подписи, дистанционного обучения, телемедицины, электронных платежных систем, электронного бизнеса, электронных бирж, аукционов и депозитариев. Конституционный Суд Украины уже признал несовершенство отечественного законодательства в сфере регулирования информационных правоотношений и его несоответствия европейским стандартам в части защиты персональных данных. В системе национального права Украины до сих пор отсутствуют единая правовая терминология и понятийный аппарат информации о лице.

Принят Закон Украины «О защите персональных данных» влечет необходимость совершенствования отдельных действующих правовых норм, непосредственно регулирующих деятельность Госспецсвязи Украины, потому предусмотрена законодательством для должностных лиц Госспецсвязи возможность составления только протоколов значительно ухудшает оперативность устранения выявленных недостатков и фактически предоставляет возможность нарушителям долго нарушать права граждан и интересы государства, охраняемых законом. Более распространенным средством государственного контроля должен быть соответствующий аттестат Госспецсвязи, отсутствие которого является основанием для ответственности.

Непосредственно перед Госспецсвязи встают вопросы срочного усовершенствования нормативно-правовой базы по организации собственной деятельности и определения нерешенных вопросов среди ее приоритетов, упорядочения структуры подразделений государственного контроля с целью обеспечения реальной защиты персональных данных.

ISSUES OF LEGAL REGULATION AUTHORITY OF STATE SPECIAL COMMUNICATION OF UKRAINE WITH SECURITY OF PERSONAL DATA

Michael Kositsyn, Edward Pleshko
Office of State Service in Odessa

Creation of State Service communication of Ukraine as a separate specially authorized central executive body, coincided with the issuance of a new concept of building an information space of the state, as reflected in the law "On basic principles of information society development in Ukraine in 2007-2015". In connection with the need of these significant changes to the legal regulation of state and local government information services to businesses and individuals using the Internet, the introduction of electronic document and digital signature, e-learning, Telemedicine, electronic payment systems, electronic business, electronic exchanges, auctions and depositories. Constitutional Court of Ukraine has acknowledged shortcomings of domestic legislation in the field of legal information and the lack of European standards in the protection of personal data. In the national law of Ukraine has not only legal terminology and conceptual apparatus of information about a person.

Adopted Law of Ukraine "About protection of personal data" entails the need to improve some existing legal provisions that directly regulate the activities of State Special communication of Ukraine, as provided by law for officers of State Special communication designing protocols only significantly affects the efficiency eliminate shortcomings and actually allows attackers to violate long-time civil rights and state interests protected by law. A more common means of state control should be an appropriate certificate of State Special communication, the lack of which is the basis for liability.

Immediately before the State Special communication arises for urgent improvement of the legal framework to organize their own activities and identify outstanding issues among its priorities, streamlining the structure of departments of state control in order to ensure real protection of personal data.

УДК 343.96+343.326+343.341

ЗАПОБІГАННЯ КОМП'ЮТЕРНОМУ ТЕРОРИЗМУ ЯК ОДИН ІЗ НАПРЯМІВ ПРОТИДІЇ ТЕРОРИЗМУ В УКРАЇНІ

Дмитро Мельник
Служба безпеки України

Стаття: ***7 стор., 8 джерел.***

Сучасні процеси глобалізації та тенденції розвитку суспільства зумовили зростання транснаціонального тероризму, появу на озброєнні терористів новітніх інформаційних технологій та виникнення й розвиток комп'ютерного тероризму. З приєднанням України до глобального інформаційного простору проблема комп'ютерного тероризму набула для нашої держави особливої актуальності. Зростаючий рівень інформатизації вітчизняного суспільства зумовлює потребу створення в державі сучасної та надійної системи забезпечення інформаційної безпеки. Вагоме місце у цій системі повинні займати заходи запобігання комп'ютерному тероризму як протиправному явищу загалом, так його окремим проявам. В статті основну увагу приділено висвітленню актуальних аспектів діяльності щодо запобігання комп'ютерному тероризму, наявним проблемам у цій діяльності, а також визначенню перспективних заходів з її удосконалення.

ПРЕДОТВРАЩЕНИЕ КОМПЬЮТЕРНОГО ТЕРРОРИЗМА, КАК ОДНО ИЗ НАПРАВЛЕНИЙ ПРОТИВОДЕЙСТВИЯ ТЕРОРИЗМА В УКРАИНЕ

Дмитрий Мельник
Служба безопасности Украины

Современные процессы глобализации и тенденции развития общества обусловили рост транснационального терроризма, появление на вооружении террористов новейших информационных технологий, возникновение и развитие компьютерного терроризма. С присоединением Украины к

глобальному информационному пространству проблема компьютерного терроризма стала для нашей страны особенно актуальной. Возрастающий уровень информатизации отечественного общества обуславливает потребность создания в государстве современной и надежной системы обеспечения информационной безопасности. Значимое место в этой системе должны иметь мероприятия по предотвращению компьютерного терроризма, как противоправного явления как в целом, так и его отдельным проявлениям. В статье рассмотрены актуальные аспекты предотвращения компьютерного терроризма, имеющиеся проблемы в этой деятельности, а также определены перспективные мероприятия по ее усовершенствованию.

PREVENTION OF COMPUTER TERRORISM AS ONE OF THE WAYS OF COUNTERING ACTION AGAINST THE TERRORISM IN UKRAINE

Dmyrto Melnyk
Security Service of Ukraine

Globalization of the social, economic and information spheres has brought about globalization of cyberterrorism, making it increasingly organized, transnational and dangerouse. Terrorist's organizations are, much faster than state systems in different countries, taking advantage of new information facilities, any loosening of IT-sphere controls, and any liberalization of communications in the world.

Last events in the world have showed, that the cyberterrorism problem had not solved within the limits of traditional resources and methods. That's why the state and society have pooled their efforts in looking for new ways of its standing up. A number of laws and practical recommendations on priority area in combating cybercrime and cyberterrorism have been worked out and adopted in Ukraine. Our law-enforcement and security agencies are rendering effective investigation of criminal cases about cybercrimes and traditional terrorism, but these efforts are not enough. That is why, anti-terrorist forces in our country look for more effective mechanisms of counteraction to cyberterrorism in order to raise the awareness of society about the danger of globalizing terrorism. One of these mechanisms must become the prevention to the cyberterrorism in Ukraine, which is the subject of the article.

УДК 519.724.681

ПРО ДЕЯКІ АСПЕКТИ ВИЗНАЧЕННЯ ЦІННОСТІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ

Олександр Архипов
НТУУ «КПІ»

Стаття: ***7 стор., 22 джерела, 1 рис.***

Розглянуто зміст поняття цінність інформації, його поширені інтерпретації, трансформацію, що її отримало це поняття із плином часу. Досліджено основні принципи, підходи та методи визначення кількісних оцінок цінності інформації, зокрема їх модифікацію в разі аналізу цінності конфіденційної інформації.

Запропоновано адитивну модель цінності інформації, сформовано структуру цієї моделі, наведено інтерпретації її окремих складових. Розглянуто питання старіння інформації, її фрагментації на окремі блоки, можливість врахування цих процесів при визначенні цінності конфіденційної інформації. Проаналізовано семантичні особливості термінів "цінність" і "важливість" інформації.

О НЕКОТОРЫХ АСПЕКТАХ ОПРЕДЕЛЕНИЯ ЦЕННОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Александр Архипов
НТУУ «КПИ»

Рассмотрено содержание понятия ценность информации, его распространенные интерпретации, трансформация этого понятия с течением времени. Исследованы основные принципы, подходы и методы

определения количественных оценок ценности информации, в частности, их модификацию в случае анализа ценности конфиденциальной информации.

Предложена аддитивная модель ценности информации, сформирована структура этой модели, даны интерпретации ее отдельных составляющих. Рассмотрены вопросы старения и фрагментации информации на отдельные блоки, возможность учета этих процессов при определении ценности конфиденциальной информации. Проанализированы семантические особенности терминов "ценность" и "важность" информации.

ABOUT SOME ASPECTS OF THE CONFIDENTIAL INFORMATION VALUE DETERMINATION

Alexander Arkhypov
NTUU "KPI"

It is considered content of the information value conception, its common interpretations and transformation of this conception with time. The basic principles, approaches and methods of quantitative estimations determinations of information value are investigated, particularly their modification in the analysis of the confidential information value.

We proposed an additive model of information value. It is formed the structure of this model and the interpretation of its individual components. The questions of information ageing and its fragmentation in separate blocks, the ability to account these processes in determining the confidential information value are considered. It is analyzed the semantic features of terms value and importance of information.

УДК 004.056; 621.391

ВИКОРИСТАННЯ АВС АНАЛІЗУ ДЛЯ ОПТИМІЗАЦІЇ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Володимир Кононович, Юрій Копитін*
*Академія зв'язку України, *Одеська національна академія зв'язку ім. О. С. Попова*

Стаття: ***10 стор., 15 джерел, 5 таблиць, 4 рис.***

У роботі показано можливість використання методу АВС аналізу в питаннях захисту інформації, а також порядок застосування АВС аналізу для вибору комплексу засобів захисту від несанкціонованого доступу.

Результати алгоритму АВС аналізу поділяються, як правило, на три групи (А: В: С). Групу А складає незначна кількість чинників з високим рівнем питомої ваги за обраним показником; групу В – середня кількість чинників з середнім рівнем питомої ваги; групу С – величезна кількість чинників з незначною величиною питомої ваги. Головний сенс дослідження у рамках АВС аналізу зводиться до того, що максимальний ефект досягається при вирішенні завдань (проблем), що відносяться до групи А.

Розглянуто приклад використання АВС аналізу в питаннях вибору оптимального комплексу засобів захисту (КЗЗ) від несанкціонованого доступу, який демонструє потенційну можливість використання АВС аналізу в питаннях захисту інформації. На основі результатів проведеного АВС аналізу методом «суми» на базі статистики вразливостей операційних систем (ОС) можна зазначити, що оптимальний КЗЗ має включати такі механізми: контролю цілісності; створення замкнутого програмного середовища; ідентифікації та автентифікації.

Авторами пропонується методика визначення рівня небезпеки загроз з використанням АВС аналізу для вибору ефективних захисних механізмів. Об'єктами аналізу виступають активи інформаційної системи. До ІТ активів відносяться: інформація/дані, апаратні засоби, програмне забезпечення тощо. Розглянуто використання АВС аналізу в питаннях визначення достатнього набору послуг під час вибору функціонального профілю захисту (ФПЗ), а також приклад використання АВС-аналізу в процесі вибору ФПЗ та визначення необхідних захисних послуг АС класу 2, призначеної для автоматизації діяльності органів державної влади (ОДВ). Використання методу АВС аналізу в питаннях захисту інформації дозволяє швидко та зручно визначити механізми захисту, які необхідно застосовувати для підтримання належного рівня політики інформаційної безпеки. Зокрема, це вибір комплексу засобів захисту, який забезпечує захист від актуальних на даний момент вразливостей.

ИСПОЛЬЗОВАНИЕ АВС АНАЛИЗА ДЛЯ ОПТИМИЗАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Владимир Кононович, Юрий Копытин *

*Академия связи Украины, * Одесская национальная академия связи им. А. С. Попова*

В работе показана возможность использования метода АВС анализа в вопросах защиты информации, а также порядок применения АВС анализа для выбора комплекса средств защиты от несанкционированного доступа.

Результаты алгоритма АВС анализа делятся, как правило, на три группы (А: В: С). Группу А составляет незначительное количество факторов с высоким уровнем удельного веса по выбранному показателю; группу В - среднее количество факторов со средним уровнем удельного веса; группу С - огромное количество факторов с незначительной величиной удельного веса. Главный смысл исследования в рамках АВС анализа сводится к тому, что максимальный эффект достигается при решении задач (проблем), относящихся к группе А.

Рассмотрен пример использования АВС анализа в вопросах выбора оптимального комплекса средств защиты (КСЗ) от несанкционированного доступа, который демонстрирует потенциальную возможность использования АВС анализа в вопросах защиты информации. На основе результатов проведенного АВС анализа методом «суммы» на базе статистики уязвимостей операционных систем (ОС) можно отметить, что оптимальный КСЗ должен включать следующие механизмы: контроль целостности; создание замкнутой программной среды; идентификации и аутентификации.

Авторами предлагается методика определения уровня опасности угроз с использованием АВС анализа для выбора эффективных защитных механизмов. Объектами анализа выступают активы информационной системы. К ИТ активам относятся: информация / данные, аппаратные средства, программное обеспечение и т.п.. Рассмотрено использование АВС анализа в вопросах определения достаточного набора услуг при выборе функционального профиля защиты (ФПЗ), а также пример использования АВС-анализа в процессе выбора ФПЗ и определение необходимых защитных услуг АС класса 2, предназначенной для автоматизации деятельности органов государственной власти (ОДВ) . Использование метода АВС анализа в вопросах защиты информации позволяет быстро и просто определить механизмы защиты, которые необходимо применять для поддержания надлежащего уровня политики информационной безопасности. В частности, это выбор комплекса средств защиты, который обеспечивает защиту от актуальных на данный момент уязвимостей.

USE OF ABC ANALYSIS FOR OPTIMIZATION SYSTEM SECURITY

Vladimir Kononovich, Yuri Kopytin*

*Academy of communications of Ukraine, *Odessa National Academy of communications named after A. S. Popov*

The paper shows the possibility of using ABC analysis method to protect information and the application of ABC analysis to select the set of protection against unauthorized access.

The results of ABC analysis algorithm are divided, as a rule, into 3 groups (A: B: C). Group A is a small number of factors with high specific gravity of the chosen indicator, group B is the average number of factors with middle-share of the gross weight, group C is a huge number of factors with little value share of the gross weight. The main meaning of research within the ABC analysis is to ensure that the maximum effect is achieved in solving problems (challenges) that belong to group A.

An example of the using ABC analysis in choosing the optimal complex of the security facilities (CSF) from unauthorized access is considered, which demonstrates the potential using of ABC analysis to protect information. Based on the results of ABC analysis by the method of the "amount" based on statistics vulnerabilities of operating systems (OS) can be noted that the optimal CSF should include the following mechanisms: control of the integrity, creating a locked programming environment, identification and authentication.

Authors proposed method of determining the level of the danger threats using ABC analysis to select effective protective mechanisms. The objects of analysis are the assets of the information system. IT assets includes information / data, hardware, software and more. There was considered the use of ABC analysis in definition of a sufficient set of services in choosing a functional profile protection (FPP), and also an example of using ABC-

analysis in the process of selecting FPP and defining appropriate protective services AS Class 2, designed to automate the activities of public authorities (PA).Using ABC analysis to protect information quickly and easily determine the remedies, which necessarily be applied to maintain the proper level of the information security policy. In particular, the choice of the complex of the security facilities, which provides protection against topical vulnerabilities at the moment.

УДК 004.056.53

АУТЕНТИФИКАЦИЯ В ЗАЩИЩЕННЫХ ПРИЛОЖЕНИЯХ

Михаил Коломыцев, Светлана Носок

Национальный технический университет Украины «Киевский политехнический институт»

Статья: ***5 стр., 4 источника, 1 рис.***

В работе рассмотрены основные аспекты и задачи защиты приложений, проанализированы различные способы аутентификации как средства безопасности приложений и освещены общие требования к реализации механизма аутентификации.

В безопасности приложения выделено следующие основные задачи:

-гарантировать, что данные, которые создаются, модифицируются, сохраняются и (или) передаются с помощью приложения, защищены от неавторизованного раскрытия, подмены, искажения или разрушения со стороны пользователей, внешних процессов и самого приложения;

-создать дополнительные сервисы безопасности, которые в общесистемной инфраструктуре безопасности (сеть, операционная система, СУБД) либо не реализованы, либо неадекватны возможным угрозам.

Для решения этих задач в приложении должен быть реализован набор сервисов безопасности одним из трех способов:реализация сервиса безопасности внутри приложения; непосредственное обращение к сервисам безопасности промежуточного ПО или других инфраструктурных компонент; путем проверки, что защита обеспечивается функциями безопасности промежуточного ПО или инфраструктурных компонент.

Исходя из этих требований определены требования к механизму аутентификации защищенного приложения, который должен реализовать администратор.

Рассмотрены общие требования к реализации механизма аутентификации: аутентификация пользователей, аутентификация процессов, аутентификационное предупреждение, выбор аутентифицирующих сущностей, цепочки доверия, доверенный путь, аутентификация групп/ролей, база безопасности, аутентификация лиц с административными полномочиями, аутентификация каждой сессии пользователя.

АУТЕНТИФІКАЦІЯ У ЗАХИЩЕНИХ ДОДАТКАХ

Михайло Коломицев, Світлана Носок

Національний технічний університет України «Київський політехнічний інститут»

У роботі розглянуті основні аспекти та завдання захисту додатків, проаналізовані різні способи аутентифікації як засоби безпеки додатків і висвітлені загальні вимоги до реалізації механізму аутентифікації.

В безпеці додатку виділено такі основні завдання:

- гарантувати, що дані, які створюються, модифікуються, зберігаються і (або) передаються за допомогою додатку, захищені від неавторизованого розкриття, підміни, спотворення або руйнування з боку користувачів, зовнішніх процесів і самого додатку;

- створити додаткові сервіси безпеки, які в загальносистемній інфраструктурі безпеки (мережа, операційна система, СУБД) або не реалізовані, або неадекватні можливим загрозам.

Для вирішення цих завдань у додатку повинен бути реалізований набір сервісів безпеки одним з трьох способів: реалізація сервісу безпеки всередині додатку; безпосереднє звернення до сервісів безпеки проміжного ПЗ або інших інфраструктурних компонент; шляхом перевірки, що захист забезпечується функціями безпеки проміжного ПЗ або інфраструктурних компонент.

Виходячи з цих вимог розроблені вимоги до механізму аутентифікації захищеного додатку, який має реалізувати адміністратор.

Розглянуто загальні вимоги до реалізації механізму аутентифікації: аутентифікація користувачів, аутентифікація процесів, аутентифікаційне попередження, вибір аутентифікуючих сутностей, ланцюжки довіри, довірений шлях, аутентифікація груп /ролей, база безпеки, аутентифікація осіб з адміністративними повноваженнями, аутентифікація кожної сесії користувача.

AUTHENTICATIONIN IN THE PROTECTED APPLICATION

Michael Kolomytsev, Svetlana Nosock
National Technical University of Ukraine "Kiev Polytechnic Institute"

In the paper the main aspects and problems of protection applications are discussed, the various authentication methods are analyzed as a means of security applications, and the general requirements for the implementation of the authentication mechanism are elucidated.

In the application security the following key tasks are marked:

- Ensure that the data are created, modified, maintained, and (or) transmitted by the application are protected from unauthorized disclosure, substitution, distortion or destruction of the users, and external processes of the application;
- Create additional security services, which are in the system-wide security infrastructure (network, operating system, database) or are not implemented, or are inadequate possible threats.

To solve these problems in the application must be implemented set of security services by one of three ways: security service implementation within the application; direct appeal to the security services of the middleware or other infrastructure component; by checking that the protection of the security features provided by the middleware or infrastructure component.

Given these requirements, are defined requirements to secure the application authentication mechanism, which the administrator must implement.

The general requirements for the implementation of authentication are examined: the user authentication, the authentication of the process, the authentication warning, the choice of the authenticated entity, a chain of trust, trusted trace, the authentication of the groups / roles, the database of security, the authentication of the persons with administrative privileges, the authentication of each user session.

УДК 656.7.085:657.71(045)

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ВІД НСД. ВАРІАНТ РЕАЛІЗАЦІЇ АЛГОРИТМУ МНОЖИННОЇ АВТЕНТИФІКАЦІЇ

Вячеслав Василенко
Національний авіаційний університет

Стаття: 10 ***стор., 4 джерела, 5 рис.***

Для систем захисту ієрархічних автоматизованих систем пропонується алгоритм множинної автентифікації з використанням можливостей програмно – технічних засобів управління доступом до ресурсів автоматизованих систем. На думку автора засоби захисту робочих станцій, як елемент комплексу засобів захисту локальної обчислювальної мережі, повинні знаходитись під централізованим управлінням монітора безпеки. До складу засобів захисту слід включати засоби автентифікації, засоби захисту операційної системи та систем керування базами даних (при їх наявності), засоби контролю цілісності та програмно – технічні засоби управління доступом. Використання у складу комплексу засобів захисту програмно – технічних засобів управління доступом дозволяє забезпечити ефективну реалізацію механізмів множинної ідентифікації і автентифікації. Автентифікацію засобів автоматизованих систем доцільно здійснювати при старті (включенні) робочих станцій засобами монітора безпеки та його агентів; таймерно згідно з установками адміністратора безпеки; за запитом адміністратора безпеки.

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НСД. ВАРИАНТ РЕАЛИЗАЦИИ АЛГОРИТМА МНОЖЕСТВЕННОЙ АУТЕНТИФИКАЦИИ

Вячеслав Василенко
Национальный авиационный университет

Для систем защиты иерархических автоматизированных систем предлагается алгоритм множественной аутентификации с использованием возможностей программно - технических средств управления доступом к ресурсам автоматизированных систем. По мнению автора средства защиты рабочих станций, как элемент комплекса средств защиты локальной вычислительной сети, должны находиться под централизованным управлением монитора безопасности. В состав средств защиты следует включать средства аутентификации, средства защиты операционной системы и систем управления базами данных (при их наличии), средства контроля целостности и программно - технические средства управления доступом. Использование в состав комплекса средств защиты программно - технических средств управления доступом позволяет обеспечить эффективную реализацию механизмов множественной идентификации и аутентификации. Аутентификацию средств автоматизированных систем целесообразно осуществлять при старте (включении) рабочих станций средствами монитора безопасности и его агентов; таймерно согласно установкам администратора безопасности; по запросу администратора безопасности.

INFORMATION SECURITY SYSTEM FROM UNAUTHORIZED ACCESS. EMBODIMENT OF THE MUTUAL AUTHENTICATION ALGORITHM

Viacheslav Vasilenko
National Aviation University

A protection system for automated hierarchical algorithm is proposed multiple authentications using the capabilities of software - hardware control access to resources automated systems. According to the author means the protection of workstations, as part of remedies against a local area network, should be under central control monitor security. The structure of protection should be included for authentication, protection of the operating system and database management systems (if any), and controls the integrity of the program - technical means of access control. Using the complex protection software - hardware access control allows for efficient implementation of multiple mechanisms for identification and authentication. Authentication of the automated systems it is advisable to start with (including) workstations means safety monitor and its agents, according to the timer settings security administrator, security administrator on request.

УДК 004.43(031):681.3.01(02)

ВИЗНАЧЕННЯ УРАЗЛИВОСТІ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ЯК СКЛАДОВА ПОРЯДКУ РОЗРОБКИ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Володимир Луценко, Валерій Худяков
НТУУ «КПІ»

Стаття: ***6 стор., 10 джерел, 3 рис.***

Реальні проекти захисту за якісними показниками мають об'єктивно відтворювати умови життєдіяльності об'єктів, але реально мають тенденцію до відставання від життєвих вимог. Для подолання такого відставання мають відтворюватися вимоги щодо життєдіяльності системи проектування окремо, для кожного об'єкту у повному обсязі. Такі вимоги передбачають необхідність використання системи захисту що базується на принципово об'єктивному проектуванні, тобто такому, котре не залежить від якісних показників проектанта. Крім того, створювана система захисту має бути динамічною у часі, тобто відкритою щодо можливості змін у часі складових методів та засобів захисту або умов існування об'єкту, а такий чинник залежить від

методологічних властивостей системи проектування, котра створювала систему захисту. І, під кінець, майже завжди є відкритим питання необхідної та достатньої завершеності проекту системи захисту.

Початком більш об'єктивного проектування має бути напрацювання методів та засобів отримання максимально повної та об'єктивної інформації про об'єкт на етапі дослідження об'єкту. Усе частіш з'являються роботи у котрих автори намагаються активізувати залучення інтелектуалізованих технологій моделювання складних процесів до напрямків проектування складних систем. Одним з підходів є залучення радикально нового підходу, наприклад - використання інформаційних технологій що базуються на засобах інтелектуальної підтримки прийняття рішень. Очевидно, що користування засобами проектування для котрих технології інтелектуальної підтримки прийняття рішень не можуть проводитись у ручному режимі, вимагає розробки та залучення спеціалізованих автоматизованих систем проектування.

ОПРЕДЕЛЕНИЕ УЯЗВИМОСТИ ОБЪЕКТОВ ИНФОРМАЦИОННОЙ ДЕЯТЕЛЬНОСТИ В КАЧЕСТВЕ СОСТАВЛЯЮЩЕЙ ПОРЯДКА РАЗРАБОТКИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Владимир Луценко, Валерий Худяков
НТУУ «КПИ»

Реальные проекты защиты по качественным показателям должны объективно отражать условия жизнедеятельности объектов, но реально отстают от требований жизни. Для преодоления отставания необходимо воспроизводить требования к жизнедеятельности системы проектирования отдельно для каждого объекта в полном объеме. Такие требования предусматривают использование систем защиты, которые базируются на принципиально объективном проектировании, не зависящем от качественных показателей проектанта. Кроме того, создаваемая система защиты должна быть динамичной, то есть открытой к возможным изменениям во времени составляющих методов и средств защиты или условиям существования объекта. Это зависит от методологических свойств системы проектирования. Почти всегда, также, открыт вопрос о необходимой и достаточной завершенности проекта защиты.

Началом более объективного проектирования должна быть наработка методов и средств получения максимально полной и объективной информации об объекте на этапе его обследования. Все чаще появляются работы, в которых авторы пытаются активизировать привлечение интелектуализированных технологий моделирования сложными процессами к направлениям проектирования сложных систем. Один из подходов это подход с привлечением радикально новых решений, например – использование средств интеллектуальной поддержки принятия решений. Очевидно, что использование средств проектирования для которых технологии интеллектуальной поддержки принятия решений не могут реализовываться в ручном режиме, требуют привлечения специальных автоматизированных средств проектирования.

DEFINITION OF VULNERABILITY OF OBJECTS OF AN INFORMATION WORK AS A COMPONENT SEQUENCE OF DEVELOPMENT OF SYSTEMS OF THE INFORMATION PROTECTION

Vladimir Lutsenko, Valery Khudyakov
NTUU "KPI"

Real projects of protection on quality objectively should reflect conditions of ability to live of objects, but really lag behind requirements of life. For overcoming backlog it is necessary to reproduce requirements to ability to live of system of designing separately for each object in full. Such requirements provide use of systems of protection on base essentially objective designing which does not depend on quality indicators of the designer. Besides the created system of protection should be dynamical, that is open to changes in time of making methods and means of protection or to conditions of existence of object. It depends on methodological properties of system of designing. Almost always the question on necessary and sufficient completeness of the project of protection, also, is open.

The beginning of more objective designing should be an operating time of methods and means of reception of maximum full and objective information on object at a stage of inspection. Even more often there are works in which

authors try to make active attraction intellectual technologies of modelling by difficult processes to directions of designing of difficult systems. One of approaches this attraction of considerably new decision, for example - use of means of intellectual support of acceptance of decisions. It is obvious, that use of means of designing for which technologies of intellectual support of acceptance of decisions may not be realized in a manual mode, demand attraction of the special automated means of designing.

УДК 681.3.06:519.248.681

ТЕСТ НА ПРОФІЛЬ ЛІНІЙНОЇ СКЛАДНОСТІ

Людмила Завадська, Максим Семибаламут
ФТІ НТУУ «КПІ»

Стаття: ***5 стор., 6 джерел, 4 табл., 2 рис.***

Розроблено новий тест для оцінювання якості випадкових послідовностей, який базується на профілі лінійної складності. Тест оперує кількістю стрибків лінійної складності і у певних випадках значно ефективніший за відповідний тест з набору NIST. Задача побудови нових ефективних критеріїв для виявлення відхилень від випадковості є актуальною.

В основу тесту, названого авторами LP-тестом (Linear Profile-тест), покладена випадкова величина $S_n = (N_n - n/4)/\sqrt{n/8}$. Швидкість роботи побудованого тесту приблизно така сама, як і швидкість тесту на лінійну складність з пакету NIST, так як в основі обох тестів лежить алгоритм Берлекемпа-Мессі. Проте реалізація LP-тесту дещо простіша, адже в ньому статистика має стандартний розподіл на відміну від специфічного розподілу статистики у тесті NIST.

В результаті досліджень авторів було виявлено, що тест LP набагато ефективніший принаймні на наступних типах неякісних вхідних послідовностей (тут шум означає інвертування кожного біту з імовірністю *p*):

a. Лінійні рекурентні послідовності з шумом.
b. Послідовності, сформовані шляхом регулярного або випадкового чергування відрізків різних лінійних рекурентних послідовностей.
c. Послідовності, сформовані шляхом регулярного або випадкового чергування відрізків лінійних рекурентних послідовностей та відрізків, утворених за допомогою гарного генератора псевдовипадкових чисел.
d. Послідовності, сформовані, як зазначено у попередньому пункті, з шумом.
e. Послідовності, сформовані з лінійних рекурентних послідовностей шляхом випадкового видалення бітів.

ТЕСТ НА ПРОФИЛЬ ЛИНЕЙНОЙ СЛОЖНОСТИ

Людмила Завадская, Максим Семибаламут
ФТИ НТУУ «КПИ»

Разработано новый тест для оценки качества случайных последовательностей, основанный на профили линейной сложности. Тест оперирует количеством прыжков линейной сложности и в определенных случаях значительно эффективнее чем соответствующий тест из набора NIST. Задача построения новых эффективных критериев для выявления отклонений от случайности актуальна.

В основу теста, названного авторами LP-тестом (Linear Profile-тест), положена случайная величина $S_n = (N_n - n/4)/\sqrt{n/8}$. Скорость работы построенного теста примерно такая же, как и скорость теста на линейную сложность из пакета NIST, так как в основе обоих тестов лежит алгоритм Берлекемпа-Месси. Однако реализация LP-теста несколько проще, ведь в нем статистика имеет стандартное распределение в отличие от специфического распределения статистики в тесте NIST.

В результате исследований было выявлено, что тест LP намного эффективнее по крайней мере на следующих типах некачественных входных последовательностей (тут шум означает инвертирование каждого бита с вероятностью *p*):

a. Линейные рекуррентные последовательности с шумом.

b. Последовательности, сформированные путем регулярного или случайного чередование отрезков разных линейных рекуррентных последовательностей.

c. Последовательности, сформированные путем регулярного или случайного чередование отрезков линейных рекуррентных последовательностей и отрезков, образованных с помощью хорошего генератора псевдослучайных чисел.

d. Последовательности, сформированы, как указано в предыдущем пункте, с шумом.

e. Последовательности, сформированные из линейных рекуррентных последовательностей путем случайного удаления битов.

TEST PROFILE LINEAR COMPLEXITY

Lyudmila Zavadskaya, Maxim Semybalamut
PTI NTU "KPI"

A new test for assessing the quality of random sequences is developed, based on the profile of linear complexity. Test operates the number of leaps of the linear complexity and in some cases much more effective than the corresponding test set of NIST. The task of composition a new effective criteria for detecting deviations from randomness is relevant.

As a basis of the test, called by the author the LP test (Linear Profile-test), is laid the random value $S_n = (N_n - n/4)/\sqrt{n/8}$,. The speed of the created test approximately the same as the speed test on the linear complexity of the package of NIST, as the basis of both tests is the algorithm Berlekempa-Messi. But the realization of LP-test somewhat easier, because it has a normal distribution statistics as against to specific distribution of test statistics in NIST.

As a result of investigations of authors it was found that the LP test is much more effective at least for these types of low-quality input sequences :

a. Linear recurrent sequences with the noise.

b. Sequence generated by a regular or random alternation of the different segments of linear recurrent sequences.

c. Sequence generated by a regular or random alternation of the segments of linear recurrent sequences and the segments created by a good generator of the pseudorandom numbers.

d. Sequence generated with the noise.

e. Sequence generated of linear recurrent sequences by accidental deletion of bits.

УДК 681.3.06

УНІВЕРСАЛЬНЕ ГЕШУВАННЯ ПО РАЦІОНАЛЬНИМ ФУНКЦІЯМ АЛГЕБРАЇЧНИХ КРИВИХ У КУБІЧНОМУ ПОЛІ

Геннадій Халімов
Харківський національний університет радіоелектроніки

Стаття: ***6 стор., 6 джерел, 4 табл.***

Подано визначення універсального гешування по раціональним функцій алгебраїчних кривих Ферма і Гурвіца з великим числом точок в кубічному полі. Отримано вираз для ймовірності колізії та асимптотичні оцінки при великих значеннях розмірності поля. Наведені приклади геш обчислень за поліноміальному базису на кривих Ферма і Гурвіца та оцінки ймовірності колізії. Асимптотика ймовірності колізії універсального гешування за кривими Ферма і Гурвіца визначається відношенням кореня квадратного довжини даних до розмірності поля, що краще, в порівнянні з гешування з проективної прямої і дорівнює асимптотики гешування по кривій Ерміта в квадратичному полі тієї ж розмірності. Практичний алгоритм обчислення геш коду за раціональними функціями кривої Ферма визначається схемою обчислення Горнера за двома змінним. Складність універсального хешування відповідає складності за кількістю операцій обчислень по кривій Ерміта в квадратичному полі і складніше в порівнянні з гешування з проективної прямої. Отримані результати є розвитком теорії побудови доказово стійкою автентифікації на основі універсального гешування.

УНИВЕРСАЛЬНОЕ ХЕШИРОВАНИЕ ПО РАЦИОНАЛЬНЫМ ФУНКЦИЯМ АЛГЕБРАИЧЕСКИХ КРИВЫХ В КУБИЧЕСКОМ ПОЛЕ

Геннадий Халимов
Харьковский национальный университет радиоэлектроники

Представлено определение универсального хеширования по рациональным функциям алгебраических кривых Ферма и Гурвица с большим числом точек в кубическом поле. Получены выражение для вероятности коллизии и асимптотические оценки при больших значениях размерности поля. Приведены примеры хеш вычислений по полиномиальному базису на кривых Ферма и Гурвица и оценки вероятности коллизии. Асимптотика вероятности коллизии универсального хеширования по кривым Ферма и Гурвица определяется отношением корня квадратного длины данных к размерности поля, что лучше, по сравнению с хешированием по проективной прямой и равняется асимптотике хеширования по кривой Эрмита в квадратичном поле той же размерности. Практический алгоритм вычисления хеш кода по рациональными функциями кривой Ферма определяется схемой вычисления Горнера по двум переменным. Сложность универсального хеширования соответствует сложности по числу операций вычислениям по кривой Эрмита в квадратичном поле и сложнее по сравнению с хешированием по проективной прямой. Полученные результаты являются развитием теории построения доказуемо стойкой аутентификации на основе универсального хеширования.

UNIVERSAL HASHING OF RATIONAL FUNCTIONS ALGEBRAIC CURVES IN A CUBIC FIELD

Gennady Khalimov
Kharkiv National University of Radio Electronics

Presented by the definition of universal hashing of rational functions of Fermat and Hurwitz algebraic curves with a large number of points in a cubic field. Obtained an expression for the probability of collisions and asymptotic estimates for large dimension of the field. The examples of hash algorithms for polynomial basis on the Fermat curves and Hurwitz and estimate the probability of collisions. Asymptotics of the probability of collision of universal hashing Fermat and Hurwitz curves determined by the ratio of the square root of length of data to the dimension of the field, which is better than hashing for the projective line and is equal to the asymptotic behavior of hashing by the Hermite curve in the quadratic field of the same dimension. A practical algorithm for computing the hash code of rational functions of the Fermat curve defined by Horner's scheme for calculating the two variables. The complexity of universal hashing complexity corresponds to the number of operations for computing the Hermite curve in the quadratic field and more complicated than hashing on the projective line. The results are a development of the theory of constructing provably resistant authentication based on universal hashing.

УДК 004.7

ВИРІШЕННЯ ПРОБЛЕМИ ДОСТУПНОСТІ ОДНОТИПНИХ ОБ'ЄКТІВ МЕРЕЖІ ЗА ДОМЕННИМ ІМ'ЯМ В ПРОТОКОЛІ ТРАНСЛЯЦІЇ МЕРЕЖЕВИХ АДРЕС

Юрій Яремчук, Дмитро Кец, Євгеній Ніколаєв, Дар'я Іванішина
Вінницький національній технічний університет

Стаття: ***4 стор., 4 джерела, 5 таблиць.***

В роботі проведено аналіз проблеми доступності однотипних локальних сервісів до глобальної мережі, зокрема доступності однотипних об'єктів мережі за доменним ім'ям.

Для вирішення даної проблеми було запропоновано метод, суть якого полягає у розширені базових таблиць протоколу NAT та створенні залежних зв'язків з таблицями DNS. За рахунок доповнення таблиць NAT додатковими відомостями про існуючі сервіси у локальній мережі та їх локалізацією (IP- адреса та

порт), а також доповненням до таблиці DNS-зв'язків з розширеною таблицею NAT та вказаням зв'язку назви доступного сервісу з його глобальною назвою DNS.

Вирішення даної проблеми дозволило значно розширити можливості протоколу трансляції мережевих адрес IPv4, забезпечивши можливість збільшення кількості глобальних сервісів, при цьому зменшуючи зростання використовуваних адрес цього протоколу. А крім того, дозволить вирішити проблему доступності однакових сервісів, розміщених в одній локальній мережі, доступних користувачеві за різними глобальними іменами DNS але через одну адресу IPv4 в глобальній мережі Інтернет. Запропонований метод також дозволив значно скоротити кількість використовуваних глобальних IPv4- адрес та підвищити стійкість до атак зловмисників з глобальної мережі.

РЕШЕНИЕ ПРОБЛЕМЫ ДОСТУПНОСТИ ОДНОТИПНЫХ ОБЪЕКТОВ СЕТИ ПО ДОМЕННОМУ ИМЕНИ В ПРОТОКОЛАХ ТРАНСЛЯЦИИ СЕТЕВИХ АДРЕСОВ

Юрий Яремчук, Дмитрий Кец, Евгений Николаев, Дарья Иванишина
Винницкий национальный технический университет

В работе проведен анализ проблемы доступности однотипных локальных сервисов к глобальной сети, в частности доступность однотипных объектов сети по доменному имени.

Для решения данной проблемы было предложено метод, суть которого заключается в расширении базовых таблиц протокола NAT и создании зависимых связей с таблицами DNS. За счет дополнения таблиц NAT дополнительными ведомостями про существующие сервисы в локальной сети с их локализацией (IP адрес и порт). Также дополнением к таблице DNS-связей с расширенной таблицей NAT и указателем связей названий доступного сервиса по его глобальному имени DNS.

Решение данной проблемы позволило значительно расширить возможности протокола трансляции сетевых адресов IPv4, обеспечив возможность увеличения количества глобальных сервисов, при этом уменьшая возрастание использующихся адресов этого протокола. А кроме этого, позволит решить проблему доступности одинаковых сервисов, размещённых в одной локальной сети, доступных пользователю по разным глобальным именам DNS но через один адрес IPv4 в глобальной сети Интернет. Предложенный метод также позволил значительно сократить количество использованных глобальных IPv4 адресов и повысил стойкость к атакам злоумышленников с глобальной сети.

SOLVING THE PROBLEM OF AVAILABLE NETWORK SAME OBJECTS FROM DOMAIN NAME IN THE PROTOCOL OF NETWORK ADDRESS TRANSLATION

Yuriy Yaremchuk, Dmytro Kec, Eugene Nikolaev, Daria Ivanishina
Vinnitsa National Technical University

The paper analyzes the problem of local availability of similar services to the global network, including access to the same objects on the network domain name.

To solve this problem was the method, the essence of which is expanded basic protocol NAT tables and creating relationships with the dependent tables DNS. By NAT tables supplement additional information about existing services in the local network and their location (IP-address and port), and in addition to the DNS-table relationships with extended NAT table and stating the name of affordable communication services to its global name DNS.

The solution to this problem greatly enhance the ability of network address translation protocol IPv4, the option to increase the number of global services, thus reducing the growth of addresses used by this protocol. And besides, will solve the problem of equal access to services located in the same local network, available to the user for various global DNS names but for one IPv4 address on the World Wide Web. The method also makes them used to reduce the number of global IPv4-addresses, and increase resistance to malicious attacks from the global network.

УДК: 004.056.5

ЗМЕНШЕННЯ ВІДХИЛЕНЬ КООРДИНАТ ТОЧОК ВНАСЛІДОК ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ВЕКТОРНІ ЗОБРАЖЕННЯ

Василь Карпінець, Юрій Яремчук
Вінницький національний технічний університет

Стаття: ***9 стор., 4 джерела, 1 табл., 2 рис.***

В роботі проведено аналіз проблеми значних відхилень окремих точок векторного зображення після вбудовування цифрових водяних знаків (ЦВЗ). Для вирішення вказаної проблеми запропоновано метод захисту векторних зображень цифровими водяними знаками із забезпеченням зменшення впливу його вбудовування на якість зображення. Особливістю методу є те, що вбудовування бітів ЦВЗ здійснюється лише у ті матриці коефіцієнтів дискретного косинусного перетворення (ДКП), зміна яких не призводить до значних відхилень координат точок зображення. Для визначення придатних для вбудовування матриць запропоновано умови відбору з використанням граничного значення величини зміни коефіцієнтів внаслідок вбудовування ЦВЗ.

Також було запропоновано метод для збільшення кількості придатних матриць при однаковому граничному значенні. Метод дозволив збільшувати кількість придатних матриць зміною лише одного коефіцієнта у більшості випадків та двох коефіцієнтів лише у двох випадках.

Було проведено аналіз запропонованого методу та порівняння його з відомим методом щодо впливу ЦВЗ на відхилення координат точок зображення. Результати аналізу показали, що запропонований метод в окремих випадках забезпечує зменшення максимального відхилення значень координат точок векторних зображень внаслідок вбудовування ЦВЗ більше ніж у 20 разів та їх рівномірне відхилення відносно точок оригіналу векторного зображення.

УМЕНЬШЕНИЕ ОТКЛОНЕНИЙ КООРДИНАТ ТОЧЕК ВСЛЕДСТВИЕ ВСТРАИВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ВЕКТОРНЫЕ ИЗОБРАЖЕНИЯ

Василий Карпинец, Юрий Яремчук
Винницкий национальный технический университет

В работе проведен анализ проблемы значительных отклонений отдельных точек векторного изображения после встраивания цифровых водяных знаков (ЦВЗ). Для решения указанной проблемы предложен метод защиты векторных изображений цифровыми водяными знаками с обеспечением уменьшения влияния его встраивания на качество изображения. Особенностью метода является то, что встраивание битов ЦВЗ осуществляется только в те матрицы коэффициентов дискретного косинусного преобразования (ДКП), изменение которых не приводит к значительным отклонениям координат точек изображения. Для определения пригодных для встраивания матриц предложено условия отбора с использованием порогового значения величины изменения коэффициентов в результате встраивания ЦВЗ.

Также был предложен метод для увеличения количества пригодных матриц при одинаковом предельном значении. Метод позволил увеличивать количество пригодных матриц изменением лишь одного коэффициента в большинстве случаев и двух коэффициентов лишь в двух случаях.

Был проведен анализ предложенного метода и сравнение его с известным методом по влиянию ЦВЗ на отклонение координат точек изображения. Результаты анализа показали, что предложенный метод в некоторых случаях обеспечивает уменьшение максимального отклонения значений координат точек векторных изображений в результате встраивания ЦВЗ более чем в 20 раз и их равномерное отклонение относительно точек оригинала векторного изображения.

REDUCING DEVIATIONS COORDINATES OF POINTS DUE EMBEDDING DIGITAL WATERMARKS IN VECTOR IMAGES

Vasyl Karpinets, Yuriy Yaremchuk

Vinnitsa National Technical University

The paper analyzes the problem of large deviations of individual points of a vector image after embedding digital watermarks. To solve this problem proposed a method for protection of vector images digital watermarks with software to reduce the influence of its incorporation on image quality. Feature of this method is that the embedding bits of digital watermarks is carried out only in those matrix coefficients of discrete cosine transform (DCT), a change which does not lead to significant deviations of coordinates of pixels. To determine suitability for embedding matrix proposed criteria with a threshold value of the change in the coefficients as a result of incorporation of the digital watermarks.

Also proposed a method for increasing the number of suitable matrices for the same limiting value. Method allowed us to increase the number of suitable matrices change only one factor in most cases and the two coefficients in only two cases.

An analysis of the proposed method and its comparison with the known method on the effect of digital watermarks on the deviation of coordinates of pixels. The results showed that the proposed method in some cases provides a reduction of the maximum deviation of the coordinates of points of vector images as a result of incorporation of digital watermarks in more than 20 times and their uniform deviation relative to the points of the original vector image.

УДК 621.317

АНАЛІЗ ВИМІРЮВАЛЬНИХ РІВНЯНЬ ПРИ ВИКОНАННІ ФУНКЦІЙ ЗБЕРІГАННЯ, ВІДТВОРЕННЯ ТА ПЕРЕДАВАННЯ ОДИНИЦЬ ВИМІРЮВАНЬ ДЕРЖАВНИМИ ЕТАЛОНАМИ З ОПТИКИ

Олександр Шевченко, Леонід Грищенко*

*Держспоживстандарт України, *ННЦ «Інститут метрології»*

*Стаття: **7 стор., 11 джерел, 4 табл.***

Для задач технічного захисту інформації (ТЗІ) питання аналізу вимірювань у державних первинних еталонах (ДЕ) можуть знайти свої застосування для проведення прецизійного калібрування засобів вимірювальної техніки, що використовуються під час випробувань з ТЗІ. У роботі наведено вимірювальні рівняння для чотирьох державних еталонів з оптики для випадків відтворення, зберігання та передавання одиниць вимірювань.

На сьогодні існує лише один принцип вимірювання потужності лазерного випромінювання – калориметричний, який забезпечує найвищу точність при застосуванні метода електричного заміщення при калібруванні і дозволяє «прив'язати» ДЕ до еталонів вольта і ома. У первинному ДЕ одиниць середньої потужності та енергії лазерного випромінювання схема передавання одиниць наступна: 1 – спочатку подається потужність лазера первинного еталона на ЕПВП, 2 – потім та сама потужність лазера подається на вторинний еталон, 3 – сигнали напруги заміщення первинного еталона та вторинного еталона порівнюються.

Однією з важливих частин еталона ДЕТУ 11-06-06 є абсолютний кріогенний радіометр (АКР), який дозволяє побудувати всю систему радіометричних, спектрометричних і фотометричних еталонів найбільш компактним чином. Разом з тим в склад еталона було введено випромінювач типу АЧТ, як універсальне джерело, випромінювання якого описуються фундаментальним законом Планка. Практично досягнута мінімальна потужність, що реєструється, виявилася пов'язаною не з шумами термобатареї (10^{-8} Вт), а зі швидкістю дрейфу ($2 \cdot 10^{-7}$ Вт). Одиниці спектральних характеристик зберігаються на групі первинних ламп змінного складу після передачі методом компарування за допомогою монохроматора МДР-41. Випромінювання, що виходить з монохроматора, реєструється за допомогою приймачів.

Авторами розроблено високоточний калориметричний вимірювальний перетворювач, який забезпечує вимірювання потужності лазерного випромінювання з сумарної похибкою, що не перевищує 0,5 % з коефіцієнтом перетворення на менше 100 мВ/Вт на довжині хвилі 10,6 мкм і коефіцієнтом поглинання не менше 0,95. Кожну секцію термопари перетворювача виготовлено з константанового дроту діаметром 0,1 мм на тонкостінному діелектричному циліндрі з подальшим покриттям половини периметра кожного витка міддю. Систему вимірювання відносного рівня середньої потужності випромінювання виконано на основі

вимірювача потужності лазерного випромінювання, який складається з болометричного вимірювального перетворювача (приймач-свідок) прохідного типу на основі решітчастого болометричного перетворювача.

В роботі проаналізовано шлях передавання одиниць фізичних величин у вимірювальних схемах чотирьох державних еталонів з оптики. Для спрощення сприйняття достатньо складних фізичних процесів, які відбуваються в державних первинних еталонах під час відтворення, зберігання та передавання одиниць вимірювань, запропоновано записувати рівняння вимірювань в символьній та символьній матричній формі. Логічні записи можуть знайти застосування під час проведення калібрувальних робіт з вторинними та робочими еталонами з метою вибору найоптимальнішого метода калібрування, а також для процедури звірень державних первинних еталонів України із закордонними. Запропоновані символьні записи можуть сприяти проведенню калібрування вторинних еталонів, а також підрахунку похибок та невизначеності вимірювань, у тому числі і в галузі ТЗІ.

АНАЛИЗ ИЗМЕРИТЕЛЬНЫХ УРАВНЕНИЙ ПРИ ВЫПОЛНЕНИИ ФУНКЦИЙ ХРАНЕНИЯ, ВОСПРОИЗВЕДЕНИЯ И ПЕРЕДАЧИ ЕДИНИЦ ИЗМЕРЕНИЙ ГОСУДАРСТВЕННЫМИ ЭТАЛОНАМИ С ОПТИКИ

Александр Шевченко, Леонид Грищенко *

*Госпотребстандарт Украины, * ННЦ «Институт метрологии»*

Для задач технической защиты информации (ТЗИ) вопросы анализа измерений в государственных первичных эталонах (ДЭ) могут найти свои применение для проведения прецизионной калибровки средств вычислительной техники, используемых при испытаниях по ТЗИ. В работе приведены измерительные уравнения для четырех государственных эталонов по оптике для случаев воспроизведения, хранения и передачи единиц измерений.

На сегодня существует лишь один принцип измерения мощности лазерного излучения - калориметрический, который обеспечивает высочайшую точность при применении метода электрического замещения при калибровке и позволяет «привязать» ДЭ до эталонов вольта и ома. В первичном ДЭ единиц средней мощности и энергии лазерного излучения схема передачи единиц следующа: 1 - сначала подается мощность лазера первичного эталона на ЕПВП, 2 - потом та же мощность лазера подается на вторичный эталон, 3 - сигналы напряжения замещения первичного эталона и вторичного эталона сравниваются.

Одной из важных частей эталона ДЕТУ 11-06-06 есть абсолютный криогенный радиометр (АКР), который позволяет построить всю систему радиометрических, спектрометрических и фотометрических эталонов наиболее компактным образом. Вместе с тем в состав эталона было введено излучатель типа АЧТ, как универсальный источник, излучение которого описываются фундаментальным законом Планка. Практически достигнута минимальная мощность, что регистрируется, оказалась связаной не с шумами термобатареи (10-8 Вт), а со скоростью дрейфа (2 • 10-7 Вт). Единицы спектральных характеристик хранятся на группе первичных ламп переменного состава после передачи методом компарирования с помощью монохроматора МДР-41. Излучения, выходящее из монохроматора, регистрируется с помощью приемников.

Авторами разработан высокоточный калориметрический измерительный преобразователь, который обеспечивает измерение мощности лазерного излучения с суммарной погрешностью, не превышающей 0,5% с коэффициентом преобразования в менее 100 мВ / Вт на длине волны 10,6 мкм и коэффициентом поглощения не менее 0,95. Каждую секцию термопары преобразователя изготовлено из константановой проволоки диаметром 0,1 мм на тонкостенном диэлектрическом цилиндре с последующим покрытием половины периметра каждого витка медью. Систему измерения относительного уровня средней мощности излучения выполнено на основе измерителя мощности лазерного излучения, состоящего из болометрического измерительного преобразователя (приемник-свидетель) проходного типа на основе решетчатого болометрического преобразователя.

В работе проанализировано путь передачи единиц физических величин в измерительных схемах четырех государственных эталонов по оптике. Для упрощения восприятия достаточно сложных физических процессов, происходящих в государственных первичных эталонах при воспроизведении, хранение и передаче единиц измерений, предложено записывать уравнения измерений в символьной и символьной матричной форме. Логические записи могут найти применение при проведении калибровочных работ с вторичными и рабочими эталонами с целью выбора наиболее оптимального метода калибровки, а также для процедуры сопоставлений государственных первичных эталонов Украины с зарубежными. Предложенные

символьные записи могут способствовать проведению калибровки вторичных эталонов, а также подсчета погрешностей и неопределенности измерений, в том числе в области ТЗИ.

ANALYSIS OF MEASURING EQUATIONS FOR PROCESSING THE FUNCTIONS MAINTENANCE, DISPLAY AND TRANSFER UNIT OF MEASUREMENTS BY STATE STANDARDS ON OPTICS

Aleksandr Shevchenko, Leonid Gryshchenko *

*State Committee of Ukraine, * NSC "Institute of Metrology"*

For problems technical protection of information (TPI) analysis of measurement issues in the state primary standards (SPS) may find its application for the precision calibration of measuring instruments used during testing of the TPI. In the paper an equations for measuring the four national standards on optics were provided for the cases of display, maintenance and transfer of units of measurement.

At present there is only one principle of measuring power laser - calorimetric, which provides the highest accuracy in applying the method of electrical substitution at calibration and allows "snap" SE to the standards volt and ohm. In the primary SE of the units of average power and energy laser the scheme of transfer units is follow, 1 - first served the laser power primary standard for EPVP, 2 - then the same laser power is fed to the secondary standards, 3 – signals of the voltage substitution pattern of primary and secondary standards are compared.

One of the important parts of the pattern SSTU 6.6.11 is an absolute cryogenic radiometer (ACR), which allows build a whole system of radiometric, spectrometric and photometric standards in the most compact way. However, the structure of the standard was introduced by the radiator AFT as a universal source of radiation which describes by the fundamental laws of Planck. Almost reached the minimum capacity that is registered, it was not due to noise of the thermopile (10-8 W) and a speed of the drift (2•10-7 W). Units of spectral characteristics are stored in the primary group of the AC lamp after the transfer by the method of Comparison via monochromator MDR-41. Radiation emanating from the monochromator, registered by receivers.

The authors developed a precision calorimetric measuring transducer, which provides a measure of the power laser radiation with a total error which does not exceed 0.5% with a conversion efficiency of less than 100 mV / W at a wavelength of 10.6 microns and absorption coefficient of at least 0.95. Each section of the thermocouple converter is made of the constantan wire with a diameter of 0.1 mm on thin-walled dielectric cylinder and then coating half of the perimeter of each loop by the copper. The system of measuring the relative levels of average radiation power carried in terms of the laser power meter, which consists of bolometric measuring transducer (receiver- testator) of the raise type based on the lattice bolometric converter.

In this work, there was analyzed the transmission trace of the physical units of the measurement schemes in the four state standards of optics. There was offered to record equations of measurements in the symbolic and the symbolic matrix form towards simplify the perception sufficiently complex physical processes that occur in the state primary standards during maintenance, display and transfer units of measurements. Logical records can be used in the calibration work with secondary and working standards to select the optimal calibration method and because of the procedure for comparisons of state primary standards of Ukraine with abroad. The proposed symbolic records may facilitate calibration of secondary standards, and counting errors and measurement uncertainty, including in TPI.

УДК 004:621.396.62

РАСЧЕТ ПАРАМЕТРОВ НЕЛИНЕЙНОСТИ ХАРАКТЕРИСТИК БИПОЛЯРНЫХ ТРАНЗИСТОРОВ ПРИ НЕЛИНЕЙНОЙ ЛОКАЦИИ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ

Владимир Чумаков

Академия ВМС им. П. С. Нахимова

Стаття: ***5 стор., 6 джерел, 2 рис.***

Приведены результаты анализа вольтамперных характеристик (ВАХ) биполярных транзисторов и получены выражения для параметров нелинейности. Показана возможность расчета режима транзистора, при котором получаются определенные значения параметров нелинейности. Рассмотрены перспективы использования полученных результатов в системах технической защиты информации.

Для обнаружения средств несанкционированного доступа к информации в системах информационной безопасности используется метод нелинейной локации. Обнаружение радиосредств, содержащих полупроводниковые приборы, осуществляется по регистрации 2-й и 3-й гармоник зондирующих радиосигналов, переизлученных в результате нелинейности ВАХ полупроводникового прибора. Основу элементной базы современных радиосредств составляют транзисторы, поэтому именно реакция нелинейных структур транзисторных компонентов определяет величину отклика на входе обнаружителя. Представляется актуальным получить оценку амплитудной зависимости относительного уровня реакции транзистора расчетным путем на основе модели транзистора. Рассмотрено модель биполярного транзистора и рассчитано параметры нелинейности ВАХ.

Проведенный анализ позволяет оценить амплитудные зависимости параметров нелинейности биполярных транзисторов и рассчитать как режимы транзисторов, так и амплитуду входного гармонического сигнала, при которой наблюдаются максимальные значения амплитуд высших гармоник. Проведенные расчеты выполнены без учета влияния собственных шумов транзисторов и внешних флуктуационных воздействий. Широкие перспективы для анализа реакций полупроводниковых приборов с учетом шумов открывают исследования эффекта стохастического резонанса и методы нелинейного анализа на основе разложения в ряд Вольтерра.

РАСЧЕТ ПАРАМЕТРОВ НЕЛИНЕЙНОСТИ ХАРАКТЕРИСТИК БИПОЛЯРНЫХ ТРАНЗИСТОРОВ ПРИ НЕЛИНЕЙНОЙ ЛОКАЦИИ ПОЛУПРОВОДНИКОВЫХ ПРИБОРОВ

Володимир Чумаков
Академія ВМС ім. П. С. Нахімова

Наведено результати аналізу вольтамперних характеристик (ВАХ) біполярних транзисторів і отримані вирази для параметрів нелінійності. Показана можливість розрахунку режиму транзистора, при якому виходять певні значення параметрів нелінійності. Розглянуто перспективи використання отриманих результатів у системах технічного захисту інформації.

Для виявлення засобів несанкціонованого доступу до інформації в системах інформаційної безпеки використовується метод нелінійної локації. Виявлення радіозасобів, що містять напівпровідникові прилади, здійснюється з реєстрації 2-й і 3-й гармонік зондуючих радіосигналів, випромінених в результаті нелінійності ВАХ напівпровідникового приладу. Основу елементної бази сучасних радіозасобів становлять транзистори, тому саме реакція нелінійних структур транзисторних компонентів визначає величину відгуку на вході виявлення. Отримано оцінку амплітудної залежності відносного рівня реакції транзистора розрахунковим шляхом на основі моделі транзистора. Розглянуто модель біполярного транзистора і розраховано параметри нелінійності ВАХ.

Проведений аналіз дозволяє оцінити амплітудні залежності параметрів нелінійності біполярних транзисторів і розрахувати як режими транзисторів, так і амплітуду вхідного гармонійного сигналу, при якій спостерігаються максимальні значення амплітуд вищих гармонік. Проведені розрахунки виконані без урахування впливу власних шумів транзисторів і зовнішніх флуктуаційних впливів. Широкі перспективи для аналізу реакцій напівпровідникових приладів з урахуванням шумів відкривають дослідження ефекту стохастичного резонансу і методи нелінійного аналізу на основі розкладання в ряд Вольтера.

CALCULATION NONLINEARITIES BIPOLAR TRANSISTORS LOCATIONS IN NONLINEAR SEMICONDUCTOR DEVICES

Vladimir Chumakov
Academy of NE named after P. S. Nakhimov

Results of the analysis of current-voltage characteristics (CVC) of bipolar transistors are introduced and the expressions for the parameters of the nonlinearity are achieved. There was shown the possibility to calculate the mode transistor, wherein certain values of the nonlinearity are obtained. The prospects of using the results are discussed in the systems of technical protection of information.

The method of nonlinear location is used for the detection of unauthorized access to information systems security. Detection of radio-containing semiconductor devices is carried out by recording the 2nd and 3rd harmonics of the sounding radio signal re-radiated as a result of nonlinearity of the CVC of a semiconductor device. The basis of

modern element base radios are transistors, so it was reaction of nonlinear structures of transistor components determines the magnitude of the response at the input of the detector. It presented actuality to obtain an estimate of the amplitude dependence of the relative level of the response of the transistor by means of calculation based on the model of the transistor. A model of the bipolar transistor is considered and parameters of the nonlinearity of the VAC are calculated.

This analysis allows to estimate the amplitude dependence of the parameters of the nonlinearity of bipolar transistors and to calculate both modes of transistors, and the amplitude of input harmonic signal, in which there are maximum amplitudes of higher harmonics. Our calculations are made without considering of the intrinsic noise of transistors and the fluctuation external influences. Great prospects for analysis of the reactions of semiconductor devices, taking into account the noise effect reveal the researches of the stochastic resonance and methods of nonlinear analysis based on Volterra series expansion.

УДК 638.235.231

МОДЕЛЮВАННЯ ВПЛИВУ НЕЛІНІЙНОСТЕЙ НА ФОРМУВАННЯ СИГНАЛУ В НЕЛІНІЙНІЙ РАДІОЛОКАЦІЇ

Максим Зінченко, Юрій Зіньковський, Михайло Прокофьєв
НДЦ «ТЕЗІС» НТУУ «КПІ»

Стаття: ***10 стор., 15 рис., 7 джерел.***

Перспективним напрямком вдосконалення нелінійних радіолокаторів є використання алгоритмів пошуку й ідентифікації напівпровідникових структур за другорядними демаскуючими внутрішніми ефектами в нелінійних розсіювачах. Для цього актуальним залишається аналіз особливостей розсіювання демаскуючого сигналу різними типами антенних структур з нелінійними навантаженнями.

Застосування рядів Вольтерра-Пікара дозволило розробити математичну модель, яка дає можливість оцінити вплив дії нелінійного радіолокатора на формування демаскуючого сигналу з врахуванням фізики процесів у напівпровіднику при дії на нього відносно потужного НВЧ випромінювання. Модель дозволяє врахувати другорядні демаскуючі ефекти в нелінійних розсіювачах та уникнути складнощів щодо формування та розв'язання систем інтегральних рівнянь, які характерні для класичних електродинамічних підходів. При цьому вихідними є внутрішні опосередковані відносно зовнішнього впливу параметри конкретної досліджуваної системи.

Використовуючи отримані в роботі вирази для випадків простого розсіювача, можна знайти ядра Вольтерра в частотній області, що дозволяє отримати інформацію про спектральний склад другорядного демаскуючого сигналу. Крім того, запропонований підхід дозволяє апроксимацію характеристик нелінійних елементів довільною функцією, тобто стає можливим використання будь-яких найбільш підходящих моделей, що відображають вторинні внутрішні ефекти в напівпровідникових структурах.

МОДЕЛИРОВАНИЕ ВЛИЯНИЯ НЕЛИНЕЙНОСТЕЙ НА ФОРМИРОВАНИЕ СИГНАЛА В НЕЛИНЕЙНОЙ РАДИОЛОКАЦИИ

Максим Зинченко, Юрий Зиньковский, Михаил Прокофьев
НИЦ «ТЕЗИС» НТУУ «КПИ»

Перспективным направлением усовершенствования нелинейных радиолокаторов является использование алгоритмов поиска и идентификации полупроводниковых структур за второстепенными демаскирующими внутренними эффектами в нелинейных рассеивателях. Для этого актуальным остается анализ особенностей рассеяния демаскирующего сигнала разными типами антенных структур с нелинейными нагрузками.

Применение рядов Вольтерра-Пікара позволило разработать математическую модель, которая дает возможность оценить влияние действия нелинейного радиолокатора на формирование демаскирующего сигнала с учетом физики процессов в полупроводнике при действия на него относительно мощного СВЧ излучения. Модель позволяет учесть второстепенные демаскирующие эффекты в нелинейных рассеивателях, а также избежать сложности относительно формирования и решения систем интегральных уравнений, которые характерны для классических электродинамических подходов. При этом исходными являются

внутренние опосредствованные относительно внешнего влияния параметры конкретной исследуемой системы.

Используя полученные в работе выражения для случаев простого рассеивателя, можно найти ядра Вольтерра в частотной области, которая позволяет получить информацию о спектральном составе второстепенного демаскирующего сигнала. Кроме того, предложенный подход позволяет аппроксимацию характеристик нелинейных элементов произвольной функцией, то есть становится возможным использование любых наиболее подходящих моделей, которые отображают вторичные внутренние эффекты в полупроводниковых структурах.

THE MODELING OF THE SIGNAL IN A NONLINEAR RADIOLOCATION, TAKING INTO ACCOUNT THE NONLINEARITIES

Max Zinchenko, George Zin'kovskiy, Michael Prokof'ev
Research center of technical protection of information "TESIS" National Technical University of Ukraine "Kyiv Polytechnic Institute"

A promising direction to improve the use of a nonlinear radar algorithms for searching and identification of semiconductor structures for the minor give-away internal effects. For this analysis becomes relevant features of the scattering of secondary unmasking signal different types of antenna structures with nonlinear loads.

Application of Volterra series-Pikara allowed to develop an appropriate for a typical radar in a nonlinear electronic object of study a mathematical model. It provides an opportunity to assess the impact of nonlinear radar on the formation of unmasking the signal with the physics of light in a semiconductor under the action of a relatively high-power microwave radiation. The model allows to take into account secondary telltale internal effects in nonlinear scatterers with nonlinear radar. There is a possibility to avoid the difficulty concerning the formation and solution of complex systems of integral equations, which are characteristic of the classical electrodynamic approaches. In this case the source is internal relative to external influences mediated by the specific parameters of the system.

Using the results obtained in cases of simple expressions for the lens, you can find the kernel of Volterra in the frequency domain, which provides information about the spectrum of the secondary unmasking signal in a nonlinear radar. In addition, the proposed approach allows an approximation of the characteristics of nonlinear elements of an arbitrary function, so it's possible to use all the most suitable models, which represent secondary internal effects in semiconductor structures.

УДК 621.395

РОЗРАХУНОК ПОКАЗНИКІВ ЯКОСТІ КАТЕГОРІЙНОГО ОБСЛУГОВУВАННЯ ЗАЯВОК ПРИ АБСОЛЮТНОМУ ПРІОРИТЕТІ НА ІНТЕЛЕКТУАЛЬНІЙ МЕРЕЖІ ЗВ'ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Дмитро Могилевич, Валерій Правило, Олексій Бреус
ВІТІ НТУУ "КПІ"

Метою даної статті є розгляд показників якості категорійного обслуговування заявок при абсолютному пріоритеті, їх розрахунок на інтелектуальній мережі спеціального призначення (ІМСП), визначення типів втрат заявок в мережах з даним типом категорійного обслуговування та математичні показникі оцінки якості обслуговування. Актуальність даної статті визначається необхідністю визначення принципів оцінки якості обслуговування заявок на ІМСП, розрахунку втрат в даній мережі та критеріїв вибору типу пріоритету для різних ділянок мережі.

При визначенні показників якості пріоритетного обслуговування заявок повинен бути визначений повний перелік вихідних даних, у тому числі і алгоритм встановлення з'єднання, особливо у випадках зайнятості всіх каналів в гілках напрямку зв'язку або в групі обслуговуючих приладів необхідної служби центру інтелектуальних послуг (ЦІП).

Наведені в статті вирази розрахунку втрат заявок при абсолютному пріоритеті отримані для однофазної системи масового обслуговування справедливі як для транспортної мережі ІМСП, так і для розподільної системи ЦІП. Дані вирази дозволяють врахувати втрати, які додатково з'являються в мережі при використанні категорування абонентів на етапі проектування інтелектуальної мережі. Розглянуто алгоритм обслуговування заявок з абсолютним пріоритетом. Визначено, що при обсолютному пріоритеті в обслуговуванні заявок для всіх категогій користувачів (крім вищої) виникають два види втрат: втрати через зайнятість всіх каналів і втрати через пріоритетне скидання. Визначено математичний апарат, що враховує всі види втрат, які присутні в мережі і дозволяє проводити розрахунок показників якості обслуговування заявок ІМСП при абсолютному пріоритеті.

РАСЧЕТ ПОКАЗАТЕЛЕЙ КАЧЕСТВА КАТЕГОРИЙНОГО ОБСЛУЖИВАНИЯ ЗАЯВОК ПРИ АБСОЛЮТНОМ ПРИОРИТЕТЕ НА ИНТЕЛЛЕКТУАЛЬНОЙ СЕТИ СВЯЗИ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Дмитрий Могилевич, Валерий Правило, Алексей Бреус
ВИТИ НТУУ "КПИ"

Целью данной статьи является рассмотрение показателей качества категорийного обслуживания заявок при абсолютном приоритете, их расчеты на интеллектуальной сети специального назначения (ИССН), определение типов потерь заявок в сетях с данным типом категорийного обслуживания и математические показатели оценки качества обслуживания. Актуальность данной статьи определяется необходимостью определения принципов оценки качества обслуживания заявок на ИССН, расчетов потерь в данной сети и критериев выбора типа приоритета для разных участков сети.

При определении показателей качества приоритетного обслуживания заявок должен быть определен полный перечень исходных данных, в том числе и алгоритм установления соединения, особенно в случаях занятости всех каналов в ветвях направления связи или в группе обслуживающих приборов необходимой службы центра интеллектуальных услуг (ЦИУ).

Приведенные в статье выражения расчетов потерь заявок при абсолютном приоритете, полученные для однофазной системы массового обслуживания, справедливы как для транспортной ИССН, так и для распределительной системы ЦИУ. Данные выражения позволяют учесть потери, которые дополнительно появляются в сети при использовании категорирования абонентов на этапе проектирования интеллектуальной сети. Рассмотрен алгоритм обслуживания заявок с абсолютным приоритетом. Определено, что при абсолютном приоритете в обслуживании заявок для всех категогий пользователей (кроме высшей) возникают два вида потерь: потери из-за занятости всех каналов и потери из-за приоритетного сбрасывания. Определен математический аппарат, который учитывает все виды потерь, присутствующие в сети и позволяет проводить расчеты показателей качества обслуживания заявок ИССН при абсолютном приоритете.

CALCULATION SERVICE OF CATEGORY QUALITY APPLICATIONS TO THE ABSOLUTE PRIORITY IN SPECIAL PURPOSE INTELLIGENT NETWORK

Dmitro Mogilevich, Valeriy Pravilo, Oleksiy Breus
MITI NTUU "KPI"

The purpose of given article is consideration of merit figures categorical service of demands at an absolute priority, their calculations on an intellectual network of a special purpose (INSP), definition of types of demands losses in networks with the given type categorical service and mathematical indicators of an estimation quality of service. The urgency of given article is defined by necessity of definition of principles of an estimation demands quality of service on INSP, calculations of losses in the given network and criteria of a choice type of a priority for different network sites.

At definition of merit figures of priority service of demands the full list of the initial data, including algorithm of call establishment, especially in cases of employment of all channels in branches of a direction of communication or in group of serving devices of necessary service of a center of intellectual services (CIS) should be defined.

The expressions of calculations of losses of demands resulted in article at the absolute priority, received for single-phase system of mass service, are fair both for transport INSP, and for distributive system CIS. The given expressions allow to consider losses which in addition appear in a network at use subscribers category at a design stage of an intellectual network. The algorithm of service of demands with an absolute priority is considered. It is defined that at an absolute priority in service of demands for all users category (except the higher) there are two kinds of losses: losses because of employment of all channels and loss because of priority reset. The mathematical apparatus which considers all kinds of losses which are present at a network and is defined allows to carry out calculations of merit figures of service of demands INSP at an absolute priority.

УДК 621.396

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТАНДАРТІВ ЦИФРОВОГО ТРАНКІНГОВОГО РАДІОЗВ'ЯЗКУ

Валерій Правило, Наталія Корчагіна
ВІТІ НТУУ "КПІ"

На сьогодняшній день процес розгортання мереж транкінгового радіозв'язку в усьому світі характеризується широким впровадженням цифрових систем. Практично всі провідні світові постачальники встаткування, системні інтегратори й оператори, а також багато великих споживачів послуг транкінгового радіозв'язку оголосили про свій перехід до цифрових систем. Основне суперництво на ринку стандартів, орієнтованих не тільки на звичайних корпоративних користувачів, але й на представників правоохоронних органів і служб суспільної безпеки, ведуть: TETRA, APCO 25 і Tetrapol.

В Україні системи радіозв'язку на основі даних стандартів поки не розгорнуті. Пояснюється це, насамперед, тим, що цифрові системи помітно дорожче аналогових, і обмежені ресурси відомств і різних об'єднань не дозволяють активно ввімкнутися в процес цифровізації своїх мереж зв'язку. Однак перехід до цифрових систем неминучий, перспективи транкінгових систем радіозв'язку як у світі, так і в Україні, однозначно пов'язані із цифровими технологіями. Цифрові системи радіозв'язку надають користувачам високий рівень послуг, різноманітні режими передачі даних, підвищену безпеку зв'язку, можливості інтеграції з фіксованими цифровими мережами й т.д.

Стандарти цифрового транкінгового зв'язку, до яких відносяться TETRA і APCO 25, забезпечують створення конкурентного середовища, залучення великої кількості виробників базового встаткування, абонентських радіостанцій, тестової апаратури для випуску сумісних радіозасобів, що сприяє зниженню їхньої вартості. Доступ до специфікацій стандартів надається будь-яким організаціям і фірмам, що вступили у відповідну асоціацію. Користувачі, що вибирають відкритий стандарт радіозв'язку, не попадають у залежність від єдиного виробника й можуть міняти постачальників устаткування. Відкриті стандарти користуються підтримкою з боку державних і правоохоронних структур, великих компаній багатьох країн миру, а також підтримані провідними світовими виробниками елементної й вузлової бази.

Все це дозволяє говорити про те, що відкриті стандарти з більшою ймовірністю в перспективі завоюють ринок систем транкінгового радіозв'язку.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ СТАНДАРТОВ ЦИФРОВОЙ ТРАНКИНГОВОЙ РАДИОСВЯЗИ

Валерий Правило, Наталья Корчагина
ВИТИ НТУУ "КПИ"

На сегодняшний день процесс развертывания сетей транкинговой радиосвязи во всем мире характеризуется широким внедрением цифровых систем. Практически все ведущие мировые поставщики оборудования, системные интеграторы и операторы, а также большое количество крупных потребителей услуг транкинговой радиосвязи объявили о своем переходе к цифровым системам. Основное соперничество на рынке стандартов, ориентированных не только на обычных корпоративных пользователей, но и на представителей правоохранительных органов и служб общественной безопасности, ведут: TETRA, APCO 25 и Tetrapol.

В Украине системы радиосвязи на основе данных стандартов пока не развернуты. Объясняется это прежде всего тем, что цифровые системы заметно дороже аналоговых и ограниченные ресурсы ведомств и различных организаций не позволяют активно включиться в процесс цифровизации своих сетей связи.

Однако переход к цифровым системам неминуем, перспективы транкинговых систем радиосвязи как в мире, так и в Украине, однозначно связан с цифровыми технологиями. Цифровые системы радиосвязи предоставляют пользователям высокий уровень услуг, различные режимы передачи данных, повышенную безопасность связи, возможности интеграции с фиксированными цифровыми сетями и т.д.

Стандарты цифровой транкинговой связи, к которым относятся TETRA и APCO 25, обеспечивают создание конкурентной среды, привлечение большого количества производителей базового оборудования, абонентских радиостанций, тестовой аппаратуры для выпуска совместных радиосредств, что способствует снижению их стоимости. Доступ к спецификациям стандартов предоставляется любым организациям и фирмам, которые вступили в соответствующую ассоциацию. Пользователи, которые выбирают открытый стандарт радиосвязи, не попадают в зависимость от единственного производителя и могут менять поставщиков оборудования. Открытые стандарты пользуются поддержкой со стороны государственных и правоохранительных структур, больших компаний многих стран мира, а также поддерживаются ведущими мировыми производителями элементной и узловой базы.

Все это позволяет говорить о том, что в перспективе открытые стандарты с большой вероятностью завоюют рынок систем транкинговой радиосвязи.

THE COMPARATIVE ANALYSIS OF DIGITAL TRUNKING RADIO SERVICES STANDARDS

Valeriy Pravilo, Nataliya Korchagina
MITI NTUU "KPI"

Today all over the world process of expansion of networks of tranking radio communications is characterized by wide introduction of digital systems. Almost all leading world suppliers of the equipment, system integrators and operators, and also a considerable quantity of large users of services of tranking radio communications declared the transition to digital systems. The main rivalry in the market of the standards focused not only on usual corporate users, but also on representatives of law enforcement bodies and services of public safety, conduct: TETRA, APCO 25 and Tetrapol.

In Ukraine systems of radio communications on the basis of the given standards aren't developed yet. It is explaned first of all with the fact that digital systems are much more expensive than analog and the limited resources of departments and various organizations don't allow to join actively in process of digitation of their communication networks. However transition to digital systems is inevitable, prospects of tranking systems of radio communications both in the world, and in Ukraine, is unequivocally connected with digital technologies. Digital systems of radio communications give high level of services to users, various modes of the data transmission, the raised safety of communication, possibility of integration with the fixed digital networks etc.

Standards of digital tranking communications which concern TETRA and APCO 25 provide creation of the competitive environment, attraction of a considerable quantity of manufacturers of the base equipment, users' radio stations, test equipment for release of joint radio means that promotes decrease in their cost. Any organization or firm which have entered corresponding association is given an access to specifications of standards. Users who choose the open standard of radio communications, don't get to dependence on the unique manufacturer and can change suppliers of the equipment. Open standards are supported by the state and law-enforcement structures, the big companies of many countries of the world, and also are supported by leading world manufacturers of element and central base.

All of it allows to say with a high probability that in the long term open standards will win the market of systems of tranking radio communications.

УДК 531/534(075.8)

ОПТИМИЗАЦІЯ ХАРАКТЕРИСТИК РАДІОЕЛЕКТРОННИХ ЗАСОБІВ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

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

Стаття: 7 ***стор., 5 джерел.***

Найвищі показники якості радіоелектронного апарата можливо одержати за допомогою методів проектування, що дають можливість сформувати оптимальну структуру майбутнього радіоелектронного засобу (РЕЗ) у вигляді цільової функції – системи рівнянь, які описують основні функціональні властивості РЕЗ та їх взаємозв'язки.

Систему рівнянь цільової функції (ЦФ) РЕЗ можливо створити за допомогою методів теорії подібності у вигляді безрозмірних критеріальних рівнянь. Система містить як одиничні, так і частинні критерії, що описують основні процеси, які протікають у РЕЗ – електричні, механічні, теплові. ЦФ повинна бути подана числовим показником – комплексним критерієм, оптимизація якого забезпечить найвищі показники якості проектованого об'єкту.

Параметрична оптимізація ЦФ є задачею великої размірності (число параметрів, що варіюються, може досягати сотень й тисяч), а для цього необхідні ефективні методи умовної оптимізації та комп'ютери великої потужності (швидкодії).

Імітаційне моделювання показує, що раціональна компоновка електрорадіоелементів, мікросхем, функціональних вузлів на основі друкованої плати чи підкладки мікрозбірки може у багатьох випадках збільшити імовірність безвідмовної роботи РЕЗ при механічних впливах на 45 – 50%, а при теплових – на 20 – 35%; у результаті параметричної оптимізації топології конструктивних модулів з вказаними елементами буде одержана максимальная надійність конструкції РЕЗ.

Наведені приклади оптимізації конструкцій РЕЗ за допомогою розроблених авторами програм автоматизованого проектування та оптимізації.

ОПТИМИЗАЦИЯ ХАРАКТЕРИСТИК РАДИОЭЛЕКТРОННЫХ СРЕДСТВ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Борис Уваров, Юрий Зиньковский

Национальный технический университет Украины "Киевский политехнический институт"

Наивысшие показатели качества радиоэлектронного аппарата могут быть достигнуты с помощью методов проектирования, позволяющих сформировать оптимальную структуру будущего радиоэлектронного средства (РЭС) в виде целевой функции – системы уравнений, описывающих основные функциональные свойства РЭС и их взаимосвязи.

Систему уравнений целевой функции (ЦФ) РЭС можно получить с помощью методов теории подобия в виде безразмерных критериальных уравнений. Система содержит как единичные, так и частичные критерии, описывающие основные процессы, протекающие в РЭС – электрические, механические, тепловые. ЦФ должна быть выражена числовым показателем – комплексным критерием, оптимизация которого обеспечивает наивысшие показатели качества проектируемого объекта.

Параметрическая оптимизация ЦФ представляет собой задачу большой размерности (число варьируемых параметров может достигать сотен и тысяч), а для этого необходимы эффективные методы условной оптимизации и компьютеры большой мощности (быстродействия).

Имитационное моделирование показывает, что рациональная компоновка электрорадиоэлементов, микросхем, функциональных узлов на основании печатной платы или подложки микросборки может в ряде случаев повысить вероятность безотказной работы РЭС при механических воздействиях на 45 – 50%, а при тепловых – на 20 – 35%; в результате параметрической оптимизации топологии конструктивных модулей с указанными элементами будет получена максимальная надежность конструкции РЭС.

Приведены примеры оптимизации конструкций РЭС с помощью разработанных авторами программ автоматизированного проектирования и оптимизации.

OPTIMIZATION of the CHARACTERISTICS of RADIOELECTRONIC MEANS of TECHNICAL PROTECTION of the INFORMATION

Borys Uvarov, Yurij Zinkovsky

National technical university of Ukraine " the Kiev polytechnical institute "

The best parameters of quality of the radioelectronic device can be achieved with the help of methods of designing allowing to generate optimum structure of the future radioelectronic means (REM) as criterion function - of system of the equations, describing the basic functional property REM and their interrelation.

The system of the equations of criterion function (CF) REM can be received with the help of methods of the theory of similarity as dimensionless criterials of the equations. The system contains both individual, and partial criteria describing basic processes proceeding in REM - electrical, mechanical, thermal. CF should be expressed by a numerical parameter - complex criterion, which optimization provides the best parameters of quality of projected object.

The parametrical optimization CF represents a task of the large dimension (number of varied parameters can reach hundreds and thousand), and the effective methods of conditional optimization and high-power computers (speed) are necessary for this purpose.

The imitating modeling shows, that the rational configuration electroradioelements, microcircuits, functional units on the basis of the printed-circuit-board or substrate of microassembly can in a number of cases raise probability of non-failure operation REM at mechanical influences on 45 - 50 %, and at thermal - on 20 - 35 %; as a result of parametrical optimization of topology of constructive modules with the specified elements maximal reliability of a design REM will be received.

The examples of optimization of designs REV with the help of the programs, developed by the authors, of the automated designing and optimization are given.