4 Реферати

АЛГОРИТМ ПРОГНОЗУВАННЯ ТЕХНІЧНОГО СТАНУ КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Євгенія Іванченко, Володимир Хорошко, Юлія Хохлачова
Національний Авіаційний Університет

Стаття: 8 стор., 7 джерел.

Прогнозування технічного стану складних систем – складна і багатопланова задача. Системи захисту інформації відносять до складних технічних систем. Тому процеси, що відбуваються в інформаційній безпеці (ІБ), відносяться до складних, багатовимірних, динамічних, нестаціонарних, активних (цілеспрямованих), що надзвичайно ускладнює завдання прогнозування показників комплексних систем захисту інформації (КСЗІ).

Невід'ємною складовою завдань управління (оптимального, автоматизованого або на рівні прийняття рішень) є побудова моделей, які описують або прогнозують поведінку підсистем, процесів і системи в цілому. У загальному випадку для отримання математичної моделі необхідно вибрати її структуру і оцінити параметри, тобто вирішити завдання структурної ідентифікації. Структурна ідентифікація далі розглядатиметься як завдання пошуку структури моделі і мінімальної дисперсії помилки прогнозування.

Більшість методів побудовано на різних підходах, що ускладнює порівняльний аналіз умов їх ефективного застосування. Для задач управління в КСЗІ важливо створювати моделі з меншою помилкою прогнозування. Це є основою для порівняння ефективності існуючих підходів.

Мета такого підходу – виявлення прихованих закономірних причинно-наслідкових зв'язків між елементами досліджуваних процесів на основі статистичних даних, в яких ці зв'язки об'єктивно відображені.

Актуальною є проблема розробки алгоритму структурної ідентифікації прогнозуючих моделей з метою створення автоматизованих способів оптимального вибору структури моделей складних об'єктів за вибірками обмеженого об'єму в умовах неповноти інформації.

Запропоновано вирішення цієї задачі згідно з ідеологією методу групового обліку аргументів (МГУА). Доцільність використання МГУА пояснюється тим, що в ньому реалізуються ітераційні схеми ускладнення моделей. Ускладнення моделей від ряду до ряду селекції відбувається за рахунок «схрещування» кращих моделей попереднього ряду.

Аналіз критеріїв і методів показав, що для побудови математичної моделі нелінійної регресійної залежності доцільно використовувати:

а) МГУА метод перебору моделей;

б) метод найменших квадратів і метод модулів як методи оцінки параметрів моделей;

в) критерії залишкової суми квадратів, регулярності, ковзаючого контролю – для оцінки якості одержуваних моделей.

Особливістю пропонованого алгоритму є:

1) багатоетапність пошуку моделі;

2) пошук моделі як у класі лінійних, так і в класі нелінійних за вхідними змінними моделей;

3) прийоми виключення окремих членів кращого окремого опису і на основі цього – розширення базисного набору аргументів;

4) оптимальна за обчислювальними затратами для ітераційних алгоритмів МГУА схема розрахунку критерію ковзаючого іспиту;

5) можливість оцінювати коефіцієнти в моделях як за методом найменших квадратів, так і за методом найменших модулів.

Крім того, алгоритм дозволяє прогнозувати технічний стан КСЗІ, а це в свою чергу дає можливість забезпечувати необхідний рівень інформаційної безпеки об'єктів різних класів, складності і призначення.

АЛГОРИТМ ПРОГНОЗИРОВАНИЯ ТЕХНИЧЕСКОГО СОСТОЯНИЯ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Евгения Иванченко, Владимир Хорошко, Юлия Хохлачева
Национальный Авиационный Университет

Прогнозирование технического состояния сложных систем – сложная и многоплановая задача. Системы защиты информации относят к сложным техническим системам. Поэтому процессы, происходящие в информационной безопасности (ИБ), относятся к сложным, многомерным, динамическим, нестационарным, активным (целенаправленным), что чрезвычайно усложняет задачу прогнозирования показателей комплексных систем защиты информации (КСЗИ).

Неотъемлемой составной частью задач управления (оптимального, автоматизированного или на уровне принятия решений) является построение моделей, описывающих или прогнозирующих поведение подсистем, процессов и системы в целом. В общем случае для получения математической модели необходимо выбрать ее структуру и оценивать параметры, то есть решать задачи структурной идентификации. Структурная идентификация нами будет рассматриваться как задача поиска структуры модели и минимальной дисперсии ошибки прогнозирования.

Большинство методов построено на различных подходах, что затрудняет сравнительный анализ определения условий их эффективного применения. Для задач управления в КСЗИ важно создавать модели с меньшей ошибкой прогнозирования. Это является основой для сравнения эффективности существующих подходов.

Цель такого подхода - выявление скрытых закономерных причинно-следственных связей между элементами исследуемых процессов на основе статистических данных, в которых эти связи объективно отражены.

Актуальной является проблема разработки алгоритма структурной идентификации прогнозирующих моделей с целью создания автоматизированных способов для оптимального выбора структуры моделей сложных объектов по выборкам ограниченного объема в условиях неполноты информации.

Предположено решение этой задачи в соответствии с идеологией метода группового учета аргументов (МГУА). Целесообразность использования МГУА объясняется тем, что в нем реализуются итерационные схемы осложнения моделей. Осложнения моделей от ряда к ряду селекции происходит за счет «скрещивания» лучших моделей предыдущего ряда.

Анализ критериев и методов показал, что для построения математической модели нелинейной регрессионной зависимости целесообразно использовать:

а) МГУА в качестве метода перебора моделей;

б) метод наименьших квадратов и метод модулей в качестве методов оценки параметров моделей;

в) критерии остаточной суммы квадратов, регулярности, скользящего контроля для оценки качества получаемых моделей.

Особенностью предлагаемого алгоритма является:

1) многоэтапность поиска модели;

2) поиск модели как в классе линейных, так и в классе нелинейных по входным переменным моделей;

3) приемы исключения отдельных членов лучшего частного описания и на основе этого – расширение базисного набора аргументов;

4) оптимальная по вычислительным затратам итерационных алгоритмов МГУА схема расчета критерия скользящего экзамена;

5) возможность оценивать коэффициенты в моделях как по методу наименьших квадратов, так и по методу наименьших модулей.

Кроме того, алгоритм позволяет прогнозировать техническое состояние КСЗИ, а это в свою очередь дает возможность обеспечивать необходимый уровень информационной безопасности объектов различных классов, сложности и назначения.

PREDICTION ALGORITHM TECHNICAL STATE OF COMPLEX SYSTEMS OF INFORMATION

Yevgeny Ivanchenko, Vladimir Khoroshko, Julia Hohlacheva
National Aviation University

Prediction of the technical condition of complex systems is complex and multifaceted problem of information security systems are complex technical systems. Therefore, the processes taking place in the information security (IS), are complex, multidimensional, dynamic, time-dependent, active (focused), making it extremely difficult task of forecasting performance of integrated security systems (KSZI).

An integral part of the management tasks (optimal, automated, or at the level of decision-making) is to construct models that describe or predict the behavior of sub-systems, processes, and systems in general. In general, to obtain a mathematical model to choose its structure and to estimate the parameters, that is, to solve the problem of structural identification. Structural identification of us will be treated as the problem of finding the model structure and the minimum variance of the prediction error.

Most of the methods is based on different approaches, which complicates the comparative analysis to determine the conditions of their effective application. As for the problems of governance in KSZI important to create a model with a smaller prediction error, it is the basis for comparing the effectiveness of existing approaches.

The purpose of this approach - identifying hidden patterns of cause-effect relationships between the elements of the investigated processes on the basis of statistical data, in which the connection is objectively reflected.

The actual problem is the structural identification algorithm development of predictive models for the creation of automated methods for selecting the optimal structure of the complex object models for samples of limited volume in conditions of incomplete information.

We consider this problem in accordance with the ideology of the group method of data handling (GMDH). The feasibility of using GMDH because it implemented iterative schemes complication models. The increasing complexity of the models from row to row selection is due to "crossing" of the best models of the previous row.

Analysis of criteria and methods showed that the mathematical model of the nonlinear regression dependence should be used:

a) GMDH as a method of sorting models;

b) the method of least squares method as a method of modules rated model parameters;

a) the criteria for the residual sum of squares, regularity, cross-validation to assess the quality of the models.

Feature of the proposed algorithm is:

1) multi-stage search model;

2) The search for a model in the class of linear and non-linear in the class of the input variables of the model;

3) techniques to exclude certain members of the best descriptions of the private and based on this extension of the basis set of arguments;

4) optimal with respect to computational cost for iterative algorithms GMDH calculation scheme criterion sliding examination;

5) the ability to estimate the coefficients of the model as the method of least squares, and the least modules.

In addition, the algorithm can predict the technical condition KSZI, and this in turn enables us to provide the required level of security of objects of different classes, the complexity and purpose.

Literatura: ***1****. Tikhonov A. N. Metody resheniya nekorrektnykh zadach / Tikhonov A. N., Arsenin V. Ya. – M.: Nauka, 1974. – 458 s.* ***2****. Osnovy ekonomicheskogo i sotsial'nogo prognozirovaniya / Pod red. Mosina N. – M.: Vysshaya shkola, 1985. – 386 s.* ***3.*** *Begma T. V. Matematichni modeli funktsionuvannya skladnikh sistem / Begma T. V., Kapustyan M. V., Khoroshko V. O. / Visnik SNU im. V. Dalya, №7(161), 2.1, 2011. – S. 252–263.* ***4.*** *Vuchkov I. Prikladnoy lineynyy regressionnyy analiz / Vuchkov I., Boldzhneva L., Salakov YE. – M.: Finansy i statistika, 1987. – 239 s.* ***5.*** *Stepashko V. S. Metody i kriterii resheniya zadach strukturnoy identifikatsii / Stepashko V. S., Kocherga Yu. L. // Avtomatika, №5, 1985. – S. 29–37.* ***6.*** *Sarychev A. P. Resheniye problemy razbiyeniya v MGUA pri raschete kriteriya regulyarnosti v usloviyakh aktivnogo eksperimenta / Sarychev A. P. // Avtomatika, №4, 1989. – S. 19–27.* ***7.*** *Golovan' S. M. Osnovi nadiynosti informatsiynikh sistem / Golovan' S. M., Korneyko O. V., Petrov O. S., Khoroshko V. O., Shcherbak L. M. – Lugans'k: Vid. «Naulidzh», 2012. – 335 s.*

УДК 004.924:534.6.08

МАТЕМАТИЧНА МОДЕЛЬ ЗМІНИ ПАРАМЕТРІВ ВОДНОГО СЕРЕДОВИЩА ЯК КАНАЛУ ТРАНСЛЯЦІЇ МОВНОВОЇ ІНФОРМАЦІЇ, ЩО ЗНІМАЄТЬСЯ

Олена Азаренко, Михайло Дівізінюк, Юлія Гончаренко, Дмитро Гончаренко
Севастопольський національний університет ядерної енергії та промисловості

Стаття: 6 стор., 3 джерела

Знімання мовної інформації в загальному випадку зводиться до рішення окремих завдань: безпосередня реєстрація мікрофонними пристроями, трансляція перетворених сигналів до приймального пристрою, перетворення отриманих сигналів у виді, необхідному зловмисникові. Трансляція перетворених сигналів може здійснюватися по конструктивних комунальних системах, вбудованих в адміністративних й житлових будівлях та спеціалізованих спорудах. Тут в системах водозабезпечення, водяною пожежною і водяною системах опалювання може здійснюватися ретрансляція шляхом модуляції високочастотного акустичного сигналу мовною інформацією, що знімається. На поширення високочастотного акустичного сигналу можуть впливати сторонні домішки, що потрапили в одну з водяних систем, використовуваних для трансляції даних, спотворюючи передавані сигнали. Рішення подібної задачі, а саме, зміна швидкості звуку залежно від кількості домішки, відноситься до класу завдань математичної фізики і вирішується наближеними методами.

Отримані результати показують, що, незалежно від властивостей домішки, її наявність призводить до зменшення швидкості звуку у воді, причому величина цієї зміни пропорційна концентрації домішки. Отримана математична модель показує, що для вирішення завдань протидії ретрансляції даних по водному каналу необхідно вводити домішки, які викликають зменшення швидкості звуку і спотворення передаваної інформації. Прикладами подібних дій можуть служити установка антикорозійних присадок в системи водяного опалювання або створення у водоймах областей аерації - повітряних бульбашок, шляхом нагнітання повітря у водне середовище за допомогою компресора.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ИЗМЕНЕНИЯ ПАРАМЕТРОВ ВОДНОЙ СРЕДЫ КАК КАНАЛА ТРАНСЛЯЦИИ СНИМАЕМОЙ РЕЧЕВОЙ ИНФОРМАЦИИ

Елена Азаренко, Михаил Дивизинюк, Юлия Гончаренко, Дмитрий Гончаренко
Севастопольский национальный университет ядерной энергии и промышленности

Съем речевой информации в общем случае сводится к решению частных задач: непосредственная регистрация микрофонными устройствами, трансляция преобразованных сигналов к приемному устройству, преобразование полученных сигналов в виде, необходимом злоумышленнику. Трансляция преобразованных сигналов может осуществляться по конструктивным коммунальным системам, встроенным в административных и жилых зданиях и специализированных сооружениях. Здесь в системах водообеспечения, водяной пожарной и водяной системах отопления может осуществляться ретрансляция путем модуляции высокочастотного акустического сигнала снимаемой речевой информацией. На распространение высокочастотного акустического сигнала могут оказывать воздействие посторонние примеси, попавшие в одну из водяных систем, используемых для трансляции данных, искажая передаваемые сигналы. Решение подобной задачи, а именно, изменение скорости звука в зависимости от количества примеси, относится к классу задач математической физики и решается приближенными методами.

Полученные результаты показывают, что, независимо от свойств примеси, ее наличие приводит к уменьшению скорости звука в воде, причем величина этого изменения пропорциональна концентрации примеси. Полученная математическая модель показывает, что для решения задач противодействия ретрансляции данных по водному каналу необходимо вводить примеси, которые вызывают уменьшение скорости звука и искажение передаваемой информации. Примерами подобных действий могут служить установка антикоррозийных присадок в системы водяного отопления или создание в водоемах областей аэрации – воздушных пузырьков, путем нагнетания воздуха в водную среду с помощью компрессора.

MATHEMATICAL MODEL OF CHANGE PARAMETERS OF THE WATER ENVIRONMENT AS A BROADCAST CHANNEL TO SHOOT THE SPEECH INFORMATION

Elena Azarenko, Michael Divizinyuk, Julia Goncharenko, Dmitry Goncharenko
Sevastopol National University of Nuclear Energy and Industry

The output of speech information in general case is taken to the decision of private tasks : direct registration by microphonic devices, translation of regenerate signals to the takers-off, transformation of the got signals to the kind, necessity to the malefactor. Translation of regenerate signals can come true on the structural communal systems built-in in administrative and dwellings building and specialized building. Here in the systems of водообеспечения, by an aquatic fire and aquatic systems of heating retransmitting can come true by modulation of high-frequency acoustic signal the taken off speech information. On distribution of high-frequency acoustic signal can render influence strangers admixtures, getting in one of the aquatic systems used for translation of data, distorting transferrable signals. Decision of similar task, namely, change of speed of sound depending on the amount of admixture, behaves to the class of tasks of mathematical physics and decides close methods.

The got results show that, regardless of properties of admixture, her presence results in diminishing of speed of sound in water, thus the size of this change is proportional to the concentration of admixture. The got mathematical model shows that for the decision of tasks of counteraction of retransmitting of data on a water channel it is necessary to enter admixtures which cause diminishing of speed of sound and distortion of transferrable information. The examples of similar actions can serve as setting of antirust additives in the systems of the aquatic heating or creation in the reservoirs of areas of airing - air phials, by air-blasting in a water environment by means of compressor.

Literatura 1. Metody i sredstva zashchity informatsii / S .V. Lenkov, D. A. Peregudov, V. A. Khoroshko. – Kiyev: ARIY, 2008. – T. 1. – 464 s. 2. Azarenko E. V. Razrabotka matematicheskoy modeli sinkhronnykh izmereniy / E V. Azarenko, Yu. Yu. Goncharenko, M. M. Divizinyuk i dr. // Sb. nauk. prats' SNUYAEtaP. – Vip. 1(37). – Sevastopol': SNUYAEtaP, 2011. – S. 225 – 231. 3. Divizinyuk M. M. Razrabotka matematicheskoy modeli identifikatsii slozhnykh akusticheskikh signalov // M. M. Divizinyuk, E. E. Smychkov, V. V. Shilin i dr. // Sb. nauk. prats' SNUYAEtaP. – Vip. 2(38). – Sevastopol': SNUYAYEtaP, 2011. – S. 257 – 261.

УДК 681.391

АНАЛИЗ И МОДЕЛИРОВАНИЕ РЕЗУЛЬТАТОВ АРТИКУЛЯЦИОННЫХ ИСПЫТАНИЙ

Александр Архипов, Елена Архипова
Национальный технический университет Украины "КПИ"

*Статья: **7 стр., 9 источников**.*

Рассмотрена задача анализа и обработки данных артикуляционной экспертизы, полученных бригадой аудиторов при распознании фрагментов речевой информации (слов артикуляционных таблиц) с аддитивно наложенным на них шумом, имитирующим влияние маскирующей помехи. Предложена описательная модель процесса возникновения ошибок у аудитора при распознавании им искаженных маскирующей помехой слов. Модель позволяет на качественном уровне интерпретировать особенности и характеристики ошибок аудитора, объяснить форму закона распределения погрешностей оценок разборчивости и в ряде случаев может быть использована для построения аппроксимативной математической модели этого распределения.

Предполагается, что действительный механизм возникновения ошибок аудиторов реализует сложноформализуемую зависимость их индивидуальных качеств от уровня и характеристик шумового маскирующего сигнала, связанную с физиологическими параметрами и эмоционально-интеллектуальными свойствами аудиторов. В этом случае погрешность оценок словесной разборчивости подчиняется нормальному закону со случайным средним квадратическим отклонением, распределенным по закону Рэлея.

Приведены аппроксимативные математические модели зависимостей словесной разборчивости и среднеквадратической погрешности ее оценивания от значений индикаторных переменных, определяемых непосредственно по данным артикуляционных испытаний.

АНАЛІЗ І МОДЕЛЮВАННЯ РЕЗУЛЬТАТІВ АРТИКУЛЯЦІЙНИХ ВИПРОБУВАНЬ

Олександр Архипов, Олена Архипова
Національний технічний університет України "КПІ"

Розглянуто задачу аналізу і обробки даних артикуляційної експертизи, отриманих бригадою аудиторів при розпізнанні фрагментів мовної інформації (слів артикуляційних таблиць) з адитивно накладеним на них шумом, що імітує вплив маскуючої завади. Запропоновано описову модель процесу виникнення помилок у аудитора при розпізнаванні ним слів, спотворених маскуючою завадою. Модель дозволяє на якісному рівні інтерпретувати особливості і характеристики помилок аудитора, пояснити форму закону розподілу похибок оцінок розбірливості та в низці випадків може бути використана для побудови апроксимативної математичної моделі цього розподілу.

Передбачається, що дійсний механізм виникнення помилок аудиторів реалізує залежність їх індивідуальних якостей від рівня і характеристик шумового маскуючого сигналу, пов'язану з фізіологічними параметрами і емоційно-інтелектуальними властивостями аудиторів. Ця залежність є складною для формалізації. У цьому випадку похибки оцінок словесної розбірливості розподілені за нормальним законом з випадковим середнім квадратичним відхиленням, розподіленим за законом Релея.

Наведені апроксимативні математичні моделі залежностей словесної розбірливості і середньоквадратичної похибки її оцінювання від значень індикаторних змінних, які визначаються безпосередньо за даними артикуляційних випробувань.

ANALYSIS AND MODELING OF ARTICULATION TESTS RESULTS

Aleksandr Arkhypov, Elena Arkhypova
National Technical University of Ukraine "KPI"

It is considered the task of analysis and processing of articulation tests data, team of auditors got at recognitions of speech information fragments (words of articulation tables) with additive noise overlaid on them, simulating the effect of masking noise. A descriptive model of errors origin at recognition by the auditor the masking hindrance distorted words is offered. This model allows qualitatively interpreting features of the auditor errors, explaining the shape of the intelligibility evaluation error distribution and in some cases can be used to construct an approximate mathematical model of this distributing.

It is assumed that the actual mechanism of auditors' errors origin realizes difficult formalizable dependence from their individual qualities and characteristics of the noise masking signal level, related to the physiological parameters of auditors and their emotional and intellectual properties. In this case the word intelligibility evaluation error submits a normal distribution with random standard deviation distributed according to the Rayleigh law.

The second paper part shows the approximate mathematical model of dependences of word intelligibility and its estimation standard error from the indicator variables values, determined directly from the articulation tests data.

Literatura: **1**. Arkhipova O. O., Zhuravl'ov V. M., Kumeyko V. M. Artikulyatsiyni tablitsi sliv ukraïns'koï movi / O. O. Arkhipova, V. M. Zhuravl'ov, V. M. Kumeyko // Pravove, normativne ta metrologichne zabezpechennya sistemi zakhistu informatsiï v Ukraïni. – K., 2009. – № 2/19. – S. 13-17. **2**. Arkhipova O. O., Zhuravl'ov V. M., Dorovs'kikh A. V. Tablitsi sliv ukraïns'koï movi dlya artikulyatsiynikh viprobuvan' rozbirlivosti informatsiï, shcho peredaєt'sya traktami zv'yazku / O. O. Arkhipova, V. M. Zhuravl'ov, A. V. Dorovs'kikh // Zv'yazok. – K., 2010. – № 1 (89). – S. 9-11. **3**. Arkhipov A. E. Analiz i obrabotka dannykh artikulyatsionnykh ispytaniy / A. E. Arkhipov, E. A. Arkhipova // Zakhist informatsiï. – 2012. – №4 (57), – S.34 – 42. **4**. Mudrov V. I. Metody obrabotki oshibok izmereniy / V. I. Mudrov, V. L. Kushko – M., Sovetskoye radio, 1976. – 192 s. **5**. Arkhipov A. YE. O modelirovanii nekotorykh tipov sluchaynykh posledovatel'nostey / A. E. Arkhipov // Vestnik Kiyev. politekhn. in-ta – Vyp. 12. – K.:1988 – S. 39-44. **6**. Arkhipov O. E. Model' oshibok ekspertnykh otsenok / O. E. Arkhipov, S. A. Arkhipova // "Suchasni problemi upravlinnya", Materiali IV Mizhnarodnoï nauk.-praktichnoï konferentsiï (28-30 listopada 2007r., m.Kiïv). – IVTS Vidavnitstvo "Politekhnika"– K.: 2007. – S. 65-66. **7**. Venttsel' E. S., Ovcharov L. A. Teoriya veroyatnostey i yeyo inzhenernyye prilozheniya / E. S. Venttsel', L. A. Ovcharov – M.: Nauka, 1988. – 480 s. **8**. Pugachev V.S. Teoriya veroyatnostey i matematicheskaya statistika / V. S. Pugachev – M.: Nauka, 1979. – 496 s. **9**.

Gradshteyn I. S. Tablitsy integralov, summ, ryadov i proizvedeniy / I. S. Gradshteyn, I. M. Ryzhik – M.: GIFML, 1971.

УДК 343/974

СТРУКТУРА КРИМІНАЛЬНИХ ВІДНОСИН У КІБЕРПРОСТОРІ

Ігор Гриненко, Дарія Прокоф'єва-Янчиленко*, Михайло Прокофьєв**

*Національна академія Служби безпеки України, *Служба безпеки України, **НДЦ "ТЕЗІС" НТУУ "КПІ"*

Стаття: ***6 стр., 12 джерел.***

Організована злочинність є одним із найнебезпечніших суспільних явищ, що становить безпосередню загрозу національній безпеці окремих країн та міжнародному правопорядку у цілому. Найбільшої небезпеки організована злочинність набуває у формі транснаціональної протиправної діяльності, не обмеженої державними кордонами та географічними відстанями. Транснаціоналізації злочинності, набуттю нею якісно нових рис сприяє використання організованими злочинними угрупуваннями новітніх телекомунікаційних технологій як для забезпечення вчинення «традиційних» злочинів, наприклад, у сфері наркобізнесу, торгівлі людьми та зброєю, нелегальної міграції тощо, так і здійснення принципово нових видів протиправної діяльності, безпосередньо пов'язаних із функціонуванням кіберпростору.

Сприятливі умови, що їх забезпечує специфіка кіберпростору маргінальним спільнотам, призводять до появи численних зон спілкування осіб з девіантною поведінкою. Глобалізація злочинності розглядається як тенденція, що в майбутньому може лише посилюватися, що, у свою чергу, сприятиме подальшому збільшенню могутності злочинних угрупувань.

При цьому структура організованих угрупувань набуває горизонтального мережевого характеру, за якого ані власна самоідентифікація, ані тривале членство надалі не можуть бути характерними для злочинних структур, що діятимуть у кіберпросторі. Такі структури формуватимуться під конкретну операцію і матимуть плинну, відкриту та мінливу природу. Єдиною передумовою членства у таких структурах є особисте бажання, намір вчинити протиправні діяння, а також наявність відповідних навичок. Кіберпростір дає додаткові можливості для приховування особистості злочинців, що, відповідно, робить менш важливою особисту довіру між членами організації, однак підвищує значення збереження конфіденційності інформації та заходів її захисту від несанкціонованого доступу. Використання телекомунікаційних технологій для забезпечення незаконних операцій «традиційними» організованими злочинними угрупуваннями також є одним із чинників їх переформатування відповідно до мережевої моделі, як це має місце і в легальних транснаціональних корпораціях

Окреслена вище специфіка кіберзлочинності створюватиме додаткові ускладнення для здійснення правоохоронної діяльності, однак і відкриває для них нові можливості, що, в свою чергу, потребує не лише розробки нової парадигми правоохоронної діяльності, а й ставить нові вимоги до рівня підготовки співробітників компетентних органів, що повинні мати відповідні навички автономної діяльності, прийняття самостійних рішень та швидкого реагування на зміни в обстановці.

СТРУКТУРА КРИМИНАЛЬНЫХ ОТНОШЕНИЙ В КИБЕРПРОСТРАНСТВЕ

Игорь Гриненко, Дария Прокофьева-Янчиленко*, Михаил Прокофьев**

*Национальная академия Службы безопасности Украины, *Служба безопасности Украины, **НДЦ "ТЕЗИС" НТУУ "КПИ"*

Организованная преступность является одним из наиболее опасных общественных явлений, которое представляет непосредственную угрозу национальной безопасности отдельных стран и международному правопорядку в целом. Самую большую опасность организованная преступность приобретает в форме транснациональной противоправной деятельности, не ограниченной государственными границами и географическими расстояниями. Транснационализации преступности, обретению ею качественно новых черт содействует использование организованными преступными группировками новейших телекоммуникационных технологий как для обеспечения совершения «традиционных» преступлений, например, в сфере наркобизнеса, торговли людьми и оружием, нелегальной миграции и т. п., так и

осуществление принципиально новых видов противоправной деятельности, непосредственно связанных с функционированием киберпространства.

Благоприятные условия, которые обеспечивает специфика киберпространства маргинальным сообществам, приводят к появлению многочисленных зон общения лиц с девиантным поведением. Глобализация преступности рассматривается как тенденция, которая в будущем может лишь усиливаться, что, в свою очередь, будет содействовать дальнейшему увеличению могущества преступных группировок.

При этом структура организованных группировок приобретает горизонтальный сетевой характер, при котором ни собственная самоидентификация, ни продолжительное членство в дальнейшем не могут быть характерными для преступных структур, которые будут действовать в киберпространстве. Такие структуры будут формироваться под конкретную операцию и будут иметь текучую, открытую и непостоянную природу. Единственной предпосылкой членства в таких структурах является личное желание, намерение на совершение противоправных действий, а также наличие соответствующих навыков. Киберпространство дает дополнительные возможности для сокрытия личности преступников, что, соответственно, делает менее важным личное доверие между членами организации, однако повышает значение сохранения конфиденциальности информации и мер ее защиты от несанкционированного доступа. Использование телекоммуникационных технологий для обеспечения незаконных операций «традиционными» организованными преступными группировками также является одним из факторов их переформатирования по образу сетевой модели, как это имеет место и в легальных транснациональных корпорациях.

Обозначенная выше специфика киберпреступности может создавать дополнительные осложнения для осуществления правоохранительной деятельности, однако и открывает для них новые возможности, которые, в свою очередь, нуждаются не только в разработке новой парадигмы правоохранительной деятельности, но и ставит новые требования к уровню подготовки сотрудников компетентных органов, которые должны иметь соответствующие навыки автономной деятельности, принятия самостоятельных решений и быстрого реагирования на изменения в обстановке.

STRUCTURE OF CRIMINAL RELATIONS IN CYBERSPACE

Igor Grynenko, Daria Prokof'eva-Yanchilenko*, Mikhail Prokofiev**

*National academy of security of Ukraine Service, *Service safety of Ukraine, ** SRC "TEZIS" NTUU "KPI"*

Organized crime is one of the most dangerous social phenomena, which presents direct threat to national security of individual states as well as international law and order in general. Organized crime acquires its most dangerous nature in the form of transnational unlawful activity not limited by state borders or geographical distances. The use of newest telecom technologies by organized criminal groups contributes to the transnationalization of crime and the appearance of its new characteristics. These technologies are used both to commit "traditional" crime like drug trafficking, THB, illegal migration, etc., and to commit new kinds of illicit activity which refer to the cyberspace itself.

These specific conditions of cyberspace contribute to the emergence of numerous communication zones for persons with deviant behavior. Globalization of crime is regarded as a trend which may only reinforce in the future, which in its turn will help boost the power of criminal groups.

Alongside with this, the structure of organized groups acquires horizontal network nature which means that neither self-idetification, nor continuous membership in the group will be characteristic for the groups acting in cyberspace. These structures will form for the specific operation and will have fluctuating, open and changing structure. The only prerequisite for membership in the group will be a personal wish, an intention to commit illegal actions as well as availability of the skills needed. Cyberspace provides additional opportunities for hiding the criminals' identities, which reduces the importance of trust between members, however increases the importance of confidentiality and information protection. The use of telecom technologies to provide illegal operations by organized criminal groups is one of the reasons they reformat into the network model as it is within legal transnational corporations.

The aforementioned specifics of cybercrime will help create additional burden in carrying out law enforcement, however it also opens up new opportunities for these agencies. Therefore, this not only requires development of a new paradigm of law enforcement activity, but also sets demands to the level of training of the personnel of responsible agencies, who should possess skills of self-sustained activity, individual decision-making and fast response to the changes in the environment.

Literatura: ***1****. Pro Kontseptsiyu derzhavnoy politiki u sferi borot'bi z organizovanoyu zlochinnistyu: Ukaz Prezidenta Ukrayny vid 21 zhovtnya 2011 roku №1000/2011. – Uryadoviy kur'єr vid 29.10.2011 — № 201.* ***2.*** *Zakonu Ukrayni «Pro organizatsiyno-pravovi osnovi borot'bi z organizovanoyu zlochinnistyu». [Elektronniy resurs]. – Rezhim dostupu: http://www.rada.com.ua* ***3.*** *Kriminal'niy kodeks Ukrayni.[Elektronniy resurs]. – Rezhim dostupu: http://www.rada.com.ua* ***4.*** *Konventsiya OON proti transnatsional'noї organizovanoy zlochinnosti. 2000 r.[Elektronniy resurs]. – Rezhim dostupu: http://www.rada.com.ua* ***5.*** *McClure G. The Role of Interpol in Fighting Organized Crime /481 International Criminal Police Review (2000) – Interpol. [Elektronniy resurs]. – Rezhim dostupu: http://www.interpol.int/Public/Publications/ICPR/ICPR481_1.asp* ***6.*** *Family Cities, AmericanMafia.com [Elektronniy resurs]. – Rezhim dostupu: http://www.americanmafia.com/ 26_Family_Cities.html* ***7.*** *Castelli B. The Globalization of the Drug Trade. – Apr. 1999. [Elektronniy resurs]. – Rezhim dostupu: http://www.unesco.org/most/sourdren.pdf* ***8.*** *Shelley L., Director, Center for Transnational Organized Crime and Corruption, Testimony Before the House Committee on International Relations. – October 1, 1997. [Elektronniy resurs]. – Rezhim dostupu: http://www.fas.org/irp/congress/1997_hr/h971001ls.htm.* ***9.*** *Brenner S. W. Organized Cybercrime How Cyberspace May Affect the Structure of Criminal Relationships / North Carolina Journal of Law & Technology. –Volume 4, Issue 1: Fall 2002. – 50 p. [Elektronniy resurs]. – Rezhim dostupu: http://www.rand.org/publications/MR/MR880.* ***10.*** *Teoriya operativno-rozysknoy deyatel'nosti: Uchebnik. 2-ye izd., pererab. i dop./Pod red. K. K. Goryainova, V. S. Ovchinskogo, G. K. Sinilova. – M.: INFRA-M, 2012. – Kh., 690 s.* ***11.*** *Arquilla J. In Athena's Camp: Preparing for Conflict in the Information Age/ J.Arquilla, D. Ronfeldt. – 1997.* ***12.*** *Arquilla J. David Ronfeldt, Swarming and the Future of Conflict / J.Arquilla, D. Ronfeldt. – 2000. [Elektronniy resurs]. – Rezhim dostupu: http://www.rand.org/publications/DB/DB311.pdf*

УДК 35.078:342.738

ДЕЯКІ ПРАКТИЧНІ АСПЕКТИ РЕАЛІЗАЦІЇ ЗАХОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПІД ЧАС ЇХ ОБРОБКИ В ІНФОРМАЦІЙНИХ (АВТОМАТИЗОВАНИХ) СИСТЕМАХ

Олексій Мервінський, *Микола Щербак

*Державна служба захисту персональних даних, *ТОВ «Data Protection Development»*

Статья: ***5 стр., 13 джерел***

Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» передбачено, що інформація з обмеженим доступом (до якої віднесено і персональні дані) повинна оброблятися в інформаційно-телекомунікаційній (інформаційній) системі (ІТС/ІС) із застосуванням комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю. В статті обгрунтовуються вимоги щодо системи захисту персональних даних (ПД) в Україні такого рівня, щоб не суперечить положеннями європейських директив і вимогами правових і нормативних документів системи ТЗІ України.

Наказом Мініюсту України № 3659/5 встановлено Типовий порядок - мінімальний перелік робіт, які необхідно реалізувати володільцю ПД під час організації заходів із їх захисту. Цей порядок передбачає застосування в ІТС/ІС мережевого захисту від несанкціонованого доступу під час обробки ПД, впровадження процедур авторизації працівників, забезпечення антивірусного захисту, а також використання технічних засобів безперебійного живлення елементів ІТС/ІС. Типовий порядок враховує Директиви 95/46/ЄС, 97/66/ЄС Європарламенту та Ради Європи таким чином, щоб юридичні, нормативні та технічні вимоги, які регламентують забезпечення захисту ПД, прав фізичних осіб та законних інтересів юридичних осіб, були чітко збалансованими та не створювали перешкод для розвитку ринку. Дані заходи не повинні спричиняти володільцю ПД великі фінансові навантаження на створення систем захисту ПД, але при цьому мати належний (достатній) рівень захисту ІТС/ІС володільця. Досягнення такого балансу є можливим за умови визначення обмеженої та обгрунтованої кількості вимог, що не перешкоджають розвитку новітніх технологій та належному функціонуванню баз ПД, зокрема, можуть розроблятися корпоративні кодекси поведінки (кодекси практики) з обробки ПД, які системно розкривають основні правила обробки і захисту ПД.

Остаточний вибір конкретних заходів захисту, технічних рішень та стандартів, якими необхідно керуватися, архітектур ІТС/АС залишається в межах компетенції володільця ПД. Так само в компетенції володільця знаходиться й безпосередня оцінка ризиків порушень безпеки даних. Типовим порядком взагалі не передбачується необхідність створення КЗЗ в базах ПД при їх обробці у складі ІТС/ІС. Одночасно з

мінімально необхідним обов'язковим використанням паролів, що регулярно змінюються, Директиви 95/46/ЄС, 97/66/ЄС також вимагають регулярного перегляду прав доступу.

Доцільно також розширити перелік видів ІТС/ІС, що обробляють ПД, для яких можливо застосовувати за бажанням їх Власника (Розпорядника) замість державної експертизи КСЗІ процедуру аналізу відомостей декларації про відповідність КСЗІ вимогам нормативних документів з ТЗІ уповноваженим центральним органом виконавчої влади з питань захисту інформації – Адміністрацією Держспецзв'язку.

НЕКОТОРЫЕ ПРАКТИЧЕСКИЕ АСПЕКТЫ РЕАЛИЗАЦИИ МЕРОПРИЯТИЙ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ВО ВРЕМЯ ИХ ОБРАБОТКИ В ИНФОРМАЦИОННЫХ (АВТОМАТИЗИРОВАННЫХ) СИСТЕМАХ

Алексей Мервінський, *Николай Щербак

*Государственная служба защиты персональных данных, *ООО "Data Protection Development"*

Согласно Закону Украины "О защите информации в информационно-телекоммуникационных системах" предусмотрено, что информация с ограниченным доступом (к которой отнесены и персональные данные) должна обрабатываться в информационно-телекоммуникационной (информационной) системе (ИТС/ИС) с применением комплексной системы защиты информации (КСЗИ) с подтвержденным соответствием. В статье обосновываются требования относительно системы защиты персональных даннях (ПД) в Украине такого уровня, чтобы не существовало противоречия между положениями европейских директив и требованиями правовых и нормативных документов системы ТЗИ Украины.

Приказом Минюста Украины № 3659/5 установлен Типовый порядок – минимальный перечень работ, какие необходимо реализовать владельцу ПД во время организации мероприятий по их защите. Этот порядок предусматривает использование в ИТС/ИС сетевой защиты от несанкционированного доступа во время обработки ПД, внедрение процедур авторизации работников, обеспечения антивирусной защиты а также использование технических средств бесперебойного питания элементов ИТС/ИС. Типовый порядок учитывает Директивы 95/46/ЕС, 97/66/ЕС Европарламента и Совета Европы таким образом, чтобы юридические, нормативные и технические требования, которые регламентируют обеспечение защиты ПД, прав физических лиц и законных интересов юридических лиц, были четко сбалансированными и не создавали препятствий для развития рынка. Данные мероприятия не должны вызывать у владельца ПД большие финансовые нагрузки на создание систем защиты ПД, но при этом иметь надлежащий (достаточный) уровень защиты ИТС/ИС владельца. Достижение такого баланса является возможным при условии определения ограниченного и обоснованного количества требований, которые не препятствуют развитию новейших технологий и надлежащему функционированию баз ПД, в частности могут разрабатываться корпоративные кодексы поведения (кодексы практики) по обработке ПД, которые системно раскрывают основные правила обработки и защиты ПД.

Окончательный выбор конкретных мер защиты, технических решений и стандартов, которыми необходимо руководствоваться, архитектур ИТС/ИС остается в пределах компетенции владельца ПД. Так же в компетенции владельца находится и непосредственная оценка рисков нарушений безопасности данных. Типовым порядком вообще не предусматривается необходимость создания КСЗ в базах ПД при их обработке в составе ИТС/ИС. Одновременно с минимальной необходимостью обязательного использования паролей, которые регулярно изменяются, Директивы 95/46/ЕС, 97/66/ЕС также требуют регулярного пересмотра прав доступа.

Целесообразно также расширить перечень видов ИТС/ИС, обрабатывающих ПД, для которых возможно применять по желанию их Владельца (Распорядителя) вместо государственной экспертизы КСЗИ процедуру анализа сведений декларации о соответствии КСЗИ требованиям нормативных документов системы ТЗИ уполномоченным центральным органом исполнительной власти по вопросам защиты информации - Администрацией Госспецсвязи.

SOME PRACTICAL ASPECTS OF PROCEDURES REALIZATION OF THE PERSONAL DATA PROTECTION ARE DURING THEIR TREATMENT IN INFORMATIVE(AUTOMATED) SYSTEMS

Oleksij Mervinskiy, *Mykola Scherbuck
*Government service of the personal data protection, *LTD. "Data Protection Development"*

Due to the Law of Ukraine "On information defence in the informational and telecomunicative systems" is envisaged that information with a limit access(to that the personal data are taken) must be processed in the informational and telecomunicative system(ITS/IS) with application of the complex defence information system (CDIS) with the confirmed accordance. In the article requirements are studied in relation to the system of the personal data protection (PD) in Ukraine in such way that there were not be any contradiction was not between positions of europian directives and requirements of legal documents of Ukraine and native normative documents of the system TID.

By the order of Ukraine Ministry of Justice № 3659/5 the Typical order - minimum list of works that must be realized to the PD owners during organization of events from their defence is set. This order envisages application in ITS/IS network protection fetch during treatment of PD, introduction of procedures of authorizing of workers, providing of anti-virus defence, and also the use of technical equipments of trouble-free feed of the cursored elements of ITS/IS. A typical order takes into account Directives of 95/46/ЄС, 97/66/ЄС of Europian Parlament and Advice of Europe thus, that legal, normative and technical requirements, that regulate providing of defence, rights for physical persons and legal interests of legal entities, were clearly balanced and not create obstacles for market development. These events must not cause to the PD owner the large financial loading on creation of the systems of defence, but here to have the sufficient level of defence of ITS/IS owner. An achievement of such balance is possible on condition of determining the limit and reasonable amount of requirements that does not prevent to development of the newest technologies and proper functioning of bases of PD, in particular the corporate codes of behavior(codes of practice) can be developed from treatment of PD, that expose the basic rules of PD system treatment and defence. These events must not cause to the PD owner the large financial loading on creation of the systems of defence of PD, but here to have the proper(sufficient) level of defence of ITS/IS proprietor. An achievement of such balance is possible on condition of determining the limit and reasonable amount of requirements that does not prevent to the development of the newest technologies and proper functioning of PD bases, in particular the corporate codes of behavior(codes of practice) can be developed from PD treatment, that expose the basic rules of treatment and defence of PD system.

Final choice of certain measures of defence, technical decisions and standards it is necessary that to follow of ITC/ACE remains within the limits of competense of PD owner. Similarly in capacity of owner there is a direct estimation of security risks of data breaches. A typical order in general is not envisage the necessity of creation of DMC for the PD bases at their treatment in composition ITS/IS. Simultaneously with the minim necessary of obligatory use of passwords that change regularly, Directives of 95/46/ЄС, 97/66/EU require also the regular revision of permissions.

It is expedient also to extend the list of types of ITS/IS, that process PD, for that it maybe to apply at Proprietor(Manager) is desire instead of state examination of КСЗІ procedure of analysis of information of declaration about accordance of IDCS to the requirements of normative documents from TID by the authorized central executive control on information defence question – by Administration of the state special communication.

*Literatura: **1**. Zakon Ukrayni «Pro zakhist informatsiї v informatsiyno-telekomunikatsiynikh sistemakh» **2.** Pro zakhist fizichnikh osib pri obrobtsi personal'nikh danikh i pro vil'ne peremishchennya takikh danikh, Direktiva 95/46/ЄS Єvropeys'kogo Parlamentu i Radi Єvropi vid 24 zhovtnya 1995 r. **3.** Zakon Ukrayni «Pro zakhist personal'nikh danikh» **4.** Zakon Ukrayni «Pro informatsiyu» **5.** Pro zatverdzhennya Tipovogo poryadku obrobki personal'nikh danikh u bazakh personal'nikh danikh, nakaz Minyusta vid 30.12.2011 № 3659/5. **6.** Direktiva 97/66/ЄS Єvropeys'kogo Parlamentu i Radi "Stosovno obrobki personal'nikh danikh i zakhistu prava na nevtruchannya v osobiste zhittya v telekomunikatsiynomu sektori" vid 15 grudnya 1997 roku **7.** Standart ISO/IEC 27001 **8.** ND TZI 2.5-004-99. Kriterії otsinki zakhishchenosti informatsiy v komp'yuternikh sistemakh vid nesanktsionovanogo dostupu. Zatverdzheno nakazom DSTSZI SB Ukraïni vid 28.04.1999 r., № 22; **9.** ND TZI 2.5-005-99. Klasifikatsiya avtomatizovanikh sistem i standartni funktsional'ni profili zakhishchenosti obroblyuvanoy informatsiy vid nesanktsionovanogo dostupu. Zatverdzheno nakazom DSTSZI SB Ukrayni vid 28.04.1999 r., № 22*

10. *ND TZI 2.5-005-99 «Klasifikatsiya avtomatizovanikh sistem i standartni funktsional'ni profili zakhishchenosti obroblyuvanoї informatsiynikh vid nesanktsionovanogo dostupu»* ***11.*** *ND TZI 3.7-003-05 "Poryadok provedennya robit zi stvorennya kompleksnoy sistemi zakhistu informatsiy v informatsiyno-telekomunikatsiyniy sistemi", zatverdzhenomu nakazom DSTSZI SBU vid 8 listopada 2005 roku № 125* ***12.*** *Polozhennya pro derzhavnu yekspertizu v sferi tekhnichnogo zakhistu informatsiї, zatverdzhenogo nakazom Administratsiї Derzhspetszv'yazku vid 16 travnya 2007 roku № 93, zareєstrovanim v Ministerstvi yustitsiy Ukrayni 16 lipnya 2007 roku za № 820/14087* ***13.*** *"Pro zatverdzhennya zmin do Polozhennya pro derzhavnu yekspertizu v sferi tekhnichnogo zakhistu informatsiy", nakaz Administratsiї Derzhspetszv'yazku vid 10 zhovtnya 2012 roku № 567 zareєstrovanim 6 listopada 2012 roku Ministerstvom yustitsiy Ukrayni za № 1863/22175*

УДК 621.391.7

МЕТОДИ АВТЕНТИФІКАЦІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Юрій Яремчук
Вінницькій національний технічний університет

Стаття: 11 стор., 13 джерел

На основі математичного апарату рекурентних V_k –послідовностей запропоновано метод автентифікації, в якому відбувається заміна піднесення до степеня обчисленням елементу рекурентної послідовності з певним індексом. Представлено протокол реалізації методу, а також необхідні для цієї реалізації алгоритми прискореного обчислення елементів V_k –послідовності з можливістю мультиплікативної зміни індексу послідовності.

Проведено дослідження та здійснено порівняльний аналіз запропонованого методу автентифікації з відомим методом Шнорра щодо криптографічної стійкості та обчислювальної складності. Встановлено, що запропонований метод є більш стійким, ніж відомий аналог, при цьому він ще й дозволяє змінювати стійкість методу залежно від параметру k –порядку послідовності. Крім того метод, що запропоновано, має значно простішу процедуру завдання параметрів.

Оскільки відомий метод має меншу обчислювальну складність і потребує меншої кількості чисел, що передаються між сторонами автентифікації, то запропоновано декілька варіантів методу автентифікації на основі V_k –послідовностей, які дозволяють за рахунок зменшення стійкості до рівня відомого методу зменшити обчислювальну складність та кількість чисел, що передаються між сторонами автентифікації. Зокрема, один з таких варіантів методу порівняно з відомим аналогом дозволяє зменшити обчислювальну складність з боку перевіряльника.

Показано можливість перетворення запропонованої схеми автентифікації в схему цифрового підписування. Представлено дві схеми цифрового підписування на основі V_k –послідовностей, які забезпечують порівняно з відомими аналогами підвищення стійкості цифрового підписування а також спрощення процедури перевірки підпису, що особливо важливо для клієнт-серверних задач.

МЕТОДЫ АУТЕНТИФИКАЦИИ НА ОСНОВЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Юрий Яремчук
Винницкий национальный технический университет

На основе математического аппарата рекуррентных V_k –последовательностей предложен метод аутентификации, в котором происходит замена возведения в степень вычислением элемента рекуррентной последовательности с определённым индексом. Представлен протокол реализации метода, а также необходимые для этой реализации алгоритмы ускоренного вычисления элементов V_k –последовательности с возможностью мультипликативного изменения индекса последовательности.

Проведено исследование и сравнительный анализ предложенного метода аутентификации с известным методом Шнорра по криптографической стойкости и вычислительной сложности. Установлено, что предложенный метод является более стойким, чем известный аналог, при этом он ещё и позволяет изменять стойкость метода в зависимости от параметра k –порядка последовательности. Кроме того предложенный метод имеет более простую процедуру задания параметров.

Поскольку известный метод имеет меньшую вычислительную сложность и требует меньшего количества чисел, которые передаются между сторонами аутентификации, предложено несколько вариантов метода аутентификации на основе V_k –последовательностей, которые позволяют за счёт уменьшения стойкости до уровня известного метода уменьшить вычислительную сложность и количество чисел, передаваемых между сторонами аутентификации. В частности, один из таких вариантов метода по сравнению с известным аналогом позволяет уменьшить вычислительную сложность со стороны проверяющего.

Показана возможность преобразования предложенной схемы аутентификации в схему цифровой подписи. Представлены две схемы цифровой подписи на основе V_k –последовательностей, которые обеспечивают по сравнению с известными аналогами повышение стойкости цифровой подписи а также упрощение процедуры проверки подписи, что особенно важно для клиент-серверных задач.

AUTHENTICATION METHODS BASED ON RECURRENT SEQUENCES

Iurii Iaremchuk
Vinnytsia national technical university

Based on the mathematical apparatus of recurrence V_k sequences, we proposed a method of authentication suggesting a replacement of exponentiation by computation of the recurrent sequence element with a definite index. We presented a protocol of the method implementation, as well as the algorithms of the accelerated computation of the V_k sequence elements necessary for the implementation, with a possibility of multiple change in the sequence index.

We conducted a study and a comparative analysis of the proposed authentication method with the known Schnorr method of cryptographic reliability and computational complexity. We established that the proposed method is more reliable than the well-known counterpart is, while it also allows for changing the reliability of the method depending on the parameter k of the sequence order. Besides, the proposed method has a simpler procedure of parameter sets.

As the known method has a lower computational complexity and requires fewer numbers, transmitted between the authentication parties, we suggested several options for the authentication method based on V_k sequences, enabling reduction of the computational complexity and the numbers, transmitted between the authentication parties, due to reduction of reliability to the level of the known method. In particular, one of such methods, compared with the known analogue, allows reducing the computational complexity from the part of the inspector.

We demonstrated a possibility of converting the proposed authentication scheme into the scheme of digital signature. We presented two digital signature schemes based on V_k sequences that, compared with the known analogues, provide for an increase of the digital signature's reliability and simplification of signature verification procedures, which is especially important for the client-server applications.

Literatura: ***1****. Menezes A. J., van Oorschot P. C., Vanstone S. A. Handbook of Applied Cryptography. – CRC Press, 2001. – 816 p.* ***2.*** *Zapechnikov S. V. Kriptograficheskiye protokoly i ikh primeneniye v finansovoy i kommercheskoy deyatel'nosti. – M.: Goryachaya liniya–Telekom, 2007. – 320 s.* ***3.*** *Shnayyer B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnyye teksty na yazyke Si. - M.: Triumf, 2002. - 816 s.* ***4.*** *Romanets Yu. V., Timofeyeva P. A., Shan'gin V. F. Zashchita informatsii v komp'yuternykh sistemakh i setyakh. – M.: Radio i svyaz', 2001. – 376 s.* ***5.*** *Vvedeniye v kriptografiyu / Pod obshch. red. V. B. Yashchenko. – M.: MTSNMO: «CheRo», 2000. – 236 s.* ***6.*** *Petrov A. A. Komp'yuternaya bezopasnost'. Kriptograficheskiye metody zashchi¬ty. – M.: DMK, 2000. – 448 s.* ***7.*** *Brassar Zh. Sovremennaya kriptologiya. – M.: POLIMED, 1999. – 176 s.* ***8.*** *Simmons G. J., Authentication theory/coding theory // Proc. CRYPTO'84, Lect. Notes in Comput. Sci. – V. 196, 1985. – Pp. 411–431.* ***9.*** *Yaremchuk*

Yu. E. Vikoristannya rekurentnikh poslidovnostey dlya pobudovi kriptografichnikh metodiv z vidkritim klyuchem // Zakhist informatsiї. – № 4, 2012. – S. 120–127. ***10.*** *Yaremchuk Yu. E. Rozrobka algoritmiv priskorenogo obchislennya yelementiv rekurentnikh poslidovnostey dlya kriptografichnikh zastosuvan' // Reєstratsiya, zberigannya i obrobka danikh. – T. 15, № 1, 2013. – S. 14–22.* ***11.*** *Yaremchuk Yu. E. Metod avtentifikatsiї storin vzaєmodiy na osnovi rekurentnikh poslidovnostey // Suchasniy zakhist informatsiy. – № 1, 2013. – S. 4–10.* ***12****. Markushevich A. I. Vozvratnyye posledovatel'nosti. – M.: Nauka, 1975. – 48 s.* ***13.*** *Knut D. Iskusstvo programmirovaniya dlya EVM, tom 2. Poluchislennyye algoritmy. – M.: Vil'yams, 2004. – 832 s.*

УДК: 004.056.5

ОЦІНЮВАННЯ СТІЙКОСТІ МЕТОДУ ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У ВЕКТОРНІ ЗОБРАЖЕННЯ ДО АКТИВНИХ ТА ПАСИВНИХ АТАК

Василь Карпінець, Юрій Яремчук, Безпалий Кирило
Вінницький національний технічний університет

Стаття: 10 стор., 6 джерел

Проведено аналіз стійкості методу вбудовування цифрових водяних знаків (ЦВЗ) у векторні зображення до активних та пасивних зловмисних атак, спрямованих на зчитування та ускладнення витягнення ЦВЗ правовласником.

Для цього були розглянуті поширені атаки на основі афінних перетворень зображення, атака шляхом внесення додаткового шуму, а також пасивна атака для визначення місця розташування ЦВЗ. Дослідження проводились на прикладі конкретних векторних зображень та ЦВЗ з різними значеннями параметрів методу, що дозволило визначити оптимальні значення для найкращого співвідношення стійкості та збереження якості зображення.

Результати аналізу показали високий рівень стійкості методу до цих атак завдяки особливостям вбудовування ЦВЗ і використаного двовимірного дискретного косинусного перетворення.

ОЦЕНИВАНИЕ СТОЙКОСТИ МЕТОДА ВСТРАИВАНИЯ ЦИФРОВЫХ ВОДНЫХ ЗНАКОВ В ВЕКТОРНЫЕ ИЗОБРАЖЕНИЯ К АКТИВНЫМ И ПАССИВНЫМ АТАКАМ

Василий Карпинец, Юрий Яремчук, Безпалый Кирилл
Винницкий национальный технический университет

Проведен анализ устойчивости метода встраивания цифровых водяных знаков (ЦВЗ) в векторные изображения к активным и пассивным злонамеренным атакам, направленным на считывание и усложнение извлечения ЦВЗ правообладателем.

Для этого были рассмотрены распространенные атаки на основе аффинных преобразований изображения, атака путем внесения дополнительного шума, а также пассивная атака для определения местоположения ЦВЗ. Исследования проводились на примере конкретных векторных изображений и ЦВЗ с различными значениями параметров метода, что позволило определить оптимальные значения для наилучшего соотношения устойчивости и сохранения качества изображения.

Результаты анализа показали высокий уровень устойчивости метода к этим атакам благодаря особенностям встраивания ЦВЗ и использованного двумерного дискретного косинусного преобразования.

EVALUATION STABILITY OF METHOD EMBEDDING DIGITAL WATERMARKS INTO VECTOR IMAGE FOR ACTIVE AND PASSIVE ATTACKS

Vasyl Karpinets, Yuriy Yaremchuk, Bezpalyi Kyrylo
Vinnitsa National Technical University

This paper analyzes the stability of the method of embedding digital watermarks in vector images for active and passive malicious attacks aimed at reading and complications extract digital watermark owner.

This was considered common attacks based on affine transformations of the image, the attack by introducing additional noise, and passive attack is to determine the location of digital watermark. Research carried out on examples of specific and vector images and digital watermark with different parameters of the method, allowing to determine the optimal value for the best balance of stability and preservation of image quality.

The analysis showed a high level of resistance to this attack method by digital watermark embedding features and used two-dimensional discrete cosine transform.

Literatura: ***1****. Zheng L. Research on Vector Map Digital Watermarking Technology / L. Zheng, Y. Jia, Q. Wang. // First International Workshop on Education Technology and Computer Science – 2009. – P. 303 – 307.* ***2.*** *Karpinets' V. V. Zmenshennya vidkhilen' koordinat tochok vnaslidok vbudovuvannya tsifrovikh vodyanikh znakiv u vektorni zobrazhennya / V. V. Karpinets', Yu. E. Yaremchuk // Pravove, normativne, ta metrologichne zabezpechennya sistemi zakhistu informatsiy v Ukraïni – 2010. – № 2(21). – S.101 – 109.* ***3.*** *Karpinets' V. V. Analiz vplivu tsifrovikh vodyanikh znakiv na yakist' vektornikh zobrazhen' / V. V. Karpinets', Yu. E. Yaremchuk // Suchasniy zakhist informatsiy. – 2011. – №1. – S.72 – 82 .* ***4.*** *Karpinets' V. V. Doslidzhennya steganografichnoï stiykosti metodu vbudovuvannya tsifrovikh vodyanikh znakiv u vektorni zobrazhennya / V. V. Karpinets', Yu. E. Yaremchuk // VISNIK Vinnits'kogo politekhnichnogo institutu. – 2011. - №3. – S. 200-205.* ***5.*** *Karpinets' V. V. Analiz stiykosti metodu vbudovuvannya tsifrovikh vodyanikh znakiv u vektorni zobrazhennya do zlovmisnikh atak / V. V. Karpinets', Yu. E. Yaremchuk // VISNIK Vinnits'kogo politekhnichnogo institutu. – 2011. - №4. – S. 154-159.* ***6.*** *Kholl M. Kombinatorika / M. Kholl // Izdatel'stvo «MIR». Moskva. — 1970. 424 s.*

УДК 512

РЕКУРЕНТНІ АЛГОРИТМИ ОБЧИСЛЕННЯ КОРЕНЯ ДОВІЛЬНОГО СТЕПЕНЮ У КІЛЬЦІ ЛИШКІВ

Людмила Ковальчук, Олексій Беспалов, Павло Огнєв
Физико-технічний інститут НТУУ "КПІ"

Стаття: 8 стор., 8 джерел

У даній роботі отримано критерій степеневості елемента скінченого поля та наведено прості алгоритми обчислення кубічного кореня та рекурентні алгоритми обчислення коренів більш високого степеню з елементу поля, який є відповідним степеневим лишком. Алгоритми розпізнавання степеневості та добування кореня за складеним модулем (наприклад, за модулем n=pq) повністю визначаються відповідними алгоритмами за простим модулем, за умови, що відомий розклад числа n на прості множники.

Цікаво також зазначити, що задача розкладу на прості множники та задача добування кореня є поліноміально еквівалентними відносно імовірнісного алгоритму.

Дані алгоритми є, перш за все, цікавими з математичної точки зору, а їх поодинокий випадок – алгоритми добування кубічного кореня – можуть бути використані як допоміжні при обчислення базової точки кривої та при "вкладанні" відкритого тексту у точку кривої, у тому числі і якщо крива задана над кільцем лишків, а не над полем.

РЕКУРРЕНТНЫЕ АЛГОРИТМЫ ВЫЧИСЛЕНИЯ КОРНЯ ПРОИЗВОЛЬНОЙ СТЕПЕНИ В КОЛЬЦЕ ВЫЧЕТОВ

Людмила Ковальчук, Алексей Беспалов, Павел Огнев
Физико-технічний інститут НТУУ "КПІ"

В данной работе получен критерий степенности элемента конечного поля и приведены простые алгоритмв вычисления кубичного коня и рекуррентные алгоритмы вычисления корней более высоких степеней из элемента поля, который является соответствующим степенным вычетом. Алгоритмы распознавания степенности и вычисления корня по составному модулю (например, по модулю $n=pq$) полностью определяются соответствующими алгоритмами для простого модуля, при условии, что известно разложение модуля на простые множители.

Интересно также заметить, что задача разложения на простые множители и задача вычисления корня являются полиномиально эквивалентными относительно вероятностного алгоритма.

Данные алгоритмы являются, прежде всего, интересными с математической точки зрения, а их частный случай – алгоритмы вычисления кубического корня – могут быть использованы как вспомагательные при вычислении базовой точки кривой и при "вложении" открытого текста в точку кривой, в том числе и если кривая задана над кольцом вычетов, а не над полем.

RECURSIVE ALGORUTHMS FOR COMPUTING THE ROOT OF ARBITRARY POVER IN RESIDUE RINGS

Ludmyla Kovalchuk, Alexey Bespalov, Pavel Ognev
Physical-technical institute NTUU "KPI"

In this paper, the criterion of power element of finite field is obtained and simple algorithms for calculating the cubic root and recursive algorithms for calculating the roots of higher powers are constructed. Power recognition algorithm and rooting for composite module (particularly for modulo $n=pq$) are completely determined by the corresponding algorithms for a simple modules, provided that factorization is known.

It is also interesting to note that for $n=pq$ the factorization problem and rooting problem are polynomial equivalent relatively probabilistic algorithm.

These algorithms are primarily interesting from a mathematical point of view, and their particular case – the cubic root extraction algorithm - can be used as aids in calculating the base point of the elliptic curve and for "imbedding" of plaintext into curve point, also if curve is defined over the residue rings instead of the field.

Literatura: ***1.*** *Koblits N. Kurs teorii chisel i kriptografii. // Per. s angl. – M.: Nauchnoye izd-vo TVP, 2001. – 254 s.* ***2.*** *O. Verbits'kiy, "Vstup do kriptologiï" // L.: Vid-vo naukovo-tekhnichnoï literaturi, 1998r., 247s.* ***3.*** *A. Bessalov, A. Telezhenko, "Kriptosistemmy na ellipticheskikh krivykh", Kiyev, 2004, 223 s.* ***4.*** *N. Babenko, "Metody i algoritmy vychisleniya struktur na EK s parallelizmom mashinnykh operatsiy" // Avtoref. na soiskaniye stepeni k.f.-m.n., Stavropol', 2011, 19s.* ***5.*** *A. Nesterenko, "Ob odnom variante metoda Lenstry faktorizatsii tselykh chisel" // Materialy 3-yey mezhdunarodnoy konferentsii "Matematika i bezopasnost' informatsii" (MaBIT-07), MGU, 25-27 oktyabrya 2007 goda, M.: MTSMNO, 2008, s. 234-240.* ***6.*** *M. Samokhina. "Ellipticheskiye krivyye" // Doklad na seminare kafedry radiotekhniki MFTI, radio.fiztex.ru//infsec/f_3kdhla/f_3erfbr/seminar_6.pdf.* ***7.*** *M. Glukhov. I. Kruglov. A. Pichkur, A. Cheryomushkin, "Vvedeniye v teoretiko-chislovyye metody kriptografii" // SPb.: Izd-vo "Lan'", 2011, 400s.* ***8.*** *Lidl R., Niderrayter G. Konechnyye polya: V 2-kh t. / Per. s angl. – M.: Mir, 1988. – 822 s.*

УДК 004.056.5

РОЗРОБКА НОВОГО ПІДХОДУ ДО ВИЯВЛЕННЯ ЗАМІЩУЮЧОЇ ОБЛАСТІ В ЦИФРОВИХ ЗОБРАЖЕННЯХ

Алла Кобозєва, Олена Лебєдєва
Одеський національний політехнічний університет

Стаття: **7 стор., 13 джерел.**

Робота присвячена питанням детектування і локалізації фальсифікації цифрових зображень, під якою розуміється заміщення частини (частин) одного зображення частиною (частинами) іншого (цього ж) зображення, яка називається заміщуючою областю. Такий вид несанкціонованого зміни зображення розглядається в силу свого широкого поширення в разі навмисного порушення його цілісності.

Останні успіхи в створенні, розвитку і загальнодоступності програмного забезпечення для редагування цифрових сигналів вимагають обов'язкового включення в комплексну систему захисту інформації методів перевірки цілісності цифрових зображень, відео, аудіо, що належать до пасивних методів інформаційної безпеки.

Пропонується новий підхід до вирішення проблеми виявлення і локалізації заміщуючої області, в тому числі малих розмірів, в цифровому зображенні довільного формату, в основу якого покладено загальний підхід до аналізу стану і технології функціонування інформаційних систем, відповідно до якого стан цифрового зображення формально описується станом сукупності сингулярних чисел і сингулярних векторів його матриці (матриць), що складають повний набір параметрів. Основою розроблюваного підходу з урахуванням кореляції в зображенні значень яскравості сусідніх пікселів є аналіз зміни поведінки максимальних сингулярних чисел і відповідних їм сингулярних векторів блоків, одержуваних при стандартному розбитті матриці зображення при послідовних зсувах початкового блоку на 1 піксель.

Показано, що лівий і правий сингулярні вектори, що відповідають максимальному сингулярному числу матриці блоку зображення, завжди знаходяться в першому координатному ортанті простору R^8. Ці вектори є нечутливими і sign-нечутливими до довільної збурювальної дії; для переважної більшості блоків зображення ці сингулярні вектори близькі до *n*-оптимальних.

Показником наявності заміщуючої області є розриви першого роду двох функцій: залежності кута між лівим і правим сингулярними векторами, що відповідають найбільшому сингулярному числу блока, від номера блоку при зсуві в 1 піксель; залежності швидкості зміни максимального сингулярного числа блоку для двох послідовних блоків при зсуві на 1 піксель.

На підставі отриманих теоретичних висновків пропонується новий метод виявлення і локалізації заміщуючої області в фальсифікованому цифровому зображенні, що використовує послідовне врахування змін характеру поведінки максимальних сингулярних чисел і відповідних їм сингулярних векторів в блоках тестованого зображення. Результат роботи методу – сукупність блоків зображення, що містять межі заміщуючої області. Основною перевагою методу є його інваріантність щодо формату зберігання зображення.

Визначені шляхи подальшого вдосконалення запропонованого методу з метою уточнення локалізації заміщуючої області шляхом сукупного врахування особливостей аналізованих сингулярних чисел і сингулярних векторів з використанням різних вагових коефіцієнтів. Підбір вагових коефіцієнтів буде проведений на основі порівняння ефективностей локалізації заміщуючої області у разі використання для цього аналізу сингулярних чисел / сингулярних векторів.

РАЗРАБОТКА НОВОГО ПОДХОДА К ВЫЯВЛЕНИЮ ЗАМЕЩАЮЩЕЙ ОБЛАСТИ В ЦИФРОВОМ ИЗОБРАЖЕНИИ

Алла Кобозева, Елена Лебедева
Одесский национальный политехнический университет

Работа посвящена вопросам детектирования и локализации фальсификации цифровых изображений, под которой понимается замещение части (частей) одного изображения частью (частями) другого (этого же) изображения, называемой замещающей областью. Такой вид несанкционированного изменения изображения рассматривается в силу своего широкого распространения в случае преднамеренного нарушения его целостности.

Последние успехи в создании, развитии и общедоступность редактирующего цифровые сигналы программного обеспечения требуют обязательного включения в комплексную систему защиты информации методов проверки целостности цифровых изображений, видео, аудио, относящимся к пассивным методам информационной безопасности.

Предлагается новый подход к решению проблемы обнаружения и локализации замещающей области, в том числе малых размеров, в цифровом изображении произвольного формата, в основу которого положен общий подход к анализу состояния и технологии функционирования информационных систем, в соответствии с которым состояние цифрового изображения формально описывается состоянием совокупности сингулярных чисел и сингулярных векторов его матрицы (матриц), составляющих полный набор параметров. Основой разрабатываемого подхода с учетом коррелируемости в изображении значений яркости близлежащих пикселей является анализ изменения поведения максимальных сингулярных чисел и соответствующих им сингулярных векторов блоков, получаемых при стандартном разбиении матрицы изображения, при последовательных сдвигах начального блока на 1 пиксель.

Показано, что левый и правый сингулярные векторы, отвечающие максимальному сингулярному числу матрицы блока изображения всегда находятся в первом координатном ортанте пространства R^8. Эти векторы является нечувствительными и sign-нечувствительными к произвольному возмущающему воздействию; для подавляющего большинства блоков изображения эти сингулярные векторы близки к *n*-оптимальному.

Показателем наличия замещающей области являются разрывы первого рода двух функций: зависимости угла между левым и правым сингулярными векторами, отвечающими наибольшему сингулярному числу блока, от номера блока при сдвиге в 1 пиксель; зависимости скорости изменения максимального сингулярного числа блока для двух последовательных блоков при сдвиге на 1 пиксель.

На основании полученных теоретических заключений предлагается новый метод выявления и локализации замещающей области в фальсифицированном цифровом изображении, использующий последовательный учет изменений характера поведения максимальных сингулярных чисел и соответствующих им сингулярных векторов в блоках тестируемого изображения. Результат работы метода – совокупность блоков изображения, содержащих границы замещающей области. Основным преимуществом метода является его инвариантность относительно формата хранения изображения.

Намечены пути дальнейшего совершенствования предложенного метода с целью уточнения локализации замещающей области путем совокупного учета особенностей анализируемых сингулярных чисел и сингулярных векторов с использованием различных весовых коэффициентов. Подбор весовых коэффициентов будет производиться на основе сравнения эффективностей локализации замещающей области в случае использования для этого анализа сингулярных чисел/сингулярных векторов.

DEVELOPMENT A NEW APPROACH TO THE IDENTIFICATION OF REPLACEMENT AREA IN A DIGITAL IMAGE

Alla Kobozeva, Helen Lebedeva

Odessa national polytechnic university

Article is devoted to questions of detecting and localization the falsification in digital images which is understood as replacement part (parts) of one image with part (parts) of other (the same) image called by replacing area. Such type of unauthorized the image change is considered because of its wide distribution in case of deliberate violation its integrity.

The last successes in creation, development and accessible of the software, which edits digital signals, demand obligatory inclusion to the complex system of the information security of methods checking the integrity of digital images, video, audio, which relates to passive methods of information security.

It is offered a new approach to a solution of the problem of detection and localization replacing area, including the small sizes in the digital image of any format which is based on the general approach to the analysis of a condition and technology of functioning information systems according to this the condition of the digital image formally is described by a condition of set of singular values and the singular vectors of its matrix (matrixes) making a full set of parameters. Basis of approach which is developed take into account correlatability in the image of brightness values of nearby pixels is the analysis of changing behavior of the maximum singular values and corresponding singular vectors blocks to them which received at standard splitting of a image matrix with consecutive shifts of the initial block for 1 pixel.

It is shown that the left and right singular vectors which are answering to the maximum singular value for the block of a image matrix are always in the first coordinate orthant of the space R^8. These vectors are insensitive and sign-insensitive to any revolting influence; for the majority blocks of the image these singular vectors are close to the n-optimum.

Indicator of existence replacing area are discontinuities of the first kind of two functions: dependences of a corner between left and right the singular vectors which are answering to the maximum singular values of the block, from block numbers with shift for 1 pixel; dependences the speed changing of the maximum singular value for the block for two consecutive blocks at shift for 1 pixel.

On the basis of the received theoretical decisions the new method of identification and localization of replacing area in the forged digital image, which is using consecutive accounting of changes the pattern of behavior of the maximum singular values and corresponding singular vectors to them in blocks of the tested image. The practical result of a method – set of image blocks, which containing borders of replacing area. The main advantage of a method is its invariance concerning a format of storage the image.

It is planned the ways of further improvement of the offered method with the purpose of elaboration the localization of replacing area by the cumulative accounting of features of singular values which are analyzed and singular vectors with using of the various weight coefficients. The selection of weight coefficients will be made on the basis of comparison of efficiency localization of replacing area in case of using of singular values / singular vectors for this analysis.

*Literatura:**1**. Narimanova E. V. Proverka tselostnosti tsifrovogo signala. – Donetsk: Izd. Tsifrovaya tipografiya, 2011. – 180 s. **2.** Kobozєva A. A. Analiz zakhishchenosti informatsiynikh sistem / A. A. Kobozєva, I. O. Machalin, V. O. Khoroshko. — K.: Vid. DUIKT, 2010. — 316 s. **3.** Zhuravel' V. V. K razvitiyu teorii vyyavleniya sledov tsifrovoy obrabotki signalogramm / V. V. Zhuravel', O. V. Rybal'skiy // Zakhist informatsiї. — 2007. — №1(32). — S. 83—85. **4.** Rybal'skiy O. V. Analiz tendentsiy razrabotki sovremennykh metodov i apparatury ekspertizy materialov i sredstv video i zvukozapisi / O. V. Rybal'skiy // Informatika ta matematichni metodi v modelyuvanni. — 2011. — T.1, №1. — S.12—16. **5.** Kobozeva A. A. Razrabotka obshchey teorii vyyavleniya sledov tsifrovoy obrabotki signalogramm i yeye realizatsiya apparatno-programmnym kompleksom «Teorema-M» / A.A.Kobozeva, O. V. Rybal'skiy, V. I. Solov'yev // Suchasna spetsial'na tekhnika. — 2010. — №1(20). — S.5—14. **6.** Popescu A. C. Exposing digital forgeries by detecting traces of re-sampling / A. C. Popescu, H.Farid // IEEE Trans. Signal Process. — 2005. — Vol. 53(2). — P. 758—767. **7.** Bayram S. Image manipulation detection / S.Bayram, B.Sankur, N.Memon // Journal of Electronic Imaging. — 2006. — Vol. 15(4). — P. 1—17. **8.** Narimanova E.V. Issledovaniye effekta dvoynogo kvantovaniya i yego ispol'zovaniye pri obnaruzhenii fal'sifikatsii TSI / YE.V. Narimanova // Visnik Skhidnoukr-go nats-go un-tu im. V. Dalya. — 2008. — №8(126), ch.1. — S.47—55. **9.** Informatsionnyye tekhnologii i sistemy v upravlenii, obrazovanii, nauke: Monografiya / Pod red. prof. V. S. Ponomarenko. – Kh.: Tsifrova drukarnya №1, 2013. – 278 s. **10.** Kobozeva A. A. Analiz informatsionnoy bezopasnosti / A. A. Kobozeva, V .A. Khoroshko. — K.: Izd.GUIKT, 2009. — 251 s. **11.** Demmel' Dzh. Vychislitel'naya lineynaya algebra / Dzh.Demmel'; per.s angl. Kh. D. Ikramova. — M.: Mir, 2001. — 430 s. **12.** Gantmakher F. R. Teoriya matrits / F. R. Gantmakher. — M.: Nauka, 1988. — 552 s. **13.** Kobozeva A. A. Vektornaya SIGN-chuvstvitel'nost' kak osnova geometricheskoy modeli sistemy zashchity informatsii / A. A. Kobozeva, V. A. Khoroshko // Zakhist informatsiї. — 2008. — №3. — S. 49—57.*

УДК 004.056.55:519.2

МЕТОДИКА ОБГРУНТУВАННЯ СТІЙКОСТІ НЕМАРКОВСЬКИХ СИМЕТРИЧНИХ БЛОЧНИХ ШИФРІВ ДО ДИФЕРЕНЦІАЛЬНОГО КРИПТОАНАЛІЗУ

Сергій Яковлєв
Фізико-технічний інститут, НТУУ «КПІ»

Стаття: ***7 стор, 7 джерел.***

Задача доказової стійкості схеми Фейстеля до диференціального аналізу була поставлена та розв’язана Ніберг та Кнудсеном; ними була виведена теоретична верхня межа імовірності існування диференціалів шифру, виражена через відповідні імовірності раундових функцій. Цей параметр дозволяє оцінити знизу складність проведення диференціальної атаки на довільний шифр, побудований на основі схеми Фейстеля. В

подальшому подібні результати були одержані для низки інших марковських шифрів та деяких немарковських схем.

В даній роботі пропонується загальна методика побудови аналітичної оцінки верхньої межі імовірності існування диференціалів через параметри раундових функцій. Ця методика базується на принципах, які використовувались при доведенні результатів попередніх дослідників, однак вона дозволяє оцінювати немарковські шифри та будувати аналітичні оцінки автоматично, що виявляється корисним для оцінки стійкості складних схем шифрування, для яких традиційний математичний підхід вимагав би дослідження великої кількості різних випадків. Суть методики полягає у розгляданні можливих шляхів тривіалізації раундових диференціалів шифру та розбитті множини диференціальних характеристик на класи відповідно до шляху тривіалізації. Кількість таких класів є порівняно невеликою, тому вони можуть бути швидко перебрані; для кожного класу будується верхня межа диференціальної імовірності, з яких потім обирається максимальне значення.

Наводяться результати аналізу та оцінки стійкості низки узагальнених схем Фейстеля: Skipjack-подібної, CAST-подібних та узагальненої MISTY-подібної схем.

МЕТОДИКА ОБОСНОВАНИЯ СТОЙКОСТИ НЕМАРКОВСКИХ СИММЕТРИЧНЫХ БЛОЧНЫХ ШИФРОВ К ДИФФЕРЕНЦИАЛЬНОМУ КРИПТОАНАЛИЗУ

Сергей Яковлев

Физико-технический институт, НТУУ «КПИ»

Задача доказательной стойкости схемы Фейстеля к дифференциальному анализу была поставлена и решена Ниберг и Кнудсеном; ними была выведена теоретическая верхняя граница вероятности существования дифференциалов шифра, выраженная через соответствующие вероятности раундовых функций. Этот параметр позволяет оценить снизу сложность проведения дифференциальной атаки на произвольный шифр, построенный на основе схемы Фейстеля. В дальнейшем подобные результаты были получены для многих других марковских шифров и некоторых немарковских схем.

В данной работе предлагается методика построения аналитической оценки верхней границы вероятности существования дифференциалов через параметры раундовых функций. Эта методика базируется на принципах, которые использовались при доказательстве результатов предыдущих исследователей, однако она позволяет оценивать немарковские шифры и строить аналитические оценки автоматически, что оказывается полезным при оценке стойкости сложных схем шифрования, в которых традиционный математический подход требовал бы исследования огромного количества разных случаев. Суть методики состоит в рассмотрении возможных путей тривиализации раундовых дифференциалов шифра и разбиении множества дифференциальных характеристик на классы в соответствии с путём тривиализации. Количество таких классов сравнительно невелико, поэтому они могут быть быстро перебраны; для каждого класса строятся верхние границы дифференциальных вероятностей, из которых потом выбирается максимальное значение.

Приводятся результаты анализа и оценки стойкости некоторых обобщённых схем Фейстеля: Skipjack-подобной, CAST-подобных и обобщённой MISTY-подобной схем.

PROCEDURE OF SECURITY ESTIMATION OF NON-MARKOV CIPHERS AGAINST DIFFERENTIAL CRYPTANALYSIS

Sergiy Yakovlev

Institute of Physics and Technology, NTUU "KPI"

Nyberg and Knudsen formulated and solved a problem of provable security of Feistel network against differential analysis. They derived analytical upper bound of cipher differential probabilities expressed in terms of corresponding round function probabilities. Such parameter gives minimal complexity of differential attack over any cipher based on Feistel network. Further, similar results was obtained for many Markov ciphers and some non-Markov schemes.

We propose a procedure of constructing an analytical estimation of differential probabilities' upper bound in terms of round functions parameters. This procedure is based on principles used in previous researches, but it allows to evaluate security of non-Markov ciphers and to build estimations automatically. The last is useful in studying of complex ciphers, for which traditional techniques would require a huge number of cases to analyze. Essence of

procedure is to consider all possible ways of round differential trivialization and to partition a set of differential characteristics according to trivialization ways. The number of parts is relatively small so that they can be quickly enumerated. The upper bound of differential probability is estimated for each such part, and the maximum is the cipher's total upper bound.

We also present the results of analysis and estimations of provable security against differential analysis for some generalized Feistel networks: Skipjack-like ciphers, two variants of CAST-like ciphers and generalized MISTY-like ciphers.

Literatura: ***1.*** *Biham E, Shamir A. Differential cryptanalysis of DES-like cryptosystems // Journal of Cryptology. – 1991. – V. 4. – № 1. – P. 3 – 72.* ***2.*** *Lai X., Massey J.L., Murphy S., Markov ciphers and differential cryptanalysis // Advances in Cryptology – EUROCRYPT'91, Proceedings. – Springer Verlag, 1991. – P. 17-38.* ***3.*** *Nyberg K., Knudsen L.R. Provable Security Against a Differential Attack // Journal of Cryptology, Vol.8, no.1 (1995).* ***4.*** *Matsui M., On a Structure of Block Ciphers with Provable Security against Differential and Linear Analysis – IEICE Trans. Fundamentals, vol. E82-A – 1999 – #1 – P. 117-122.* ***5.*** *Vaudenay S. On the security of CS-cipher // Fast Software Encryption. – FSE'99, Proceedings. – Springer Verlag, 1999. – P. 260 – 274.* ***6.*** *Koval'chuk L. V., Sherstyuk A. O. Doslidzhennya riznitsevikh kharakteristik raundovoï funktsiï blochnikh shifriv MISTY1 ta MISTY2 // Prikladnaya radioelektronika. – №3. – 2009. – S. 15–27.* ***7.*** *Hong S., Sung J., Lee S., Lim J., Kim J. Provable Security for 13-round Skipjack-like Structure // Information Processing Letters, 2001.*

УДК 004.056.53(045)

ПРАКТИЧНІ СХЕМИ РЕАЛІЗАЦІЇ АЛГОРИТМІВ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Анна Чунарьова
Національний авіаційний університет

Стаття: ***8 стор., 9 джерел.***

Проведено порівняльний аналіз асиметричних схем формування ЕЦП, які засновані на проблемі дискретного логарифмування над скінченним полем та еліптичними кривими. На основі проведеного аналізу складена порівняльна таблиця оцінки ефективності використання даних алгоритмів.

Описані основні стандарти, такі як DSA, ElGamal, ECDSA, ГОСТ Р 34.10-2001, що базуються на складності вирішення задачі дискретного логарифмування у скінченному полі. Також детально розглянуто криптографічні алгоритми з можливістю відновлення повідомлення при проведенні процедури верифікації цифрового підпису. Аналіз дозволив сформувати переваги і недоліки даних алгоритмів та виділити ефективний алгоритм цифрового підпису на дискретному логарифмі з властивістю відновлення повідомлення.

ПРАКТИЧЕСКИЕ СХЕМЫ РЕАЛИЗАЦИИ АЛГОРИТМОВ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Анна Чунарева
Национальный авиационный університет

Проведен сравнительный анализ асимметричных схем формирования ЭЦП, основанных на проблеме дискретного логарифмирования над конечным полем и эллиптическими кривыми. На основе проведенного анализа составлена сравнительная таблица оценки эффективности использования данных алгоритмов.

Описаны базовые стандарты, такие как DSA, ElGamal, ECDSA, ГОСТ Р 34.10-2001, основанные на сложности решения задачи дискретного логарифмирования в конечном поле. Также подробно рассмотрены криптографические алгоритмы с возможностью восстановления сообщения при проведении процедуры верификации цифровой подписи. Данный анализ позволил сформировать преимущества и недостатки данных алгоритмов и выделить эффективный алгоритм цифровой подписи на базе дискретного логарифма со свойством восстановления сообщения.

PRACTICAL SCHEMES OF THE ALGORITHM ELECTRONIC SIGNATURE

Anna Chunareva
National Aviation University

The article provides a comparative analysis of the formation of the asymmetric digital signature schemes based on the discrete logarithm problem over finite fields and elliptic curves. Based on the analysis compiled a comparative table of assessing the efficiency of these algorithms.

This paper describes the basic standards, such as DSA, ElGamal, ECDSA, GOST R 34.10-2001, based on the complexity of solving the discrete logarithm problem in a finite field. Also discussed in detail the cryptographic algorithms with the ability to recover the message during the procedure of verification of the digital signature. This analysis helped to formulate the advantages and disadvantages of these algorithms, and an efficient algorithm to allocate the digital signature of the discrete logarithm with property recovery messages.

Literatura: ***1****. Bryus Shnayyer. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnyye teksty na Si. - M.: Izd. TRIUMF, 2008. – 816 c.* ***2****. Nyberg K., Rueppel R. A New Signature Scheme Based on the DSA Giving Message Recovery / K. Nyberg, R. Rueppel // 1st ACM Conference on Computer and Communications Security. Springer-Verlag, 1998. P. 182 193.* ***3.*** *Ateniese, G., Medeiros, B.D. A Provably Secure Nyberg-Rueppel Signature Variant with Applications./ G. Ateniese, B.D Medeiros // IACR Cryptology ePrint Archive 2004.– 2004. – P. 93-110.* ***4.*** *Sujata M., Banshidhar M. A Digital Signature Scheme with Message Recovery and without One-Way Hash Function / M. Sujata, M. Banshidhar // International Conference on Advances in Computer Engineering. – Bangalore, 2010. – P. 265-267.* ***5.*** *Miyaji A. A message recovery signature scheme equivalent to DSA over elliptic curves // In Proceedings of ASIACRYPT'96. – Springer-Verlag, 1996. – P. 1-14.* ***6.*** *Pintsov L., Vanstone S. Postal Revenue Collection in the Digital Age / L. Pintsov, S. Vanstone // Financial Cryptography, Lecture Notes in Computer Science 1962. Springer, 2000. P. 105-120.* ***7.*** *Zhang. F. Identity-based partial message recovery signatures (or How to shorten ID-based signatures) / F. Zhang, W. Susilo, Y. Mu // Lecture Notes in Computer Science, 3570. – 2005. – P. 45–56.* ***8.*** *An Efficient ID-based Digital Signature with Message Recovery Based on Pairing / Raylin Tso, Chunxiang Gu, Takeshi Okamoto, and others // IACR Cryptology ePrint Archive, Vol. 2006. – 2006/195.* ***9.*** *Mao V. Sovremennaya kriptografiya: teoriya i praktika. – Per. s angl. – M.: Izdatel'skiy dom Vil'yams, 2005. – 768 s.*

УДК 004.056.5

АНАЛИЗ И ОЦЕНКА НОРМАТИВНЫХ ДОКУМЕНТОВ, ПРИМЕНЯЕМЫХ ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ SMART GRID СИСТЕМ

Алексей Юдин, Глеб Пирогов
ГосНИИ Спецсвязи

Стаття: ***7 стор., 5 джерел***.

Рассматривается Smart Grid система как совокупность подсистемы передачи электрической энергии и информационно-телекоммуникационной подсистемы и в соответствии с этим осуществляется анализ действующих нормативных документов.

Объектом анализа являются нормативные документы, относящиеся к обеспечению информационной безопасности систем управления, систем диспетчерского управления и сбора данных (SCADA), автоматизированных систем управления технологическим процессом (АСУ ТП) и Smart Grid, а именно:

Международные стандарты

1. IEEE 1402. IEEE Guide for Electric Power Substation Physical and Electronic Security, -IEEE 1686. IEEE Standard for Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities, IEEE P1711. Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.

2. ISO 27019. Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002.

3. IEC TR 62210. Power system control and associated communications. Data and communication security, IEC 61784-4. Digital data communications for measurement and control – Profiles for secure communications in

industrial networks, IEC 62443. Security for industrial process measurement and control – Network and system security, IEC 62351. Data and Communication Security, IEC/TR 62357. Power system control and associated communications - Reference architecture for object models, services and protocols.

Национальные отраслевые стандарты

4. NIST SP800-82. Guide to Industrial Control Systems (ICS) Security, NIST SP800-53. Security and Privacy Controls for Federal Information Systems and Organizations, NISTIR 7628. Guidelines for Smart Grid Cyber Security.

5. ISA 99.00.01. Security for Industrial Automation and Control Systems: Concepts, Models and Terminology.

6. AGA 12-3 Protection of Networked Systems, AGA 12-4 Protection Embedded in SCADA Components.

7. NERC CIP-002. Cyber Security - Critical Cyber Asset Identification, NERC CIP-003. Cyber Security - Security Management Controls, NERC CIP-007. Cyber Security - Systems Security Management, NERC CIP-011. Cyber Security - Information Protection.

В ходе анализа и оценки нормативных документов были сделаны следующие выводы.

1. Стандарты, разработанные Институтом инженеров по электротехнике и электронике, касаются электрических подстанций и различных интеллектуальных устройств. Данные документы не описывают вопросы обеспечения безопасности во всех доменах Smart Grid.

2. Документы Международной организации по стандартизации на сегодня находятся на стадии разработки. Стандарт ISO 27019, судя по содержанию проекта документа, будет содержать сведения о базовых механизмах защиты электрических подстанций и интеллектуальных устройств. То есть стандарты этой серии смогут охватить четыре из семи доменов – генерирующие, передающие, распределяющие организации и потребителя.

3. Стандарты, разработанные Международной электротехнической комиссией, а именно IEC 61784, 62443, 62351 и TR 62210, также ориентированы на обеспечение информационной безопасности систем производства и управления производством. Данная серия довольно детально и полно описывает защиту трех доменов - генерирующих, передающих и распределяющих организаций.

4. Серия стандартов NERC CIP, в основном, ориентирована на обеспечение кибербезопасности в SCADA. Эти документы носят декларативный характер и также не учитывают специфику обеспечения информационной безопасности в Smart Grid.

5. Стандарты Национального института стандартизации и технологий описывают вопросы безопасности в промышленных системах. В тоже время технический отчет NISTIR 7628 вводит понятие кибербезопасности в Smart Grid системах. Данный документ является первым ориентированным именно на Smart Grid и наиболее полно дает описание множества объектов и субъектов Smart Grid, их взаимодействия и механизмов защиты.

Таким образом, можно предположить, что для понимания процесса обеспечения информационной безопасности Smart Grid систем наиболее полно подходит технический отчет NISTIR 7628, так как именно этот документ описывает отличия в подходах к обеспечению информационной безопасности SCADA, АСУ ТП и Smart Grid.

АНАЛІЗ ТА ОЦІНКА НОРМАТИВНИХ ДОКУМЕНТІВ, ЯКІ ЗАСТОСОВУЮТЬСЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ SMART GRID СИСТЕМ

Олексій Юдін, Гліб Пирогов
ДержНДІ Спецзв'язку

В статті розглядається Smart Grid система як сукупність підсистеми передавання електричної енергії та інформаційно-телекомунікаційної підсистеми, і відповідно до цього здійснюється аналіз діючих нормативних документів.

Об'єктом аналізу є нормативні документи, що відносяться до забезпечення інформаційної безпеки систем управління, систем диспетчерського керування та збору даних (SCADA), автоматизованих систем управління технологічним процесом (АСУ ТП) і Smart Grid, а саме:

Міжнародні стандарти

1. IEEE 1402. IEEE Guide for Electric Power Substation Physical and Electronic Security, -IEEE 1686. IEEE Standard for Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities, IEEE P1711. Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.

2. ISO 27019. Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002.

3. IEC TR 62210. Power system control and associated communications. Data and communication security, IEC 61784-4. Digital data communications for measurement and control – Profiles for secure communications in industrial networks, IEC 62443. Security for industrial process measurement and control – Network and system security, IEC 62351. Data and Communication Security, IEC/TR 62357. Power system control and associated communications - Reference architecture for object models, services and protocols.

Національні галузеві стандарти

4. NIST SP800-82. Guide to Industrial Control Systems (ICS) Security, NIST SP800-53. Security and Privacy Controls for Federal Information Systems and Organizations, NISTIR 7628. Guidelines for Smart Grid Cyber Security.

5. ISA 99.00.01. Security for Industrial Automation and Control Systems: Concepts, Models and Terminology.

6. AGA 12-3 Protection of Networked Systems, AGA 12-4 Protection Embedded in SCADA Components.

7. NERC CIP-002. Cyber Security - Critical Cyber Asset Identification, NERC CIP-003. Cyber Security - Security Management Controls, NERC CIP-007. Cyber Security - Systems Security Management, NERC CIP-011. Cyber Security - Information Protection.

В ході аналізу та оцінки нормативних документів були зроблені наступні висновки:

1. Стандарти, які розроблені Інститутом інженерів з електротехніки та електроніки, стосуються електричних підстанцій та різних інтелектуальних пристроїв. Ці документи не описують питання забезпечення безпеки в усіх доменах Smart Grid.

2. Документи Міжнародної організації зі стандартизації, на сьогодні, знаходяться на стадії розробки. Стандарт ISO 27019, виходячи зі змісту проекту документу, буде містити відомості про базові механізми захисту електричних підстанцій та інтелектуальних пристроїв. Тобто, стандарти цієї серії зможуть охопити чотири з семі доменів – генеруючи, передаючі, розподіляючі організації та споживачі.

3. Стандарти розроблені Міжнародною електротехнічною комісією, а саме - IEC 61784, 62443, 62351 и TR 62210, також орієнтовані на забезпечення інформаційної безпеки систем виробництва та керування виробництвом. Ця серія стандартів доволі детально та повно описує захист трьох доменів – генеруючих, передаючих та розподіляючих організацій.

4. Серія стандартів NERC CIP, в основному, орієнтована на забезпечення кібербезпеки в SCADA. Ці документи носять декларативний характер і на враховують специфіку забезпечення інформаційної безпеки в Smart Grid.

5. Стандарти Національного інституту стандартизації і технологій описують питання безпеки в промислових системах. В той же час, технічний звіт NISTIR 7628 вводить поняття кібербезпеки в Smart Grid системах. Цей документ є першим, орієнтованим виключно на Smart Grid. Він найповніше дає опис множини об'єктів та суб'єктів Smart Grid, їх взаємодії і механізмів захисту.

Таким чином можна припустити, що для розуміння процесу забезпечення інформаційної безпеки Smart Grid систем найповніше підходить технічний звіт NISTIR 7628. Це пов'язано з тим, що саме цей документ описує відмінності в підходах до забезпечення інформаційної безпеки SCADA, АСУ ТП та Smart Grid.

ANALYSIS AND EVALUATION OF REGULATORY DOCUMENTS USED FOR INFORMATION SECURITY SMART GRID SYSTEM

Oleksii Yudin, Gleb Pirogov
SRI for STIP

In the article the Smart Grid system is considered as a set of subsystems transmission of electrical energy, and information and telecommunication sub-system, and in accordance with this analysis is relevant regulations.

The object of the analysis are the regulations pertaining to information security control systems, supervisory control and data acquisition (SCADA), automated process control systems (PCS) and the Smart Grid:

International Standards

1. IEEE 1402. IEEE Guide for Electric Power Substation Physical and Electronic Security, -IEEE 1686. IEEE Standard for Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities, IEEE P1711. Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links.

2. ISO 27019. Information security management guidelines for process control systems used in the energy utility industry on the basis of ISO/IEC 27002.

3. IEC TR 62210. Power system control and associated communications. Data and communication security, IEC 61784-4. Digital data communications for measurement and control – Profiles for secure communications in industrial networks, IEC 62443. Security for industrial process measurement and control – Network and system security, IEC 62351. Data and Communication Security, IEC/TR 62357. Power system control and associated communications - Reference architecture for object models, services and protocols.

National industry standards

4. NIST SP800-82. Guide to Industrial Control Systems (ICS) Security, NIST SP800-53. Security and Privacy Controls for Federal Information Systems and Organizations, NISTIR 7628. Guidelines for Smart Grid Cyber Security.

5. ISA 99.00.01. Security for Industrial Automation and Control Systems: Concepts, Models and Terminology.

6. AGA 12-3 Protection of Networked Systems, AGA 12-4 Protection Embedded in SCADA Components.

7. NERC CIP-002. Cyber Security - Critical Cyber Asset Identification, NERC CIP-003. Cyber Security - Security Management Controls, NERC CIP-007. Cyber Security - Systems Security Management, NERC CIP-011. Cyber Security - Information Protection.

The analysis and evaluation of regulations has made the following conclusions:

The standards developed by the Institute of Electrical and Electronics Engineers, concerning electrical substations and various intelligent devices. These documents do not describe the security issues in all domains of Smart Grid.

1. Documents of the International Organization for Standardization for today are still under development. Standard ISO 27019, judging from the content of the draft document will contain information about the basic mechanisms for the protection of electrical substations and smart devices. That is, the standards of this series will cover four of the seven domains - generating, transmitting, distributing the organization and the consumer.

The standards developed by the International Electrotechnical Commission, namely IEC 61784, 62443, 62351 and TR 62210, also focused on the provision of information security systems of production and management. This series is quite detailed and complete protection describes three domains - generation, transmission and distribution organizations.

2. A series of standards NERC CIP, primarily focused on cyber security in SCADA. These documents are of a declarative nature and also do not take into account the specificity of information security in the Smart Grid.

3. Standards of the National Institute of Standards and Technology describe cyber security in industrial systems. At the same time, Technical Report NISTIR 7628 introduces the concept of cyber security in the Smart Grid systems. This paper is the first to specifically target Smart Grid and provides the most complete description of a set of objects and subjects of the Smart Grid, their interactions and mechanisms of protection.

Thus, it can be assumed that an understanding of the process of information security Smart Grid systems more fully suited Technical Report NISTIR 7628, since this document describes the differences in the approaches to information security SCADA, DCS and Smart Grid.

Literatura: ***1.*** *Energetichna bezpeka Ukrayni: strategiya ta mekhanizmi zabezpechennya / [Shevtsov A. I., Zemlyaniy M. G., Barannik V. O. ta in.] / Za red. A. I. Shevtsova. Dnipropetrovs'k: Porogi, 2002. – 264 s.* ***2.*** *Ukraïna. Zakoni. Pro yelektroyenergetiku : ofits. tekst : [priynyatiy Verkhovnoyu Radoyu 16 zhovtnya 1997 r.]. K.: Vidomosti Verkhovnoï Radi Ukraïni, 1998, № 1.* ***3.*** *Ukraïna. Zakoni. Pro zakhist informatsiï v informatsiyno-telekomunikatsiynikh sistemakh : ofits. tekst : [priynyatiy Verkhovnoyu Radoyu 5 lipnya 1994 r.]. K.: Vidomosti Verkhovnoï Radi Ukraïni, 1994, №31.* ***4.*** *The path of the smart grid / H. Farhangi. // IEEE Power and Energy Magazine, 2010. Vol. 8, № 1. – P. 18-28.* ***5.*** *NISTIR 7628. Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements // National Institute of Standards and Technology. – 2010. – 15 p.*

УДК 621.396.4

ПІДВИЩЕННЯ ЕНЕРГЕТИЧНОЇ ЕФЕКТИВНОСТІ СТАНЦІЙ ТРОПОСФЕРНОГО ЗВ'ЯЗКУ

Дмитро Вергелес, Геннадій Леоненко, Андрій Паламарчук, Олексій Юдін
ДержНДІ Спецзв'язку

Стаття: ***3 стор, 4 джерел***.

Бурхливий розвиток засобів супутникового зв'язку на початку 70-х років та починаючи з 80-х років широке їх застосування значно скоротили галузь використання станцій тропосферного зв'язку. Це обумовлено характером поширення хвиль, який викликаний як своїми випадковими параметрами, так і

великими енергетичними втратами на трасі поширення. Серед усіх видів зв'язку тропосферні лінії є одними з найбільш складних в технічному відношенні. В той же час, вони мають безперечні переваги перед іншими видами зв'язку, маючи більш високу живучість в умовах надзвичайних ситуацій, озброєних конфліктів та/або антитерористичних заходів, а також при організації зв'язку в труднодоступних, гірських і малонаселених районах.

В значній мірі здійснення тропосферного радіозв'язку ускладнюється внаслідок міжсимвольної інтерференції, яка пов'язана з інтервалом часу затримки останнього достатньо сильного лунасигналу порівняно з першим прийнятим сигналом. Вплив міжсимвольної інтерференції при передачі цифрової інформації має першорядне значення, бо вона обумовлює виникнення нескоротних помилок, виключити які неможливо навіть при необмеженій енергетиці радіолінії. Тому питання, пов'язані з удосконаленням методів усунення впливу міжсимвольної інтерференції на тропосферних радіолініях, а, відповідно, і підвищення енергетичної ефективності, є актуальними.

Для вирішення цієї проблеми пропонується використовувати багатоступінчату обробку сигналу з розширеним спектром (широкосмуговий сигнал) у сполученні з завадостійким кодуванням за алгоритмом Вітербі. Порівняння енергії сигналу без обробки з енергією сигналу з багатоступеневою обробкою, при заданій потужності передавачів та однаковій ймовірності похибок, показали значні переваги, які надає використання багатоступеневої обробки. Це підтверджують лабораторні дослідження макетів модемів на імітаторі тропосферної лінії зв'язку.

ПОВЫШЕНИЕ ЭНЕРГЕТИЧЕСКОЙ ЭФФЕКТИВНОСТИ СТАНЦИЙ ТРОПОСФЕРНОЙ СВЯЗИ

Дмитрий Вергелес, Геннадий Леоненко, Андрей Паламарчук, Алексей Юдин
ГосНИИ Спецсвязи

Бурное развитие в начале 70-х годов средств спутниковой связи и широкое их применение начиная с 1980-х годов значительно сократили область использования станций тропосферной связи. Это обусловлено тем, что из-за характера распространения волн, который характеризуется как своими случайными параметрами, так и большими энергетическими потерями на трассе распространения, среди всех видов связи тропосферные линии являются одним из наиболее сложных в техническом отношении устройств. Однако они имеют бесспорные преимущества перед другими видами связи, имея более высокую живучесть в условиях чрезвычайных ситуаций, вооруженных конфликтов и/или антитеррористических мероприятий, а также при организации связи в труднодоступных, горных и малонаселенных районах.

В значительной мере осуществление тропосферной радиосвязи осложняется из-за межсимвольной интерференции связанной с интервалом временем задержки последнего достаточно сильного эхосигнала по сравнению с первым принятым сигналом. Влияние межсимвольной интерференции при передаче цифровой информации имеет первостепенное значение, так как она обуславливает возникновение несократимых ошибок, исключить которые невозможно даже при неограниченной энергетике радиолинии. Поэтому вопросы, связанные с совершенствованием методов устранения влиянием межсимвольной интерференции на тропосферных радиолиниях, а следовательно и повышения энергетической эффективности, являются актуальными.

Для решения этой проблемы предлагается использовать многоступенчатую обработку сигнала с расширенным спектром (широкополосный сигнал) в сочетании с помехоустойчивым кодированием по алгоритму Витерби. Сравнение энергии сигнала без обработки с энергией сигнала с многоступенчатой обработкой, при заданной мощности передатчиков и одинаковой вероятности ошибок, показали значительные преимущества, которые дает использование многоступенчатой обработки. Это подтверждают лабораторные исследования макетов модемов на имитаторе тропосферной линии связи.

IMPROVING ENERGY EFFICIENCY OF STATION OF TROPOSPHERIC COMMUNICATION

Dmitro Vergeles, Gennady Leonenko, Andriy Palamarchuk, Oleksii Yudin
SRI for STIP

The rapid development in the early 70's satellite-based communications and their wide use since the 1980s, have significantly reduced the area of use of tropospheric communication stations. This is due to the fact that due to the

nature of wave propagation, which is characterized as its random parameters and large energy losses in the propagation path, among all types of tropospheric communication lines are one of the most technically complex devices. However, they have undeniable advantages over other forms of communication, with a higher survivability in emergency situations of armed conflict and anti-terrorism measures, as well as the organization of communication in remote, mountainous and sparsely populated areas.

To a large extent the implementation of the tropospheric radio complicated because the intersymbol interference associated with the delay time interval of the last sufficiently strong echo compared to the first received signal. Effect of intersymbol interference when transmitting digital information is of paramount importance, since it determines the emergence of irreducible error that can not be deleted even when unlimited power radio. Therefore, the issues related to the improvement of methods of eliminating the influence of inter-symbol interference in the tropospheric radio lines, and thus improve energy efficiency, are relevant.

To solve this problem, we propose to use a multi-processing the spread spectrum signal (wideband signal) in combination with error-correcting coding Viterbi. Comparison of the signal energy without treatment with signal energy with a multistage treatment, for a given transmitter power and equal error probability, showed significant advantages provided by the use of multi-processing. This is confirmed by laboratory testing of models of modems on the simulator tropospheric link.

Literatura: ***1****. Viterbi A. D., Omura Dzh. K. Printsipy tsifrovoy svyazi i kodirovaniya. M,: «Radio i svyaz'», 1982. - 538 s.* ***2.*** *Shennon K. Matematicheskaya teoriya svyazi. SB. Raboty po teorii informatsii i kibernetike./Per. s angl. pod red. N. A. Zheleznova. – M.: IL, 1963. – 829s.* ***3.*** *L. E. Varakin. Teoriya sistem signalov M,: «Radio i svyaz'», 1978. - 303 s.* ***4.*** *Shumopodobnyye signaly v sistemakh peredachi informatsii pod red. V. B. Pestryakova – M.: «Radio i svyaz'», 1973. – 424 s.*

УДК.621.791

ТЕХНІКА АКТИВНОГО ВИБРОАКУСТИЧНОГО ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ В УКРАЇНІ: СТАН І ПЕРСПЕКТИВИ

Ігор Порошин, Михайло Прокофьєв, Володимир Дворський
НДЦ "ТЕЗІС" НТУУ "КПІ"

Стаття: ***8 стор., 12 джерел***

Серед технічних засобів, призначених до комплектування систем активного віброакустичного захисту (АВЗ) мовної інформації, дванадцять виробів, що пропоновані в даний час на споживчому ринку України, мають сертифікат відповідності або експертний висновок. Це дозволяє сформувати з них шість дозволених до використання на території України фірмових комплектів, постачальниками яких є наступні підприємства та організації: «Укрспецтехніка система», АТВТ «МАРС», ТОВ «Об'єднаний центр захисту інформації», ПП «РІАС», Відділ ТЗІ ВАТ « Миколаївське підприємство ЕРА »,« Digital and Analog Systems ».

Дозволені до застосування в Україні системи АВЗ можуть бути укомплектовані генераторами захисної перешкоди Базальт-4ГА, МАРС-ТЗО-4-2, ОЦЗІ-ВА/Г (тип1), ОЦЗІ-ВА/Г (тип2), РІАС-2ГС, РІАС-2ГМ , Топаз ГША-4, Топаз ГША-4М, Топаз ГША-4МК, DNG-2300, вібраційними випромінювачами Базальт-4ДВМ, ВИ 3, ВИ 4, ОЦЗІ-ВА/В, РІАС-2ВП, Топаз ВВ-1, TRN-2000 , акустичними випромінювачами Базальт-4ДА, МАРС-АКЗ, РІАС-2ВА, OMS-2000.

Генератори захисної перешкоди для систем АВЗ, пропоновані українськими фірмами, є, як правило, двоканальними пристроями без вбудованого контролю працездатності і без можливості підключення дистанційного керування (ДУ), що мають спрощене 2-3 - смугове регулювання спектру захисної перешкоди. Виняток становлять наступні моделі:

- Базальт-4ГА (5-смуговий еквалайзер, можливість підключення дротяного ДУ);
- МАРС-ТЗО-4-2 (вбудований контроль працездатності, вбудована індикація вихідного рівня);
- ОЦЗІ-ВА/Г (5-смуговий еквалайзер, вбудований контроль працездатності, до чотирьох незалежних універсальних каналів / виходів).

Головною проблемою сучасного етапу розвитку техніки АВЗ є забезпечення прийнятної акустичної комфортності виділених приміщень. Один з шляхів вирішення цієї проблеми - застосування захисних перешкод із більш «комфортним» забарвленням спектру, зокрема, «мовоподібний» шум. Другий шлях

вирішення проблеми пов'язаний із застосуванням багатокомпонентних захисних перешкод, що містять мовоподібні складові, зокрема, фонемні.

Відсутність вбудованого контролю працездатності і відсутність можливості під'єднання ДУ в більшості генераторів захисної перешкоди, а також відсутність на споживчому ринку України сертифікованих мобільних комплексів оперативного контролю працездатності систем АВЗ також обмежує можливості застосування техніки АВЗ на об'єктах інформаційної діяльності. Вирішення цих проблем, хоча і зажадає додаткових витрат на проведення досліджень і розробок, у перспективі дозволить істотно підвищити якість захисту мовної інформації від витоку віброакустичними каналами.

ТЕХНИКА АКТИВНОЙ ВИБРОАКУСТИЧЕСКОЙ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ В УКРАИНЕ: СОСТОЯНИЕ И ПЕРСПЕКТИВЫ

Игорь Порошин, Михаил Прокофьев, Владимир Дворский
НИЦ "ТЕЗИС" НТУУ "КПИ"

Среди представленных в настоящее время на потребительском рынке Украины технических средств, предназначенных для комплектования систем активной виброакустической защиты (АВЗ) речевой информации, двенадцать изделий имеют сертификат соответствия или экспертное заключение. Это позволяет сформировать из них шесть разрешённых к использованию на территории Украины фирменных комплектов, поставщиками которых являются следующие предприятия и организации: «Укрспецтехника система», АООТ «МАРС», ООО «Объединённый центр защиты информации», ЧП «РІАС», Отдел ТЗИ ОАО «Николаевское предприятие ЭРА», «Digital and Analog Systems».

Разрешённые к применению в Украине системы АВЗ могут быть укомплектованы генераторами защитной помехи Базальт-4ГА, МАРС-ТЗО-4-2, ОЦЗІ-ВА/Г(тип1), ОЦЗІ-ВА/Г(тип2), РІАС-2ГС, РІАС-2ГМ, Топаз ГША-4, Топаз ГША-4М, Топаз ГША-4МК, DNG-2300, вибрационными излучателями Базальт-4ДВМ, ВИ 3, ВИ 4, ОЦЗІ-ВА/В, РІАС-2ВП, Топаз ВВ-1, TRN-2000, акустическими излучателями Базальт-4ДА, МАРС-АКЗ, РІАС-2ВА, OMS-2000.

Генераторы защитной помехи для систем АВЗ, предлагаемые украинскими фирмами, являются, как правило, двухканальными устройствами без встроенного контроля работоспособности и без возможности подключения дистанционного управления (ДУ), имеющими упрощённую 2-3 – полосную регулировку спектра защитной помехи. Исключение составляют следующие модели:

- Базальт-4ГА (5-полосный эквалайзер, возможность подключения проводного ДУ);
- МАРС-ТЗО-4-2 (встроенный контроль работоспособности, встроенная индикация выходного уровня);
- ОЦЗІ-ВА/Г (5-полосный эквалайзер, встроенный контроль работоспособности, до четырёх независимых универсальных каналов/выходов).

Главной проблемой современного этапа развития техники АВЗ является обеспечение приемлемой акустической комфортности выделенных помещений. Один из путей решения этой проблемы – применение защитных помех с более «комфортной» окраской спектра, в частности, «речеподобного» шума. Второй путь решения проблемы связан с применением многокомпонентных защитных помех, содержащих речеподобные составляющие, в частности, фонемные.

Отсутствие встроенного контроля работоспособности и отсутствие возможности подключения ДУ в большинстве выпускаемых украинскими фирмами генераторов защитной помехи, а также отсутствие на потребительском рынке Украины сертифицированных мобильных комплексов оперативного контроля работоспособности систем АВЗ также ограничивает возможности применения техники АВЗ на объектах информационной деятельности. Решение этих проблем, хотя и потребует дополнительных затрат на проведение исследований и разработок, в перспективе позволит существенно повысить качество защиты речевой информации от утечки по виброакустическим каналам.

TECHNICS OF THE ACTIVE VIBRO-ACOUSTIC PROTECTION OF SPEACH INFORMATION IN UKRAINE: THE PRESENT AND FUTURE

Igor Poroshin, Mikhail Prokofiev, Vladimir Dvorsky
SRC "TEZIS" NTUU "KPI"

Among the hardware designed for acquisition of active vibro-acoustic protection (AVP) systems for speech information, which are presently available in the consumer market of Ukraine, twelve products have the certificates of conformity or expert opinions. This allows to create six allowed on the territory of Ukraine branded kits, which are supplied by the following companies and organizations: "Ukrspetstekhnika system", "MARS", "Joint Center for information security", "RIAS", TZI Department of the " Mykolayiv enterprise ERA », « Digital and Analog Systems».

AVP systems, permitted in Ukraine, can be equipped with a protective noise generators Basalt-4ga, MARS-TZO-4-2, OCZI-VA/G (type 1), OCZI-VA/G (type 2), RIAS-2GS, RIAS-2GM , Topaz GSHA-4, Topaz GSHA -4M, Topaz GSHA-4MK, DNG-2300, vibration transducers Basalt-4DVM, VI 3, VI 4, OCZI-VA /V, RIAS-2VP, Topaz VV-1, TRN-2000 , acoustic transducers Basalt-4DA, MARS-AKZ, RIAS-2VA, OMS-2000.

Defensive noise generators, offered by Ukrainian firms, are, as a rule, dual-channel devices without built-in test performance and without the possibility of connection of remote control (RC), having a simplified 2-3 – frequency range way of protective noise adjustment. The exceptions from them are the following models:

- Basalt-4ga (5-band equalizer, the ability to connect a wired RC);
- MARS-TZO-4-2 (built-in performance monitoring, built-in display of output level);
- OCZI-VA/G (5-band equalizer, built-in performance monitoring, up to four independent universal channels).

The main problem of the present stage of AVP technology development is to provide an acceptable acoustic comfort of the allocated spaces. One way of solving the problem is the use of more comfortable protective noise signal, in particular "speech-like" noise. The second way to solve the problem is associated with the use of multi-component protective signals containing speech-like components, such as phonemic.

No built-in monitoring performance and the inability to connect the RC in most Ukrainian defensive noise generators and also the lack of certified mobile sets for operational health control of AVP system in the Ukraine consumer market also limits the use of AVP equipment at the facilities of information activities. The solution of these problems will require additional expenses for research and development, but in the future it will significantly improve the protection of the speech information from leaking via vibro-acoustic channels.

Literatura: ***1.*** *http://www.dstszi.gov.ua/dstszi/control/uk/publish.* ***2.*** *http://prom.ua/Generatory-shuma.* ***3****. NDTZI R-001-2000. Zasobi aktivnogo zakhistu movnoï informatsiï z akustichnimi ta vibroakustichnimi dzherelami viprominyuvannya. Klasifikatsiya ta zagal'ni tekhnichni vimogi. Rekomendatsiï.* ***4.*** *Galanskiy V., Vashchenko N., Korolyov T., Lavrent'yev A., Poroshin I., Sigayev A. Kompleksy vibroakusticheskoy zashchity rechevoy informatsii otechestvennogo proizvodstva. - // Pravove, normativne ta metrologichne zabespechennya sistemi zakhistu informatsii v Ukraini. – K., vip.10, 2005, s. 185-189.* ***5.*** *Poroshin I., Sigayev A., Nepochatykh Yu. Obespecheniye komfortnosti vydelennykh pomeshcheniy pri ispol'zovanii sistem aktivnoy vibroakusticheskoy zashchity. // Pravove, normativne ta metrologichne zabespechennya sistemi zakhistu informatsii v Ukraini. – K., vip.(1)12, 2006, s. 100-106.* ***6.*** *Poroshin I. Obosnovaniye printsipa strukturnoy optimizatsii zashchitnoy vibroakusticheskoy pomekhi. - Pravove, normativne ta metrologichne zabezpechennya sistemi zakhistu informatsiï v Ukraïni, 2009, vip. 2(19), s. 81-88.* ***7.*** *http//www.usts.kiev.ua/products.* ***8.*** *http//www.rias.com.ua/produkciya.* ***9.*** *http//www.oczi.com.ua.* ***10.*** *http//www.sergant.com.* ***11.*** *http://mars.pat.ua.* ***12****. http//www.ualeks.com/images//temp/DNG-2300.*