Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0516U000268

Особливі позначки: відкрита

Дата реєстрації: 05-04-2016

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Замула Олександр Андрійович
2. Zamula Oleksandr Andriyovich

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор наук

Аспірантура/Докторантура: ні

Шифр наукової спеціальності: 05.12.02

Назва наукової спеціальності: Телекомунікаційні системи та мережі

Галузь / галузі знань: Не застосовується

Освітньо-наукова програма зі спеціальності: Не застосовується

Дата захисту: 25-03-2016

Спеціальність за освітою: 7.091401

Місце роботи здобувача: Харківський національний університет імені В.Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: Україна, 61022, м. Харків, майдан Свободи,4

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): Д64.820.01

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Харківський національний університет імені В.Н. Каразіна

Код за ЄДРПОУ: 02071205

Місцезнаходження: Україна, 61022, м. Харків, майдан Свободи,4

Форма власності:

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR: Не застосовується

V. Відомості про дисертацію

Мова дисертації:

Коди тематичних рубрик: 49.03.07

Тема дисертації:

1. Моделі і методи синтезу складних сигналів з необхідними властивостями для захищених телекомунікаційних систем

2. Models and methods of the synthesis of complex signals with the required properties for secure telecommunication systems

Реферат:

1. Об'єктом дослідження є процеси інформаційного обміну та управління цим обміном, що протікають в ТКС та мережах. Метою роботи є покращення показників завадозахищеності та інформаційної безпеки захищеної ТКС в умовах зовнішніх і внутрішніх впливів на основі розвитку теорії та практики інформаційного обміну, а також методів синтезу складних нелінійних дискретних сигналів з необхідними властивостями. Методи дослідження: положення теорії інформації і завадостійкого кодування, теорії систем зв'язку та теорії систем сигналів, теорії криптографічного захисту інформації, теорії ймовірностей і випадкових процесів, методи аналізу та синтезу, теорії чисел, груп, кілець, полів, методи теорії цифрових автоматів, математичного та імітаційного моделювання, теорії ймовірності та математичної статистики. Наукові результати: Вперше отримано: 1. метод синтезу нелінійних криптографічних дискретних складних сигналів, який використовує випадкові (псевдовипадкові) процеси, і дозволяє створювати сигнали з необхідними ансамблевими,

структурними та кореляційними властивостями, що дає можливість покращити показники завадозахищеності та інформаційної безпеки ТКС в умовах зовнішніх і внутрішніх впливів; 2. математичну модель структури складних нелінійних дискретних сигналів у кінцевих полях, що визначає залежність характерів елементів мультиплікативної групи поля Галуа і символів дискретних послідовностей, синтезованих з використанням характерів елементів мультиплікативної групи поля, що дозволяє визначити значення показників завадозахищеності (структурної скритності) дискретних сигналів; 3. метод реалізації арифметичних модульних операцій додавання і віднімання, заснований на табличному принципі реалізації арифметичних операцій за допомогою використання спеціального коду табличного множення, що дозволяє підвищити швидкодію виконання модульних операцій додавання і віднімання; 4. метод реалізації арифметичної модульної операції множення, заснований на використанні табличного принципу шляхом використання процедури порозрядного визначення результату операції, що дозволяє підвищити швидкодію виконання модульних операцій модульного множення. Удосконалено: 1. метод синтезу нелінійних дискретних складних сигналів, у якому, на відміну від відомих, використовується залежність між елементами та індексами елементів кінцевого поля, що дозволяє підвищити швидкодію синтезу сигналів; 2. метод синтезу нелінійних дискретних складних сигналів, у якому, на відміну від відомих, використовуються механізми спрямованого (обмеженого) перебору сигналів для відбору сигналів, які відповідають певним вимогам, що дозволяє підвищити продуктивність синтезу системи сигналів з необхідними властивостями; 3. метод оцінки властивостей нелінійних дискретних складних сигналів, у якому на відміну від відомих, використано алгебраїчні властивості елементів кінцевого поля, що дозволяє збільшити швидкодію процесу дослідження властивостей сигналів, і, таким чином, підвищити продуктивність синтезу системи сигналів з необхідними властивостями; 4. метод синтезу всієї системи нелінійних дискретних сигналів, у якому, на відміну від відомих, використовується процедура зчитування та запису (за певним правилом) символів сигналу для формування всієї множини сигналів, що відноситься до цієї системи сигналів, що дозволяє підвищити продуктивність синтезу сигналів; 5. метод інформаційного обміну даними, в якому, на відміну від відомих, застосовується зміна відповідності: біт повідомлення складний сигнал і, як складні сигнали, застосовуються нелінійні дискретні сигнали з необхідними ансамблевими, структурними та кореляційними властивостями, що дозволяє покращити показники інформаційної безпеки та завадозахищеності; 6. метод реалізації арифметичних модульних операцій додавання і віднімання, який, на відміну від відомих, заснований на використанні принципу кільцевого зсуву, за допомогою представлення залишків числа двійковим кодом, за рахунок використання властивостей циклічних перестановок вмісту кільцевого регістра, що дозволяє підвищити швидкодію виконання модульних операцій. Практичне значення: 1. Практичне використання складних нелінійних завадозахищених сигналів (НС) (метод синтезу яких вперше отримано в роботі), дозволить підвищити скритність функціонування ТКС. Так, для періоду сигналу порядку 1000 елементів структурна скритність НС перевищує даний показник для лінійних класів сигналів (М-послідовностей) більш ніж в 30 разів. 2. Застосування удосконаленного в роботі методу синтезу системи НС на основі спрямованого (обмеженого) перебору сигналів для відбору таких, які володіють необхідними ансамблевими та кореляційними властивостями, дозволяє підвищити продуктивність процесу синтезу системи сигналів (від 45 до 60 відсотків). 3. Застосування удосконаленого в роботі методу синтезу систем нелінійних сигналів (НС) у кінцевих полях дозволяє підвищити (за рахунок покращених кореляційних властивостей) завадостійкість прийому. Так, під час використання нелінійних сигналів як синхропослідовностей (для періоду сигналу 256 елементів) завадостійкість прийому НС на 4 дБ вище, ніж у випадку використання лінійних класів сигналів. Застосування запропонованих в дисертації методів синтезу НС дозволить підвищити продуктивність синтезу сигналів. Так, для періоду нелінійного сигналу 10098 елементів (об'єм системи складає 2 880 сигналів) виграш у продуктивність синтезу сигналів на основі використання розробленого методу синтезу сигналів, порівняно з відомим методом, складає більше 720 разів. 4. Методи табличної реалізації модульних операцій в модулярній системі числення (МСЧ) з використанням спеціального коду табличного подання операндів, які отримані в роботі, дозволяють, залежно від величини l-байтового (l = 1 - 4, 8) машинного слова, наприклад, при виконання операції

модульного множення, від 64 до 4096 разів скоротити час виконання операцій, порівняно з використанням суматорного методу в позиційній системі числення. 5. На основі розроблених і удосконалених методів синтезу систем НС та методів швидкої реалізації модульних операцій розроблено алгоритми для їх реалізації, відповідно до яких синтезований клас апаратних засобів формування і обробки сигналів у ТКС, на які отримано 14 патентів України, що підтверджує новизну і практичну значущість отриманих у дисертації наукових результатів роботи. 6. Отримано обчислювальні алгоритми і програмний комплекс, які дозволяють реалізувати методи синтезу систем складних нелінійних дискретних сигналів та здійснювати дослідження властивостей (кореляційних, ансамблевих, структурних) вищезазначених систем сигналів. 7. При застосуванні нелінійних дискретних сигналів з періодом 10000 елементів, імітостійкість системи на три порядки вище, ніж під час використання лінійних дискретних сигналів з трирівневою функцією кореляції, які є кращими з погляду ансамблевих і кореляційних властивостей у даному класі сигналів. Отримані в роботі результати знайшли практичне впровадження і використання у процесі побудови телекомунікаційної системи в приватному акціонерному товаристві "Інститут інформаційних технологій" (м. Харків), відповідно до Договору №0003 / 01-15 від 08.07.15. (Акт використання від 28.09. 2015р.); під час виконання науково-дослідних робіт з розробки перспективних засобів зв'язку та визначення шляхів модернізації "малогабаритної завадозахищеної короткохвильової радіостанції малої потужності", яка розроблена і виготовлена в Державному підприємстві "Центральне конструкторське бюро "Протон" (м. Харків) (Акт впровадження від 23.09. 2015р.); під час виконання науково-дослідних і дослідно-конструкторських робіт: "Побудова моделюючого комплексу для управління функціонуванням корабельного з'єднання"; "Дослідження і розробка методів забезпечення живучості комп'ютерних інформаційних мереж для високотехнологічних об'єктів" в Інституті проблем реєстрації інформації Національної Академії наук України (м. Київ), (Акт впровадження від 07.09. 2015р.); у навчальному процесі кафедри безпеки інформаційних систем і технологій Харківського національного університету ім. В.Н. Каразіна під час викладання дисциплін "Управління інформаційною безпекою", "Комплексні системи захисту інформації: проектування, впровадження, супровід", "Нормативно-правове забезпечення інформаційної безпеки", що підтверджується Актом використання від 21.09. 2015р.

2. Object of research - process of information exchange and management of the exchange occurring in TCS and networks. The aim of the thesis - improvement in noise immunity and information security protected TCS in terms of external and internal influences on the basis of the theory and practice of information exchange, as well as methods for the synthesis of complex nonlinear discrete signals with the desired properties. Methods: position information theory and error-correcting coding, theory of communication and theory of signal systems, the theory of cryptographic protection of information, probability theory and stochastic processes, methods of analysis and synthesis, the theory of numbers, groups, rings, fields, methods of digital automata theory, mathematical and simulation, probability theory and mathematical statistics. Scientific results: the first time obtained by: 1. the method of synthesis of nonlinear cryptographic discrete complex signals, which uses random (pseudo-random) processes, and allows you to create the necessary signals from the ensemble, structural and correlation properties, thereby improving noise immunity and performance of information security TCS in terms of external and internal influences; 2. The mathematical model of the structure of complex non-linear digital signals in finite fields, defines the relationship of the characters of the multiplicative group of elements of the Galois field and the characters of discrete sequences synthesized using the character elements of the multiplicative group of the field, to determine the values of the indicators of noise immunity (structural secrecy) of discrete signals; 3. The method of implementation of modular arithmetic operations of addition and subtraction, based on the principle of table implementation of arithmetic operations by using a special code table multiplication, can increase the speed of implementation of modular operations of addition and subtraction; 4. The method of implementing arithmetic modular multiplication operation based on the use of the principle of the table through the use of the procedure determine the result of bitwise operations can improve performance performing modular operations modular multiplication. Improved: 1. The method of synthesis of complex nonlinear discrete signals, in which, unlike the prior art, uses a relationship between elements of a finite field and index elements allows to increase the speed of

synthesis signals; 2. The method of synthesis of complex nonlinear discrete signals, in which, unlike the known mechanisms used directional (limited) sorting signals for selecting signals that meet certain requirements to improve performance signal synthesis system with the required properties; 3. The method of evaluation of the properties of nonlinear discrete complex signals, which unlike the prior art, applied algebraic properties of finite field elements, thus increasing the process speed of investigating the properties of the signals and thus improve the performance of the synthesis signal with the required properties of the system; 4. The method of synthesis of the entire system of nonlinear discrete signals, in which, unlike the known procedure is used to read and write (for a particular rule) pilot symbols to generate a plurality of signals only relates to the system of signals to improve performance synthesis signals; 5. The method of information communication, which, in contrast to the known, applies a change of conformity: bit message and a complex signal as complex signals, are applied non-linear digital signals with the necessary ensemble, structural and correlation properties that can improve information security performance and noise immunity ; 6. The method of implementing the modular arithmetic operations of addition and subtraction, which, unlike the prior art, based on the use of the principle of the shear ring, by representing the number of residual binary code, by using a cyclic permutation properties annular register content improves execution performance of modular operations. Practical value: 1. Practical use of complex non-linear interference-proof signal (NS) (which is a method of synthesis for the first time obtained in), will improve the functioning of the secrecy of TCS. So, for a period of about 1000 members of the National Assembly structural stealth signal exceeds the figure for the class of linear signals (M-sequence) is more than 30 times. 2. Application of improvements in the synthesis method of emergency system based on directional (limited) sorting signals for the selection of those that have the necessary ensemble and correlation properties, improves the performance of the process of synthesis of signal systems (from 45 to 60 percent). 3. Application of an improved method in the synthesis of non-linear systems signals (NS) in finite fields can increase (due to improved correlation properties) Immunity reception. Thus, when using a non-linear signals as a synchronization sequence (256 elements for a period of the signal) reception immunity NS 4 dB higher than in the case of linear signal classes. The application proposed in the thesis NS synthesis methods will improve the performance of the synthesis signals. Thus, for a period of 10098 nonlinear signal components (the volume of the system is 2,880 signals) based on the gain in efficiency of the synthesis signal using synthesizing signals developed method compared to the conventional method, it is more than 720 times. 4. Methods tabular implementation of modular operations in radix modular using a specific code table view operands obtained in enable, depending on the l-byte (l = 1 - 4, 8) of the machine word, for example, the operation of modular multiplication, from 64 to 4096 times to reduce the execution time of operations compared to using summation method in a positional number system. 5. On the basis of the developed and improved methods of synthesis of the National Assembly of systems and methods for the rapid implementation of modular operations, the algorithms for their implementation, in accordance with which synthesized a class of hardware formation and processing of signals in TCS, which received 14 patents of Ukraine, which confirms the novelty and practical significance of the research in the dissertation work results. 6. obtained computational algorithms and software package that allow you to implement methods for the synthesis of complex nonlinear systems, discrete signals and carry out studies of the properties (correlation, ensemble, structural) above signal systems. 7. In the application of non-linear digital signals with a period of 10,000 items imitoprotection system to three orders of magnitude higher than when using linear digital signals to the three-level correlation function, which are the best in terms of ensemble and correlation properties in this class of signals. The obtained results have found practical implementation and use in the process of building a telecommunications system in the private joint-stock company "Institute of Information Technology" (Kharkov), in accordance with the Contract №0003 / 01-15 on 07/08/15. (Use Act of 28.09.2015.); in carrying out research work on the development of advanced communications and ways of modernization "interference-protected compact shortwave radio stations of low power", which is designed and manufactured in the State Enterprise "Central Design Bureau" Proton "(Kharkov) (implementation of the Act 23.09. 2015) in the performance of research and development work:. "The construction of modeling complex to control the operation of the ship connection", "research and development of methods to ensure the survivability of computer information networks for high-tech facilities" at the Institute for information

recording of National Academy of Sciences of Ukraine (Kiev), (Act of introduction from 07.09 2015), in the educational process of the department of security of information systems and technologies Kharkov national University VN Karazin at teaching discipline "information security Management", "Complex protection of the information system: design , implementation and maintenance, "" Regulatory information security ", as evidenced by the use of the Act 21.09. 2015.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки:

Стратегічний пріоритетний напрям інноваційної діяльності:

Підсумки дослідження:

Публікації:

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації:

Зв'язок з науковими темами:

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Горбенко Іван Дмитрович
2. Gorbenko Ivan Dmytrovich

Кваліфікація: д.т.н., 20.02.12

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Бондаренко Олег Володимирович

2. Бондаренко Олег Володимирович

Кваліфікація: д.т.н., 05.12.02

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Климаш Михайло Миколайович
2. Климаш Михайло Миколайович

Кваліфікація: д.т.н., 05.12.02

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Власне Прізвище Ім'я По-батькові:

1. Кучук Георгій Анатолійович
2. Кучук Георгій Анатолійович

Кваліфікація: д.т.н., 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

Рецензенти

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Приходько Сергій Іванович
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Приходько Сергій Іванович
Відповідальний за підготовку облікових документів	
Реєстратор	
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Т.А.