

УДК 621.39

Н.Ф. БОГОМОЛОВ

Национальный технический университет Украины «Киевский политехнический институт»

А.А. ТРОЦ

Национальный университет биоресурсов и природопользования Украины

МЕРОПРИЯТИЯ ПО ТЕХНИЧЕСКОЙ РЕАЛИЗАЦИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ ПЕРСОНАЛЬНЫХ ЭВМ

Проектирование системы защиты информации на этапе ее технической реализации на данном этапе связано с решением следующей проблемы:

-необходимость формирования на основе классических методов аппроксимации и линеаризации информативного изображения базового объекта контроля;

формирование и анализ пороговых входных сигналов управления, определяющие количество каналов ввода информативного комплексного сигнала;

-определение комплексных факторов, вносящих обезображивающую действие на информативное изображение базового объекта контроля;

-обеспечение защиты информации контролируемого объекта, от искажений;

-кодирование защиты и кодированные преобразования информации контроля для дальнейшей обработки и передачи потребителю.

Ключевые слова: системы защиты информации; методы аппроксимации и линеаризации; объект контроля; кодированный защиту.

M.F. BOGOMOLOV

National Technical University of Ukraine "Kyiv Polytechnic Institute", Kyiv, Ukraine

A.A. TROTS

National university of life and environmental sciences of Ukraine, Kyiv, Ukraine

MEASURES FOR IMPLEMENTATION OF THE TECHNICAL INFORMATION PROTECTION OF PERSONAL COMPUTER

Design of information security at the stage of technical implementation at this stage is due to address the following issues:

-neobhidnist formation based on classical methods of approximation and linearization informative base object image control;

-forming threshold analysis and input control signals, determining the number of channels informative input complex signal;

-definition complex factors that contribute distorting effect on the underlying object informative image control;

-security information security facility that is controlled from distortion;

-kodovanyy defense transformation and coded control information for further processing and transmission to consumers.

Keywords: information security system; approximation and linearization techniques; object control; coded protection.

Введение

Теория материально-энергетической избыточности информативно может быть обеспечена разработкой основных понятий информативной информации, передаваемой обрабатываемой воспринимается заказчиком и может быть запечатленной, зарегистрированной и воспроизведенной с гарантированным степенью защищенности. Теория дает трактовку о новейших общенаучные подходы к восприятию материальной действительности в смысле ее теоретического объяснения. Она позволяет трактовать понятие объектов исследования как отдельных целостных информативно-материальных динамических структур. В современных информативных технологиях информация об объекте имеет определенные границы и определяется как информативный объем объекта отображения. Искажение информативного объема объекта отображения приводит к нарушению точности отображения, обработки, передачи и восстановления информации. На этапе восстановления информации принимаются меры по ее кодифицированности методами специальных искажений информации, передаваемой или ее подачу отдельно параллельными каналами связи отдельными кодированными блоками, которые независимо друг от друга доставляются.

В рамках теории сформированы основные понятия информативных объемов, позволяющих интегрировать их в общих чертах физическую теоретическую основу. Такой подход позволяет использовать эту методику и в других научных сферах при отражении реальных процессов.

Исходные предпосылки:

Определение основных понятий информативности сигнала

1. Объект сигнала - это объект, действие сигнала на который вызывает реакцию (информативную) объекта.

2. Сигнал объекта - это энергетическое воздействие окружающей среды, способно вызвать

возбуждение (в энергетическом смысле) объекта сигнала.

3. Сигнал "1" - сигнал, вызвавший возбуждения объекта сигнала.

Сигнал "0" - сигнал, вызвавший возбуждения объекта сигнала в нулевом (начальном) состоянии.

4. Сигнал фона - сигнал среды, способен сравнить энергетику объекта сигнала и самой среды.

Сигнал фона определяет уровень самого сигнала: "1" или "0".

Таким образом сочетание объекта, на который действует сигнал, сигнала объекта и сигнала фона дают возможность интерпретации действия сигнала в рамках количественной характеристики ряда

Маклорена для (см. Рис.1.) $e = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \dots + \frac{1}{n!} + \dots \rightarrow \infty$.

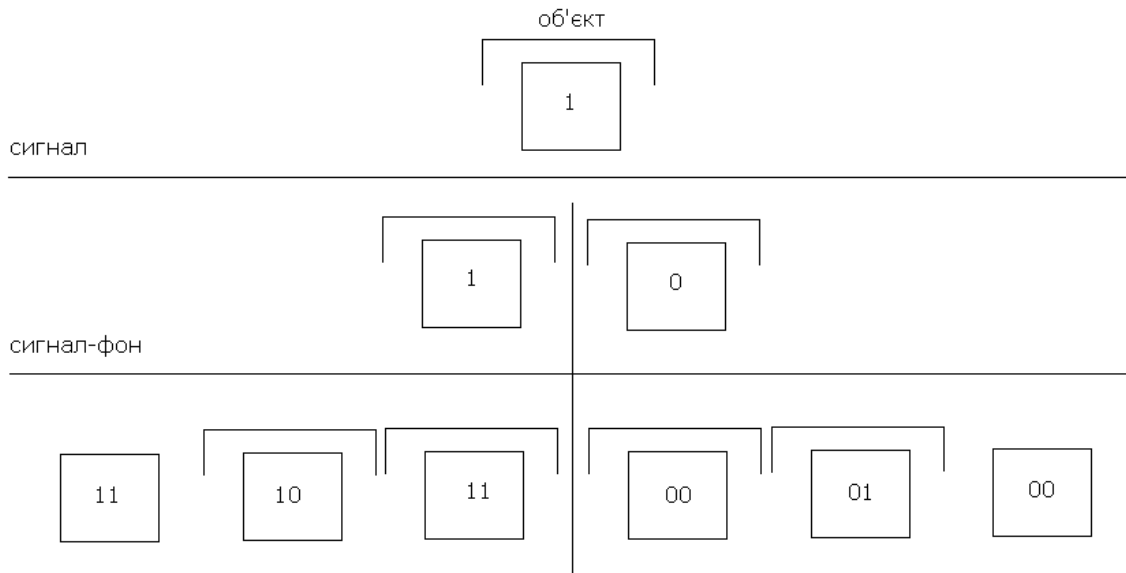


Рис.1. Взаимодействие сигнала отклика, объекта информирования и фона передачи информации.

Цель

При разработке комплексной системы защиты информации (КСЗИ) сформулируем основу построения КСЗИ при передаче информативных объемов информации:

1. КСЗИ предполагает двухканальную независимую передачу информации средствами передачи информации от поставщика информации заказчику. Первый канал - это передача "ключа" кодирования; второй канал - это передача кодированного объема информации (даже открытым доступом).

2. Пусть информация о состоянии объекта информативно анализируется, представленная в прогрессирующем пространстве по количеству энергетических состояний, образует объект на базе информативно-энергетических возможностей оборудования передачи-восприятия информации от поставщика информации в ее заказчика. Тогда при передаче реальных объемных изображений (например), то есть трехмерных, прогрессирующий пространство состояний объекта, подлежащего информированию со стороны поставщика информации, записывается зависимостью

$$N_E = e^{xyz}$$

где N_E - функция энергетических состояний объекта; - Координаты информативного объема объекта информирования.

3. Перед передачей информация превращается из полученного прогрессирующего пространства в евклидово путем формирования соответствующего оператору перехода из прогрессирующего пространства в евклидово. Есть:

$$e^{xyz} = Q(N_E)xyz = Q(N_E)V$$

где $Q(N_E)$ - оператор перехода с прогрессирующего информативного пространства в евклидово, V - трехмерный информативный объем в евклидовом пространстве (некоторое объемное изображение информативного объема, подлежащего передаче заказчику).

4. Сигнал V к заказчику поставляется обычными каналами передачи информации в свободном доступе. Сигнал $Q(N_E)$ является ключом кодирования и подается при необходимости в кодированном виде заказчику по конфидициальных каналах передачи информации. Без знания ключа кодирования восстановления прогрессирующего информативного объема поставщика информации невозможно.

5. Таким образом сигнал V может быть передан в виде обычного объемного изображения.

Решение проблемы

Энергетическое пространство Дирака, а также и Реалиума, будучи прогрессирующим, описывается формулой

$$E = e^{x \cdot y \cdot z} \tag{1}$$

Причем для Дирака $x, y, z \leq 1$,
А для Реалиума $x, y, z \geq 1$.

Состояние $x = y = z = 1$ является состоянием пределы Дирак-Реалиум (Д-Р). Если предел Д1-Р = Р-Д2, то Д1-Р-Д2 является взаимосвязанный Д-Р-Д-переход, который имеет свои определенные свойства равновесия.

Условием перехода Д1-Р является равенство пространства Д1 и Р (ПД1, ПР) к евклидова пространства Пе, в котором Д1 и Р существуют.

Объем пространства Д1е

$$V_{D1e} = e^{x \cdot y \cdot z}, \quad 0 \leq x, y, z \leq 1. \tag{2}$$

Объем пространства Ре

$$V_{Re} = e^{x \cdot y \cdot z}, \quad 1 \leq x, y, z \leq \infty. \tag{3}$$

Объем пространства Пе

$$V_e = exyz. \tag{4}$$

Таким образом, условием перехода Д1 в Р является

$$e^{x \cdot y \cdot z} = exyz \text{ при } 0 \leq x, y, z \leq \infty. \tag{5}$$

Как будет показано далее, это условие выполняется для целого взаимосвязанного Z из ряда значений x, y (оператор перехода ПД1, Р в Пе). Для наглядности одномерный пространство имеет две следующие величины:

$$e^x = ex \text{ при } x = 1, \text{ и } 1,8 \leq x \leq 1,9. \tag{6}$$

Есть

$$f(x) = \frac{e^x}{ex}, \tag{7}$$

имеет вид (см. Рис. 2).

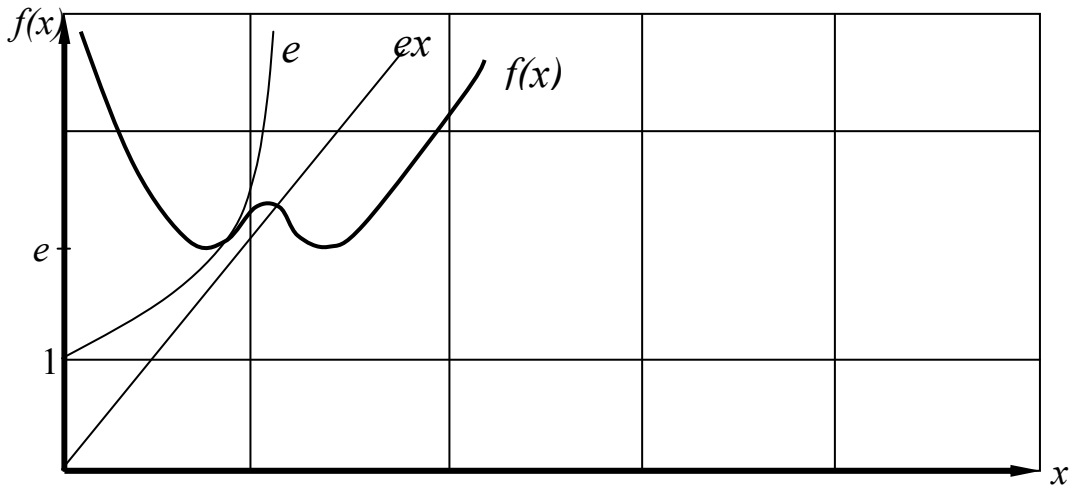


Рис. 2. Взаимосвязь пространств.

Исходя из того, что для n-мерных пространств условие равновесия выполняется n + 1 раз, условием возникновения Д1-Р-Д2-перехода является условие:

$$\begin{cases} x_{D1}^* = x_P^* = x_e^* = x_{D2}^* \\ y_{D1}^* = y_P^* = y_e^* = y_{D2}^* \\ z_{D1}^* = z_P^* = z_e^* = z_{D2}^* \end{cases} \tag{8}$$

Если условие (8) не выполняется при наличии других Ди, то Д1-Р-Ди-переход может возникнуть для других Ди при условии выполнения (8) для каждого из них конкретно. В этом случае Д1-Р-Д2-переход может и не быть.

Следующим замечанием является то, что пара Д1-Р может образовывать с другими полные Д-Р-Д-переходы одновременно несколько Д-Р-Д-переходов на разных ступенях (значениях x, y, z) своего развития.

Таким образом, реальный замкнутый процесс это:

- Движение Д-Р-Д-переходов к равновесию;
- Нарушение равновесия из-за изменений условий среды (x, y, z);
- Движение к следующему Д-Р-Д-перехода.

То есть условие существования замкнутой системы - это наличие связанных между собой Д-Р-Д-переходов. Учитывая одновременно энергетическое высвобождение и поглощение, разнесены в пространстве, ривногава Д-Р-Д-перехода является неустойчивой, и каждый Д-Р-Д-переход - это конкретное энергетическое перегруппировки пространства с изменением конкретных балансов энергий для конкретных Дирак-Реалиумив-Дирака при полной независимости от других Дирак-Реалиумив-Дирака. Переход Д-Р-Д является временная энергетическое взаимодействие трех пространств, одновременно существуют в одном или немногих евклидовой.

Если Д, Р и Д имеют разную евклидову размерность (то есть, существуют в различных евклидовых пространствах), то для условия (8) возникновения Д-Р-Д-перехода добавляется условие равенства метрик евклидовых пространств:

$$Pe_{D_1} = Pe_P = Pe_{D_2} \quad (9)$$

есть

$$\begin{cases} x_{e_{D_1}} = x_{e_P} = x_{e_{D_2}} \\ y_{e_{D_1}} = y_{e_P} = y_{e_{D_2}} \\ z_{e_{D_1}} = z_{e_P} = z_{e_{D_2}} \end{cases} \quad (10)$$

Судя по (10) и (8) нетрудно доказать, что условие (10) - это условие (8), но для евклидова пространства, общего для трех независимых евклидовых пространств (9), только более высокого порядка (в этом случае, порядок совместного евклидова пространства $Pe\Sigma$ на единицу больше). Очевидно, если порядок евклидовых пространств в (9) равен трем, то $Pe\Sigma$ - четырем, что для реальной воображения сложно. В таких случаях оперируют $Pe\Sigma$ третьего порядка, но как временного (то есть - возник и исчез) с функцией своего описания.

Реализация результатов исследования

Проектирование системы защиты информации на этапе ее технической реализации на данном этапе связано с решением следующей проблемы

- необходимость формирования на основе классических методов аппроксимации и линеаризации информативного изображения базового объекта контроля;
- формирование и анализ пороговых входных сигналов управления, определяющие количество каналов ввода информативного комплексного сигнала;
- определение комплексных факторов, вносящих обезображивающую действие на информативное изображение базового объекта контроля;
- обеспечение защиты информации контролируемого объекта, от искажений;
- кодовых защиту и кодированные преобразования информации контроля для дальнейшей обработки и передачи потребителю.

В качестве пути решения поставленной проблемы проектирования конкретной системы защиты информации, поступающей от конкретного объекта контроля, на этапе технической реализации предложено предварительное выполнение ряда теоретико-технических мероприятий:

- 1) разработка и анализ комплекса кодов параметра, формирует устойчивое изображение базового объекта контроля на мониторе ЭВМ;
- 2) обеспечение режима сохранения полученного кодированного изображения / информации / путем создания ключа кодирования на базе программной реализации системы кодирующих импульсов, используя прогрессивные методы кодирования;
- 3) создание программного комплекса кодирования ключа в режиме кодирования входа в базу данных
- 4) объекта обработки необходимой информации
4. обеспечение автоматизации доступа к каналам получения, обработки и дальнейшей отправки информации;
- 5) предлагается разработка «идеи абсолютного шифра» - обеспечение нуля на входе при обработке полученной информации;
- 6) создание комплекса нормируемых «входов» для обработки персональной информации;

Кроме этого рекомендуется ряд мероприятий организационного характера, в частности: разработка рекомендаций обеспечения гарантий пользователей кодированной информации; дальнейшая стандартизация средств ЭВМ персонального пользования; урегулирование вопросов сметы производства и содержание персональных кодирующих средств; урегулирование вопросов контроля качества персональных средств кодирования и тому подобное.

Вывод

Таким образом для разработки эффективной конкретной системы защиты информации, поступающей обрабатывается, хранится в отдельной ЭВМ и передается другим пользователям, предлагается путь персонального программного кодирования информации на базе персонального средства кодирования.

Литература

1. Таланчук П.М., Рущенко В.Т. Основы теории проектирования измерительных приборов: Учеб.пособие. – К.: Выща школа. Головное изд-во, 1989. – 454 с., ил.
2. А.Г. Конюхов. Метрологическое обеспечение в приборостроении. Аспекты управления. – М.: Изд-во стандартов, 1990. – 208 с., ил.
3. Методы синтеза нелинейных систем автоматического управления. Под ред. д.т.н.,проф. С.М.Федорова. – М.: Наука, 1986. – 210 с.
4. Засоби вимірювання автоматичного зрівноваження: Навч.посібник. За ред. П.М. Таланчука. – К.: Либідь, 1994. – 288 с.
5. Троц А.А. Основы математического опису теорії Дірака-Реаліума. Нац.техн.ун-т України “Київ.політехн. ін-т”, - Київ, 1995, - 38 с.: іл. – Бібліогр.: 5 назв. – Рос. – Деп. в ДНТБ України 20.12.95 № 130-Ук96.
6. Кокаровцев В.В., Троц А.А. Фізичні аспекти теорії Дірака-Реаліума. Нац.техн. ун-т України “Київ.політехн. ін-т”, - Київ, 1995, - 50 с.: іл. – Бібліогр.: 6 назв. – Рос. – Деп в ДНТБ України 20.12.95 № 129-Ук96.
7. Таланчук П.М., Остафьев В.А., Троц А.А., Махмудов К.Г., Мирзаев А.А., Глушенко Ю.Б. Дифференциальное уравнение причинно-следственных связей. К.: Вестник КПИ. Приборостроение, - 1995. – В 25. – С. 3-19.
8. Троц А.А., Буряк В.Г., Глушенко Ю.Б. Причинно-следственные аспекты проектирования оснастки. Перспективные технологии, оснастка и методология подготовки производства. Научный технический сборник / Под ред. проф. Румбешты В.А., Глоби А.В. – К.: ООО “Международ.фин. агенство”, 1997. – С. 64-66.
9. Дружинин В.В., Кондоров Д.С. Системотехника. – М.: Радио и связь, 1985. – 200 с, ил.
10. Розенталь И.Л. Элементарные частицы и структура Вселенной. - М.: Наука, 1984. – 112 с.
11. Бояринов В.А., Рущенко В.Т. Синтез математической модели средств измерений индуктивным методом самоорганизации на ЭВМ // Вестн. Киев. политехн. ин-та. Приборостроение. – К.:, 1985. – Вып. 15. – С. 37.
12. 12. УДК 510.2:541.1 ГАСНТІ 27.23;27.21 Основы математического опису теорії Дірака-Реаліума (Троц А.А Науково-технічний університет України „Київський політехнічний інститут”), - Київ, 1995, - 38 стр. Іл.- Бібліогр. 5 назв. – Рос.- Деп. в ДНТБ України 20.12.95 № 130 – Ук 96.
13. Кузьмичев В.Е. Законы и формулы физики / Отв. ред. В.К.Тартаковский. К.: Выща школа, 1989. – 864 с.
14. Ваня Я. Анализаторы газов и жидкостей / Под ред. О.С.Арутюнова. М.: Машиностроение, 1970.– 490 с.
15. Мирзаев А.А. Автоматизированное определение обрабатываемости металлов: Дис.... канд. техн. наук. К.: КПИ, 1988.– 197 с.

References

1. Talanchuk P.M., Rushchenko V.T. Osnovy teorii proyektirovaniya izmeritel'nykh priborov: Ucheb.posobiye. – K.: Vyshcha shkola. Golovnoye izd-vo, 1989. – 454 s., il.
2. A.G. Konyukhov. Metrologicheskoye obespecheniye v priborostroyenii. Aspekty upravleniya. – M.: Izd-vo standartov, 1990. – 208 s., il.
3. Metody sinteza nelineynykh sistem avtomaticheskogo upravleniya. Pod red. d.t.n.,prof. S.M.Fedorova. – M.: Nauka, 1986. – 210 s.
4. Zasobi vimiryuvannya avtomatichnogo zrivnovazheniya: Navch.posibnik. Za red. P.M. Talanchuka. – K.: Libid', 1994. – 288 s.
5. Trots A.A. Osnovi matematichnogo opisu teorii Diraka-Realiuma. Nats.tekhn.un-t Ukraini “Kiyv.politekhn. in-t”, - Kiyv, 1995, - 38 s.: il. – Bibliogr.: 5 nazv. – Ros. – Dep. v DNTB Ukraini 20.12.95 № 130-Uk96.
6. Kokarovtsev V.V., Trots A.A. Fizichni aspekti teorii Diraka-Realiuma. Nats.tekhn. un-t Ukraini “Kiyv.politekhn. in-t”, - Kiyv, 1995, - 50 s.: il. – Bibliogr.: 6 nazv. – Ros. – Dep v DNTB Ukraini 20.12.95 № 129-Uk96.
7. Talanchuk P.M., Ostaf'ev V.A., Trots A.A., Makhmudov K.G., Mirzayev A.A., Glushenko YU.B. Differentsial'noye uravneniye prichinno-sledstvennykh svyazey. K.: Vestnik KPI. Priborostroyeniye, - 1995. – V 25. – S. 3-19.
8. Trots A.A., Buryak V.G., Glushenko YU.B. Prichinno-sledstvennyye aspekty proyektirovaniya osnastki. Perspektivnyye tekhnologii, osnastka i metodologiya podgotovki proizvodstva. Nauchnyy tekhnicheskyy zbornik / Pod red. prof. Rumbeshty V.A., Globi A.V. – K.: ООО “Mezhdunar. fin. agenstvo”, 1997. – S. 64-66.
9. Druzhinin V.V., Kondorov D.S. Sistemotekhnika. – M.: Radio i svyaz', 1985. – 200 s, il.
10. Rozentall I.L. Elementarnyye chastitsy i struktura Vselennoy. - M.: Nauka, 1984. – 112 s.
11. Boyarinov V.A., Rushchenko V.T. Sintez matematicheskoy modeli sredstv izmereniy induktivnym metodom samoorganizatsii na EVM // Vestn. Kiyev. politekhn. in-ta. Priborostroyeniye. – K.:, 1985. – Vyp. 15. – S. 37.
12. UDK 510.2:541.1 GASNTI 27.23;27.21 Osnovi matematichnogo opisu teorii Diraka-Realiuma (Trots A.A Naukovo-tekhnichniy universitet Ukraini „Kiyv'skiy politekhnichniy institut”), - Kiyv, 1995, - 38 str. Il.- Bibliogr. 5 nazv. – Ros.- Dep. V DNTB Ukraini 20.12.95 № 130 – Uk 96.
13. Kuz'michev V.Ye. Zakony i formuly fiziki / Otв. red. V.K.Tartakovskiy. K.: Vyshcha shkola, 1989. – 864 s.
14. Vanya YA. Analizatory gazov i zhidkostey / Pod red. O.S.Arutyunova. M.: Mashinostroyeniye, 1970.– 490 s.
15. Mirzayev A.A. Avtomatizirovannoye opredeleniye obrabatyvayemosti metallov: Dis.... kand. tekhn. nauk. K.: KPI, 1988.– 197 s.

Рецензія/Peer review : 19.4.2017 р.

Надрукована/Printed : 15.6.2017 р.

Стаття рецензована редакційною колегією