МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ «МИКОЛАЇВСЬКА ПОЛІТЕХНІКА»

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

СТАН ТА УДОСКОНАЛЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО – ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

(SITS'2015)

09 – 12 червня 2015 року

МИКОЛАЇВ – КОБЛЕВО

Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2015) – Миколаїв: 2015. - 108 с.

У збірник ввійшли матеріали, представлені і обговорені під час проведення 7-ої Всеукраїнської науково-практичної конференції «**СТАН ТА УДОСКОНАЛЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО – ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ (SITS'2015)**» 09-12 червня 2015 року в с. Коблево, Миколаївської області.

Матеріали збірника можуть бути корисними для науковців і фахівців сфери інформаційних технологій та кібербезпеки, персоналу з безпеки установ і підприємств різних форм власності, керівників вищих навчальних закладів, професорсько-викладацького складу, аспірантів і студентів.

Редакційна колегія випуску:
Вільський Г.Б., д.ф.-т.н., професор; Корнейко О.В., к.т.н., професор;
Корченко О.Г., д.т.н., професор; Козловський В.В., д.т.н., професор;
Мельник С.В., к.е.н., доцент; Голубєв В.О., к.ю.н., доцент;
Михалишин Б.Є., к.т.н.

Матеріали публікуються за оригіналами, наданими авторами.
Претензії до організаторів не приймаються.

МИКОЛАЇВ – КОБЛЕВО
2015

ЗМІСТ

1. Гавриленко О.В., Корнейко О.В. **Шляхи гармонізації національної нормативної бази із захисту інформації в інформаційно-телекомунікаційних системах з міжнародними стандартами** **5**

2. Воронов В.Р. **Проблемні питання нормативного забезпечення захисту інформації від витоку технічними каналами та шляхи їх вирішення** **8**

3. Гнатюк С.О. **Інформаційно-психологічна безпека держави в умовах ведення інформаційної війни** **9**

4. Вільський Г.Б. **Інформаційна безпека і ризики субстандартного судноплавства** **10**

5. Пядишев В.Г., Сіфоров О.І. **Про необхідність боротьби з кіберзлочинністю в зонах міжнародних операцій з підтримання миру і безпеки.** **11**

6. Майданюк П. В. **Проблеми захисту інформації в ІТС державних органів** **12**

7. Рябий М.О., Гнатюк І.Ю. **Застосування методів ведення інформаційної війни для здобуття конкурентних переваг на ринку** **13**

8. Левківський К.М., Івлєва Л.М. **Якісна освіта – запорука самореалізації особистості** **16**

9. Мельник С.В. **Реформування професійних та освітньо-кваліфікаційних стандартизованих систем України: зиски та ризики** **17**

10. Сухарніков Ю.В. **Освітнє законодавство України в контексті глобалізаційного розвитку** **18**

11. Білоусов В.В. **Своєрідність освітніх положень в Україні та США** **21**

12. Герганов Л.Д. **Освітні парадигми сучасної системи професійної підготовки фахівців для морської галузі** **22**

13. Вільський Г.Б., Михалишин Б.Є. **Формування критеріїв оцінювання наукової значимості студентських конкурсних досліджень** **26**

14. Манькусь І.В., Недбаєвська Л.С. **Освітній проект «Повертаємося до реальності» як шлях профілактики комп'ютерної залежності** **28**

15. Голубєв В.О. **Соціальні мережі як поле битви в інформаційній війні** **29**

16. Шипілов В.А. **Проблеми інформаційно-особистої безпеки при навчанні молоді** **31**

17. Юдін О.К., Весельська О.М. **Аналіз параметрів оцінки якості функціонування інформаційно-комунікаційної системи державного призначення** **34**

18. Одарченко Р.С., Мачалін І.О., Ткаліч О.П. **Удосконалення систем безпеки безпроводових мереж нових поколінь** **37**

19. Василіу Є.В., Лімар І.В. **Квантовий криптографічний захист системи електронного голосування з використанням схеми «неперервних змінних»** **40**

20. Корченко А.О. **Формування лінгвістичних еталонів на основі кортежної моделі для систем виявлення вторгнень** **43**

21. Кищенко В.В., Рябий М.О. **Особливості захисту критичних державних інформаційних ресурсів від спаму: класифікаційний підхід** **46**

22. Чернявський О.С. **Застосування парольних систем аутентифікації для забезпечення конфіденційності інформації** **48**

23. Обозна А.О. **Інструменти підвищення інформаційної безпеки в банківських установах** **50**

24. Кошевий В.М., Шишкін О.В. **Вдосконалення морських суднових систем навігації і радіозв'язку в рамках розвитку електронної навігації** **53**

25. Ткач Ю.М. **Якісна оцінка ризиків інформаційної безпеки державних вищих навчальних закладів** **55**
26. Мехед Д.Б., Базилевич В.М., Петренко Т.А. **Оцінка ризиків інформаційної безпеки на підприємстві** **59**
27. Козловський В.В., Міщенко А.В. **Методологія інформаційної безпеки в авіатранспортному комплексі** **62**
28. Корченко О.Г., Ахметов Б.С., Казмирчук С.В., Гололобов А.Ю. **Метод інкрементуваня еталонів параметрів для систем аналізу та оцінювання ризиків** **65**
29. Дудатьєв А.В., Дудатьєва В.М., Коротаєв Д.О. **Метод управління інформаційною безпекою** **69**
30. Хохлачова Ю.Є. **Математичне моделювання критеріїв оптимальності та обмеження загроз інформації** **70**
31. Мохор В.В., Максименко Є.В., Зінченко Я.В., Цуркан В.В. **Умови використання спектрального підходу для оцінювання ризику безпеки інформації** **72**
32. Гнатюк В.О., Труфанов А.І. **Мережево-центричний підхід до процесу управління інцидентами інформаційної безпеки** **73**
33. Кінзерявий В.М., Грабінський Д.М., Вороніна А.В. **Оцінка стійкості блокових симетричних шифрів до деяких видів криптоаналізу** **75**
34. Сніжко В.В. **Використання когнітивного моделювання при побудові систем захисту інформації** **78**
35. Фесенко А.О., Швець В.А. **Метод ідентифікації користувачів на базі райдужної оболонки ока** **81**
36. Гізун А.І. **Системи виявлення інцидентів – потенційних кризових ситуацій** **84**
37. Васєв В.О. **Принципи побудови захищених систем пакетної передачі даних на основі IP-протоколу** **87**
38. Гур'єв В.І. **Використання технології хмарних обчислень у вищих навчальних закладах** **90**
39. Гнатюк С.О., Жмурко Т.О., Стояновіч А., Сєйлова Н.А. **Метод підвищення захищеності систем захисту інформації на базі квантових технологій** **93**
40. Струбицький П.Р. **Проблеми і аспекти збору соціальних даних в Інтернет-мережах** **97**
41. Струбицький Р.П. **Підходи до мультиплексування передачі документів у розподілених мережах** **99**
42. Нємкова О.А. **Швидка ідентифікація об'єктів у кіберпросторі за допомогою біометричних шаблонів** **101**
43. Васянович В.В. **Інтелектуальні технології в управлінні інформаційною безпекою** **103**
44. Глущук Ю.О., Ханько Я.Б. **Сучасні напрямки розвитку банківських інформаційних сервісів** **106**

Корнейко Олександр Васильович, *к. т. н., професор,*
Гавриленко Олексій Вадимович, *к. т. н.,*
Адміністрація Державної служби спеціального зв'язку
та захисту інформації України

ШЛЯХИ ГАРМОНІЗАЦІЇ НАЦІОНАЛЬНОЇ НОРМАТИВНОЇ БАЗИ ІЗ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ З МІЖНАРОДНИМИ СТАНДАРТАМИ

В умовах здійснення інтеграції з європейським суспільством в усіх сферах життєдіяльності держави одним з пріоритетних напрямків її проведення є гармонізація національної нормативної бази з міжнародними стандартами. На сьогодні розвиток галузі технічного захисту інформації (далі – ТЗІ) є одним з важливих факторів забезпечення інформаційної, та, відповідно, національної безпеки держави. Актуальним напрямком розвитку галузі є вивчення можливих шляхів проведення гармонізації відповідної нормативної бази, зокрема, стосовно захисту інформації в інформаційно-телекомунікаційних системах (далі – ІТС).

Для визначення того, чи відповідає національна база у сфері ТЗІ міжнародним стандартам, чи гармонізована вона з ними і яким є рівень гармонізації, слід провести певне їх зіставлення. На наш погляд, найбільш об'єктивним підходом до його проведення є аналіз з позицій стандартів міжнародної організації зі стандартизації ISO.

Загальносвітове визнання мають стандарти серії ISO-9000 стосовно систем управління якістю продукції. На їх базі за останні роки впроваджено значну кількість стандартів, у тому числі, й у сфері інформаційної безпеки. Під продукцією, у даному випадку, будемо розуміти комплексні системи захисту інформації (далі – КСЗІ) в ІТС, а також їх складові. Розгляд переліку мінімально необхідних вимог ДСТУ ISO-9001:2000 [1], пов'язаних з проектуванням, виробництвом (розробленням), реалізацією та обслуговуванням продукції, до якості створеної КСЗІ в ІТС на всіх етапах її життєвого циклу показує, що на сьогодні в Україні відповідні вимоги до КСЗІ та етапи робіт з її створення унормовано.

Системно та структурно зі стандартом ISO 9001:2000 узгоджений міжнародний стандарт системи управління інформаційною безпекою (далі – СУІБ) ISO/IEC 27001:2013 [2], що визначає вимоги для створення, впровадження, експлуатації, моніторингу, аналізу, підтримки і поліпшення документованої СУІБ в контексті загальних ризиків організації бізнесу. Стандарт призначений для сертифікації СУІБ в органах оцінки відповідності. В Україні у 2012 році вступив дію стандарт ДСТУ ISO/IEC 27001:2010.

ISO/IEC 27002:2013 [3] встановлює принципи та надає рекомендації з розробки, впровадження, підтримки і поліпшення управління інформаційною безпекою в організації. В стандарті викладено детальний звід правил для такого управління, він містить його цілі і розкриває відповідні елементи управління, перелік яких представлений в ISO/IEC 27001. Положення стандарту слугують основою для вибору організаціями, що впроваджують СУІБ згідно ISO/IEC 27001, відповідних елементів управління і їх застосування для окремих бізнес-процесів.

Стандарти визначають основні не технічні аспекти захисту інформації, представлені в будь-якій формі і призначені для демонстрації здатності організації захищати свої інформаційні ресурси. Вони є нейтральними в технологічному плані і завжди залишають можливість вибору технологій. Стандарти описують заходи із забезпечення безпеки в загальному вигляді, але, не містять жодних технічних аспектів з їх реалізації.

Розробки міжнародних критеріїв забезпечення безпеки інформації в ІТС для спільного використання велись в середині 90-х років групою розробників з США, Канади, Франції, Німеччини, Великобританії, Нідерландів разом з групою WG 3 "Критерії оцінки безпеки"

об’єднаного технічного комітету JTC1 "Інформаційні технології" ISO/IEC і вилились у створення стандарту ISO/IEC 15408, який має історичну назву “Спільні критерії” (СК).

Загалом СК на сьогодні узгоджені з іншими існуючими стандартами у сфері інформаційної безпеки, відповідають сучасному рівню розвитку інформаційних технологій і є найбільш універсальним, найбільш формалізованим і функціонально повним набором критеріїв, який може бути застосовано для будь-яких ІТ-продуктів на всіх етапах життєвого циклу (проектування, розробка, впровадження, оцінка захищеності, експлуатація). Критерії СК поділено на два класи – функціональні критерії (послуги безпеки) (ISO/IEC 15408-2:2008 [4]) та критерії гарантій (ISO/IEC 15408-3:2008 [5]). Відповідно, стандарт застосовується для вирішення, в основному, технічних питань забезпечення безпеки інформації в ІТС.

Оскільки створення КСЗІ базується на поєднані вирішення як організаційних, так і технічних питань, для дослідження можливих шляхів гармонізації проведено порівняння національних та міжнародних стандартів по відношенню до не технічних та технічних аспектів окремо.

Що стосується технічних питань, то зіставлення регуляторів управління інформаційною безпекою, закладених в стандарти ISO/IEC 27001 та 27002 і відповідних організаційних положень нормативної бази України стосовно захисту інформації в ІТС свідчить про таке. Стандарти ISO розглядають ширше коло питань безпеки порівняно з ІТС та не деталізують вимог і порядку проведення робіт стосовно охоплюваних питань. З іншого боку, кожний документ національної бази (за виключенням нормативно-правових актів), як правило, має конкретно визначену направленість та розглядає один або кілька суміжних питань захисту інформації. Відповідно, паралель проведено по відношенню до основних принципів (цілей), закладених у ISO та сукупності відповідних національних нормативних документів.

Національні документи, якими визначений склад КСЗІ, встановлюють також процедуру її оцінювання. Всі аспекти які оцінюються за ISO, повинні бути оцінені і в Україні. Порівняння повноти документів показує, що сукупність національних документів глибше розглядає відповідні питання, особливо стосовно оцінки ІТС. Можливо стверджувати, що переважна більшість основних аспектів управління, передбачених в ISO, є гармонізованими за принципами і підходами з організаційними аспектами побудови КСЗІ.

Питання гармонізації нормативної бази відносно технічного аспекту захисту стосується, в першу чергу, нормативних документів системи ТЗІ (НД ТЗІ). Відповідні документи вищого рівня (зокрема, НД ТЗІ 1.1-002, НД ТЗІ 1.1-003, НД ТЗІ 2.5-004 [6], НД ТЗІ 2.5-005) містять вимоги, які не залежать від особливостей технології обробки інформації, ІТС тощо, і є універсальними. Зазначений комплект НД ТЗІ за принципами і підходами до побудови захисту відповідає міжнародному стандарту ISO/IEC 15408. Принципової різниці немає, за винятком деяких відмінностей. При цьому саме базові національні документи доцільно гармонізувати з цим стандартом з метою встановлення відповідності між вітчизняною системою оцінювання продукції та системами інших країн (що дасть можливість за необхідності користуватися результатами останніх). Можна розглядати два основні шляхи гармонізації – перейти на міжнародну нормативну базу, прийнявши стандарт ISO/IEC 15408, або розробити НД ТЗІ, який би встановлював відповідність між ним та національними критеріями.

Перший шлях вважаємо мало перспективним для розвитку галузі, оскільки на певний час буде втрачено досвід і надбання національної системи оцінювання продукції, набуті за попередні роки. Крім того, просте прийняття міжнародних стандартів неминуче призведе до необхідності здійснювати супроводження двох систем створення й оцінювання продукції, адже діюча на сьогодні система повинна буде працювати до виведення з експлуатації останньої ІТС, яка створювалася у відповідності до НД ТЗІ. З цього приводу достатньо звернутися до негативного досвіду Росії, де на цей час (після введення в дію у 2003 році стандарту ISO 15408) паралельно функціонують дві системи створення й оцінювання продукції і неможливо зробити будь-які оцінки, коли ця паралель закінчиться.

Тому актуальним, на нашу думку, може бути тільки другий шлях. На встановлення відповідності між критеріями НД ТЗІ 2.5-004 та ISO/IEC 15408 направлено науково-дослідну роботу, що виконується з 2012 року на замовлення Адміністрації Держспецзв'язку. Розроблений при цьому пакет НД ТЗІ надасть можливість, використовуючи результати оцінки (сертифікації) засобів захисту інформації, отриманих на основі вимог ISO/IEC 15408, будувати технічні вимоги до них у національних критеріях та проводити державну експертизу засобу на відповідність чинних НД ТЗІ за спрощеною схемою. Отримані таким чином оцінені засоби можуть, відповідно, використовуватися під час побудови КСЗІ. Два основних документи пакету вже розроблено та готуються до затвердження.

Отже, на сьогодні за принципами і підходами українська нормативна база відповідає міжнародним стандартам, що розглядалися, з урахуванням національних особливостей. Це справедливо і з позиції стандарту ISO-9001 стосовно систем управління якістю продукції, і стандартів ISO/IEC 27001, 27002, 15408. Для вирішення питання гармонізації з останнім документом потрібно завершити роботу із зіставлення його вимог з НД ТЗІ 2.5-004. Розвиток національної нормативної бази доцільно спрямувати на створення НД ТЗІ нижчого рівня, які будуть еквівалентними одному з профілів, включених до відповідного розділу ISO.

Сучасна національна нормативна база у сфері ТЗІ не забороняє застосування будь-яких міжнародних стандартів з питань інформаційної безпеки. Що стосується стандарту ISO/IEC 27001 та взаємопов'язаних з ним стандартів, то вони можуть використовуватися в доповнення до діючих норм стосовно інформації, що потребує захисту згідно з законом, та в повному обсязі для будь-якої іншої інформації. Описаний в них набір кращих практик може бути застосований практично для будь-якої організації незалежно від форми власності, виду діяльності, розміру та зовнішніх умов. Їх прийняття в Україні надасть можливість отримати таким організаціям відповідні міжнародні сертифікати на СУІБ для забезпечення демонстрації здатності організацій захищати свої інформаційні ресурси на міжнародному рівні. Відповідну роботу з гармонізації цих та інших стандартів ISO серії 27k передбачено Програмою робіт з національної стандартизації на 2015 рік.

ВИКОРИСТАНІ ДЖЕРЕЛА:

1. ДСТУ ISO 9001:2000. Системи управління якістю. Вимоги. [Електронний ресурс]. – Режим доступу: http://normativ.ucoz.org/load/ dstu_iso_9001_2009/3-1-0-433 .

2. ISO/IEC 27001:2013 Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. [Електронний ресурс]. – Режим доступу: https://www.iso.org/obp/ui/ #iso:std:iso-iec:27001:ed-2:v1:en.

3. ISO/IEC 27002:2013 Информационные технологии. Методы обеспечения безопасности. Свод правил по управлению защитой информации. [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber =54533.

4. ISO/IEC 15408-2:2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 2. Функциональные требования безопасности. [Електронний ресурс]. – Режим доступу: http://www. iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46414

5. ISO/IEC 15408-3:2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 3. Требования к обеспечению защиты. [Електронний ресурс]. – Режим доступу: http://www. iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46413.

6. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. [Електронний ресурс]. - Режим доступу: http:// dstszi.kmu.gov.ua/dstszi/control/uk/publish/article?art_id =89740&cat_id=89734.

Воронов Віктор Романович, *к. т. н., доцент,*
Адміністрація Державної служби спеціального зв'язку та захисту інформації України

ПРОБЛЕМНІ ПИТАННЯ НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ ТА ШЛЯХИ ЇХ ВИРІШЕННЯ

На даний час у державі створена нормативна база системи ТЗІ, яка в цілому забезпечує регулювання технічного захисту інформації. Проте розвиток технічних систем обробки інформації і засобів технічної розвідки (засобів несанкціонованого перехоплення та зняття інформації) обумовлює деякі невідповідності чинного нормативного забезпечення реальним потребам сфери ТЗІ. Є проблемні (невирішені) питання. Зокрема, немає загальносистемного базового нормативно-правового документа: захист інформації на різних об'єктах регулюється різнорівневими за юридичною силою документами (в ІТС – [1], на ОІД – [2]), – деякі питання регулюються старими документами СРСР, наслідками чого є недостатня ефективність державного регулювання у сфері ТЗІ, певна необґрунтованість вимог до захисту інформації, неадекватність таких вимог реальним загрозам інформації, невідповідність витрат на захист інформації досягнутому стану захисту інформації. Необхідне нормативне врегулювання захисту інформації від витоку каналами "ВЧ-нав'язування", акусто-електричними каналами та візуально-оптичними каналами. Необхідно науково-технічне обґрунтування та прийняття методик спеціальних досліджень засобів електронної техніки та телекомунікаційних засобів, а також методик інструментального контролю (інструментальної перевірки) захищеності інформації від витоку каналами побічних електромагнітних випромінювань, в тому числі при використанні активних засобів захисту інформації. Потребують корегування методики інструментального контролю (інструментальної перевірки) захищеності інформації від витоку каналами побічних електромагнітних наведень на лінії електроживлення, заземлення та лінії комунікацій допоміжних технічних засобів та систем. Відсутні сучасні методики інструментального контролю (інструментальних перевірок) захищеності інформації від витоку каналами "ВЧ-нав'язування", акусто-електричними каналами та візуально-оптичними каналами.

На даний момент Адміністрацією Держспецзв'язку послідовно вирішуються згадані вище проблемні питання. Прийняте нове положення, що регламентує категоріювання об'єктів, яке встановлює єдині вимоги та порядок категоріювання об'єктів інформаційної діяльності де обробляється та де озвучується інформація, прийняти нормативні документи стосовно вимог, рекомендацій та методики оцінювання захищеності інформації від витоку лазерними акустичними каналами. Розроблено Положення про захист інформації від витоку технічними каналами на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, де визначено загальні вимоги щодо захисту інформації від витоку технічними каналами, організація захисту інформації від витоку технічними каналами, суб'єкти створення комплексів технічного захисту інформації, функції цих суб'єктів, єдиний підхід та загальний порядок захисту від витоку технічними каналами інформації, яка озвучується на об'єктах інформаційної діяльності та яка обробляється в інформаційно-телекомунікаційних системах, вимоги до робіт зі спеціальних досліджень технічних засобів обробки інформації та перевірки захищеності інформації на об'єктах інформаційної діяльності та на об'єктах електронно-обчислювальної техніки. Підготовлено документ про порядок створення комплексів ТЗІ на об'єктах інформаційної діяльності. Підготовлені та узгоджуються методика спеціальних досліджень технічних засобів обробки інформації та методика інструментального контролю захищеності інформації від витоку каналами побічних електромагнітних випромінювань. Здійснюється узгодження (консолідація) норм та положень чинних нормативних документів, узгодження вимог різних документів, виключення дублювання та протиріч.

Все це буде сприяти забезпеченню захищеності інформації, яка озвучується на об'єктах та обробляється у системах, зменшенню нераціональних витрат на захист інформації від витоку технічними каналами за рахунок підвищення ефективності державного регулювання у сфері технічного захисту інформації.

ЛІТЕРАТУРА:

1 Закон України "Про захист інформації в інформаційно-телекомунікаційних системах".

2 Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 29 вересня 1999 р. № 1229.

Гнатюк Сергій Олександрович, *к.т.н., доцент,*
Національний авіаційний університет

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНА БЕЗПЕКА ДЕРЖАВИ В УМОВАХ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ

Відповідно до чинного законодавства України *інформаційна безпека* визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. Традиційно, під *забезпеченням інформаційної безпеки* прийнято розуміти застосування комплексу заходів для створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів, протидії комп'ютерній злочинності (кіберзлочинності), захисту персональних даних, розвитку Національної системи конфіденційного зв'язку тощо. Саме ці заходи визначаються пріоритетними для вирішення проблеми інформаційної безпеки відповідно до Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». Проте більшість заходів носять більш технічний характер, не зважаючи на те, що негативний інформаційний вплив може бути спрямований не лише на технічну інфраструктуру інформаційних та комунікаційних систем. Іншими словами, *інформаційний вплив* – це організоване цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення змін у свідомість особи чи населення (корекція поведінки) та (або) інформаційно-технічну інфраструктуру об'єкта та (або) фізичний стан людини.

Останні події у нашій державі, зокрема втягнення її у відкриту *інформаційну війну* (комплекс заходів щодо досягнення інформаційної переваги шляхом впливу на інформацію, інформаційні процеси, інформаційні системи та комп'ютерні мережі противника при одночасному захисті своєї інформації, інформаційних процесів, інформаційних систем і комп'ютерних мереж – Статут Сухопутних військ США FM 100-6), змусили говорити про інформаційно-психологічну складову інформаційної безпеки держави. *Метою цієї роботи* є висвітлення основних понять інформаційно-психологічної безпеки держави в умовах ведення інформаційної війни. З огляду на зазначене, інформаційний вплив варто поділяти на інформаційно-технічний та інформаційно-психологічний. *Інформаційно-технічний вплив* – це вплив на інформаційно-технічну інфраструктуру об'єкта з метою забезпечення реалізації необхідних змін у її функціонуванні (зупинка роботи, несанкціонований доступ до інформації та її перекручення (спотворення), програмування на певні помилки, зниження швидкості оброблення інформації тощо), а також вплив на фізичний стан людини. Інформаційно-технічний вплив становить загрозу безпеці інформаційно-технічної інфраструктури й фізичному стану людини. *Інформаційно-психологічний вплив* – це вплив на свідомість та підсвідомість особистості й населення з метою внесення змін у їхню поведінку

і світогляд. Базовими методами інформаційно-психологічного впливу є *переконання* (цілеспрямований і свідомо організований вербальний вплив на конкретну масову аудиторію, що апелює до раціональної сфери свідомості особистості й здійснюється з метою формування певних установок, закріплення або зміни раніше засвоєних установок, а, в кінцевому рахунку, зміни поведінки індивіда відповідно до визначених цілей) й *навіювання* або *сугестія* (спрямовується на суб'єкти, які некритично сприймають інформацію і являє собою процес впливу на психіку людини, пов'язаний зі зниженням свідомості й критичності при сприйнятті навіяного змісту, який не вимагає ні розгорнутого особистого аналізу, ні оцінки спонукання до певних дій).

Засобами ведення інформаційної війни є *інформаційна зброя* (комплекс програмних і технічних засобів, призначених для контролю інформаційних ресурсів об'єкта впливу та втручання в роботу його інформаційних систем). За методами впливу інформаційну зброю можна поділити на *фізичну* (протирадіолокаційні ракети, спеціалізовані акумуляторні батареї генерування імпульсів високої напруги, засоби генерування електромагнітного імпульсу, графітові бомби, біологічні й хімічні засоби впливу на елементну базу тощо), *інформаційну* (засоби масової інформації та глобальних інформаційних мереж, зокрема медіа-віруси, нейролінгвістичне програмування, Інтернет-пропаганда, медіа-маніпулювання, а також станції голосової дезінформації та ін.), *програмно-технічну* (комп'ютерні віруси, сніфери, трояни, логічні бомби та апаратні закладки, а також спеціальні засоби проникнення в інформаційні мережі) та *радіоелектронну* (засоби радіоелектронного придушення, радіоелектронної розвідки тощо).

Таким чином, *інформаційно-психологічну безпеку держави* в умовах ведення інформаційної війни можна визначити як стан захищеності інтересів держави, за якого досягається її нормальне функціонування та гармонійний розвиток незалежно від дії негативних інформаційно-психологічних впливів противника.

Список використаних джерел

1. Історія інформаційно-психологічного протиборства : підруч. / [Я.М. Жарков, Л.Ф. Компанцева, В.В. Остроухов В.М. Петрик, М.М. Присяжнюк, Є.Д. Скулиш] ; за заг. ред. Є.Д. Скулиша. – К. : Наук.-вид. відділ НА СБ України, 2012. – 212 с.

2. Сугестивні технології маніпулятивного впливу : навч. посіб. / [В.М. Петрик, М.М. Присяжнюк, Л.Ф. Компанцева, Є.Д. Скулиш, О.Д. Бойко, В.В. Остроухов]; за заг. ред. Є.Д. Скулиша. – 2-ге вид. – К. : ЗАТ "ВІПОЛ", 2011. – 248 с.

3. Жарков Я.М. Небезпеки особистості в інформаційному просторі [Електронний ресурс]. – Режим доступу: http://www.justinian.com.ua/article.php?id=2554 (12.05.2015)

4. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» // Відомості Верховної Ради України (ВВР). – 2007. – № 12.

Вільський Г.Б., *PhD, професор, ректор,*
ВНЗ «Міжнародний технологічний університет «Миколаївська політехніка»

ІНФОРМАЦІЙНА БЕЗПЕКА І РИЗИКИ СУБСТАНДАРТНОГО СУДНОПЛАВСТВА

Наявність серйозних недоліків в суднових конструкціях, устаткуванні, рятувальних та протипожежних засобах субстандартних морських суден (СМС), кваліфікації членів екіпажу призводять до зниження рівня і інформаційної безпеки. Таке становище в судноплавстві, яке представляє вагому складову держави, додає значне погіршення

національної безпеки [1 – 3]. Дослідженню питань та процесів з забезпечення інформаційної безпеки в субстандартному судноплавстві (ССС) передує виконання наступних умов [4]:

1. Проведення аналізу статистичних даних аварійності СМС для ідентифікації загроз і ризиків з офіційних матеріалів розслідування морських інцидентів за встановлений інтервал часу та визначення кількісних показників імовірнісного розподілу чинників небезпек на маршруті судна.
2. Виконання розрахунків прогнозу динаміки зміни факторів небезпек з відображенням ризиків шляхом побудови математичних моделей інтегруючих процесів, які відбуваються в кластері інформаційної безпеки ССС, дослідження яких дозволяє гарантувати реальність оцінки обстановки на маршруті судна.
3. Одержання графічної щільності імовірності можливих аварійних подій, побудованих поверхонь залежності ризиків від загроз інформаційної безпеки та показника "еластичності", що характеризує залежність просідання судна від його розмірів та імовірності аварій. Це забезпечує порівнянність отриманих результатів при прийнятті рішень з безпечного руху суден.

Встановлення розрахунково-імовірнісних моделей та діаграм інформаційної безпеки руху судна для районів з зонами підвищеної небезпеки, зі створенням відповідних паспортів, дозволяє стверджувати про доцільність наведеного переліку умов забезпечення процесів інформаційної безпеки ССС.

1. Вильский Г. Б. Информационная безопасность судовождения [Текст] : монография. – Николаев : Швец В. Д., 2014. – 336 с.
2. Егоров Г. В. Исследование риска аварий корпусов транспортных судов ограниченных районов плавания за 1991–2010 годы [Текст] / Г. В. Егоров // Вісник ОНМУ. – 2010. – Вип. 30. – С. 53–76.
3. Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013. – Second edition 2013-10-01. – Geneva, 2013. – P. 23.
4. Вильский Г. Б. Управление рисками информационной безопасности судовождения [Текст] / Г. Б. Вильский // IV Міжнар. наук.-техн. конф. «ITSEC», 20–23 травня 2014, м. Київ, Україна / НАУ. – К., 2014. – С. 15–17.

Пядишев Володимир Георгійович, *к. т. н., доцент,*
Сіфоров Олександр Іванович, *к. т. н., доцент,*
Одеський державний університет внутрішніх справ

ПРО НЕОБХІДНІСТЬ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В ЗОНАХ МІЖНАРОДНИХ ОПЕРАЦІЙ З ПІДТРИМАННЯ МИРУ І БЕЗПЕКИ

В умовах відсутності добре навчених, оснащених надійних правоохоронних органів у зонах міжнародних операцій з підтримання миру і безпеки (МОПМБ), тобто на теренах після збройних конфліктів, досягають небувалого розмаху найприбутковіші види злочинів: торгівля зброєю, наркотиками, дорогоцінними місцевими копалинами, людьми, людськими органами. Зміцнілі в погано контрольованих правоохоронними органами зонах збройних конфліктів у колишній Югославській республіці Македонії та Косово албанські злочинні угруповання потіснили італійську мафію в Італії та відомих своєю жорстокістю ямайських сутенерів у Великобританії. Список можна продовжити.

Але в наш час увагу світової спільноти притягує кіберзлочинність [1], яка, з одного боку — багаторазово перевищує прибутковість інших видів організованих злочинів, з іншого боку — відрізняється високим ступенем латентності (з багатьох причин). При цьому в

наявній науковій літературі та звітах важко знайти поруч ключові вирази: “кібер-злочини” та “МОПМБ”. Це пов'язано з тим, що, на перший погляд, важко уявити єдність високих технологій і злиднів зруйнованої конфліктом країни. Разом з тим, за чисельних даними, найбільш потужний потік кібер-атак на провідні банки США і Західної Європи спостерігається з Африки, зокрема, з найбідніших регіонів. Спостерігаються кібер-атаки з інших зон збройних конфліктів [2]. Це може бути викликано наступними причинами. По-перше, розмістити сучасний злочинний кібер-центр “далеко від цивілізації” сьогодні немає особливих проблем у зв'язку з його малогабаритністю і з використанням супутникових телекомунікацій. По-друге, при виявленні злочинного кібер-центру, злочинців простіше затримати в умовах розвинутої правоохоронної інфраструктури сучасних міст, ніж в зонах МОПМБ, де місцева поліція або відсутня, або не має відповідної підготовки, погано оснащена і схильна до корупції, крім того, озброєні маси населення, підгодовані організованою злочинністю, можуть дати потужний відсіч. По-третє, немає даних про підбір й підготовку службовців для поліції МОПМБ за напрямами боротьби з кібер-злочинністю, в той час, як ведеться підготовка по боротьбі з порушенням прав людини, з гендерними злочинами, з насильством в сім'ї, з торгівлею людьми та іншими, безумовно важливими, аспектами злочинності.

Оскільки багаторазово підтверджено, що організована злочинність ніколи не втрачає свої шанси, нам представляється необхідним розвивати підготовку (підбір і навчання) службовців поліції МОПМБ в напрямку боротьби з кібер-злочинами. З одного боку йдеться про підготовку безпосередньо міжнародного складу поліції. З іншого — про вдосконалення навчальних програм у напрямку боротьби з кібер-злочинністю для місцевих поліцейських академій, які створюються і керуються поліцейськими силами МОПМБ.

Література:

1. Convention on Cybercrime, Budapest, 23 November 2001.

2. Ogundeji O.A. Cyberattacks in West Africa spark debate over online security [Electronic source] / Olusegun Abolaji Ogundeji // PC Wold. Feb 12, 2015 – Access Mode : http://www.pcworld.com/article/2883932/cyberattacks-in-west-africa-spark-debate-over-online-security.html.

Майданюк Павло Володимирович, *гол. інсп. по захисту праці,*
Управління Державної служби спеціального зв’язку
та захисту інформації в Миколаївській області

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ ДЕРЖАВНИХ ОРГАНІВ

Життя сучасного суспільства неможливе без постійного застосування інформаційних технологій. Збільшення рівня автоматизації обробки інформації ставить суспільство в залежність від ступеня захищеності інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, в яких ця інформація обробляється.

На сьогоднішній день державні органи, підприємства, установи та організації України здійснюють переведення інформаційних ресурсів в електронну форму з метою її систематизації, легкості доступу та передачі каналами зв’язку, одночасно з цим все більш актуальною стає проблема забезпечення захисту інформації від загроз витоку, знищення, блокування, порушення цілісності та режиму до її доступу.

Однією з основних проблем захисту інформації в інформаційно-телекомунікаційних системах (далі – ІТС) є недостатня координованість дії у сфері технічного захисту інформації (далі – ТЗІ) з боку вищих органів влади. На сьогодні відсутність системності та обґрунтованості управлінських рішень призводить до розбалансованості, внутрішньої суперечливості та непослідовності впровадження заходів із захисту інформації.

Також слід зазначити, що до сих пір в законодавстві України відсутнє визначення технічного захисту інформації, як одного з основних напрямів діяльності органів державної влади, та відсутня гармонізація нормативно-правового забезпечення України із міжнародними стандартами у сфері ТЗІ.

Існує ще ряд факторів, які обумовлюють необхідність подальшого удосконалення розвитку та поліпшення захисту державних інформаційних ресурсів, до яких можна віднести:

- відсутність кваліфікованих кадрів з технічного захисту інформації;
- відсутність у більшості державних органів штатних посад (підрозділів) з технічного захисту інформації;
- відсутність належного фінансування на проведення робіт із захисту інформації в ІТС;
- відсутність затвердженої процедури створення комплексних систем захисту інформації в складних ІТС;
- відсутність розуміння деякими керівниками державних органів важливості захисту інформації в інформаційних системах;
- наявність певних дублювань і неоднозначностей, які існують в нормативно-правових документах системи ТЗІ та системи захисту інформації в цілому;
- відповідальність за порушення законодавства про захист інформації в ІТС недостатньо класифікована та визначена.

Отже, на мій погляд, першочерговими заходами з розв’язання проблем захисту держав них інформаційних ресурсів в ІТС є:

- розробка обґрунтованої концепції ТЗІ України з урахуванням перспектив розвитку інформаційних технологій;
- гармонізація стандартів у сфері ТЗІ із міжнародними, з урахуванням того, що більшість міжнародних стандартів носить рекомендаційний характер;
- урегулювання питання щодо отримання якісної підготовки кадрів у сфері ТЗІ, з подальшим їх працевлаштуванням на посади, що безпосередньо зв’язані із захистом інформації;
- розробка та затвердження на державному рівні процедури створення систем захисту інформації в інформаційно-телекомунікаційних системах;
- інтеграція захисту інформації в процес створення та розвитку інформаційних систем як обов'язковий елемент.

Висновок.

Система захисту інформації в ІТС потребує постійного удосконалення з урахуванням розвитку телекомунікаційних мереж та досвіду європейських країн, тому що державні інформаційні ресурси перетворились на стратегічний ресурс економічного й науково-технологічного прогресу, життєдіяльності та розвитку держави. Захист державних інформаційних ресурсів в інформаційно-телекомунікаційних системах є одним із першочергових завдань національної безпеки.

Рябий Мирослав Олександрович, *к.т.н.,*
Гнатюк Іван Юрійович, *викладач,*
Європейський університет

ЗАСТОСУВАННЯ МЕТОДІВ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ ДЛЯ ЗДОБУТТЯ КОНКУРЕНТНИХ ПЕРЕВАГ НА РИНКУ

Сьогодні процес інформатизації суспільства, його державних та суспільних інститутів, розвивається стрімко і як правило непередбачено і некеровано [1, 2]. Суспільство, на наш погляд, з великим запізненням починає осмислювати політичні, економічні,

соціальні, військові, психологічні та інші наслідки. Широке використання в процесі інформатизації сучасної техніки уже сьогодні дозволило створити в технологічно розвинутих державах світовий інформаційний простір, в якому створюється, накопичується, розподіляється, передається, приймається, перетворюється та знищується інформація.

Сучасні військові конфлікти не обходяться без використання інформаційно-психологічних операцій. Їхньому деструктивному впливу може бути піддана будь-яка особистість, соціальна група, суспільство. Зважаючи на те, що інформаційне протистояння є невід'ємною частиною сучасних політичних відносин, як на глобальному рівні, так і на регіональному, проблема дослідження їх природи постає важливим фактором розуміння процесів суспільного розвитку.

Витоки застосування інформації в якості зброї згадуються у біблійній легенді згадано Гедеона, який під час воєн регулярно вдавався до залякування ворога. Одного разу він так залякав супротивника, що той розгубився і вдарив по своїх військах. Видатними майстрами техніки впливу на маси були римляни, зокрема Юлій Цезар. Всякий раз перед військовими битвами він домагався народної підтримки за допомогою поширення спеціально підібраних звернень та проведення театралізованих вистав. В епоху феодалізму яскравим прикладом інформаційного тиску є боротьба з «єрессю», за «істинну віру» і т.д. Сучасні дослідники знаходять характерні риси психологічних війн у наполеонівській пропаганді: настійливі твердження про єдність у власному таборі й розлади у противника; замовчування несприятливих відомостей і висвітлення вигідних; висунення легкодоступних гасел; фальсифікація історичних фактів; постійне повторення вигідних тем; викривлення повідомлень преси противника; спроби висміювання ворогів, звинувачуваних у своїх власних злочинах. Саме Наполеону належить твердження, що «чотири газети можуть заподіяти ворогу більше зла, ніж стотисячна армія».

Особливого значення інформаційні війни набули у XX столітті, коли газети, радіо, а потім і телебачення стали справді засобами масової інформації, а поширювана через них інформація - справді масовою. Уже у 20-х роках США транслювали радіопередачі на регіони своїх «традиційних інтересів» - країни Латинської Америки, Великобританія - на свої колонії. Німеччина, яка домагалася перегляду умов Версальського миру - на німців Померанії і Верхньої Сілезії у Польщі, судетів - у Чехії. Тоді ж, у 30-х роках, інформаційні війни перестають бути додатком до збройних і перетворюються у самостійне явище - як то німецько-австрійська радіовійна 1933-1934 рр. з приводу приєднання Австрії до рейху. Саме тоді з'явилося і набуло поширення поняття «інформаційний агрессор».

Отож, все сказане переконує, що мистецтвом воювати за допомогою інформації людство оволодівало тривалий час, послідовно та наполегливо. Чи то цілком усвідомлено, чи то послуговуючись інтуїцією, можновладці ніколи не нехтували можливістю змінювати свідомість мас і завойовувати їх саме таким чином.

Деякі вчені вважають, що вперше поняття «інформаційна війна» було введене в 1985 році в Китаї. В основу теоретичних підходів китайських фахівців у галузі інформаційного протиборства покладені погляди давньокитайського військового діяча Сунь Цзи (V ст. до н. е.). Він першим аргументував необхідність інформаційного впливу на супротивника. В своєму «Трактаті про військове мистецтво» Сунь Цзи відмічав: «У всякій війні, як правило, найкраща політика зводиться до захоплення держави цілісною... Здобути сотню перемог у боях - це не край мистецтва. Підкорити суперника без бою - ось вінець мистецтва».

Найпотужнішим знаряддям впливу, який винайшли в Стародавньому Китаї і яким користуються досі в політиці, військовій справі і бізнесі є стратагеми. Під стратагемою розуміють стратегічний план, який передбачає використання хитрощів з метою заманити супротивника в пастку. Їх авторство приписується саме Сунь Цзи. В згаданому трактаті Сунь Цзи стверджував, що війна – це шлях брехні, а тому:

- Якщо ти можеш щось, переконай противника, що не можеш;
- Хоч ти і близько – показуй, що ти далеко;
- Заманюй супротивника вигодою;

- Зруйнуй душевну рівновагу і бери його;
- Якщо ворог сильний, ухиляйся від нього;
- Якщо сили ворога свіжі, стоми його;
- Якщо в таборі супротивника злагода, посій розбрат;
- Нападай на ворога, коли він не чекає [3].

Існує й інша думка серед вчених, згідно з якою вперше термін «психологічна війна» в 1920 р. застосував британський історик Дж. Фуллер, котрий аналізував першу світову війну. Цей термін взяли на озброєння американці. Вони датують власне використання цього терміна 1940 роком. Відповідний англійський варіант цього терміна – «політична війна». Термін «психологічні операції» вперше в документі застосував капітан Е. Захаріас. Саме цей термін почали з 1957 р. використовувати в американських офіційних документах, адже він дав змогу застосувати відповідний інструментарій в ситуації відсутності широкомасштабних військових операцій. Тобто цей інструментарій можна застосовувати не лише до ворогів, а й до нейтральних країн чи навіть союзників.

У інформаційному протиборстві застосовуються численні способи і форми (технології) тиску. Серед них: шахрайство, блеф, стратагеми, політичні ігри і містифікації, маніпулятивні дії, провокації, психологічні і таємні операції, пропаганда, політичні ігри і рекламні кампанії, дезінформація, чутки і оперативні ігри – це далеко не повний перелік понять, використовуваних для позначення способів таємного примусу людини.

Приклади інформаційного впливу на широку аудиторію у великій кількості можна прослідковувати протягом усієї історії суспільства в різних , та в якості одного з основних видів протистояння, воно постає у XX ст. разом зі зміцненням засобів масової комунікації, їхнім розширенням та урізноманітненням. Проте, інформаційне протистояння є прерогативою не тільки військових дій, вони сьогодні є невід’ємною частиною конкуренції в бізнес-середовищі.

Якщо говорити про ринкову економіку, то це — економіка, організована на основі ринкової саморегуляції, при якій координація дій учасників здійснюється державою, а саме законодавчої та судової владою безпосередньо, а виконавчої тільки опосередковано, шляхом запровадження різних податків, зборів, пільг тощо. Це економіка, в якій тільки рішення самих покупців, постачальників товарів і послуг визначають структуру розподілу. Вона заснована на наступних принципах:

- підприємництва;
- різноманіття форм власності на засоби виробництва;
- ринкове ціноутворення;
- договірних відносин між господарюючими суб'єктами (людьми, підприємствами і т. д.);
- обмеженого втручання держави в господарську діяльність.

Одним з досягнень ринкової економіки прийнято називати рівність, рівні можливості, хоча насправді можливості визначає соціальний стан. Виходячи з вище сказаного та аналізу медійних потоків виробників товарів та послуг простежується перенесення методів ведення інформаційних війн на ринок товарів та послуг.

До методів інформаційних війн, що використовуються на рику можна віднести: використання авторитетів (груп впливу; стверджуючі заяви; використання ціннісних слів (що відносяться до основних цінностей суспільства); невизначені вирази (позитивно забарвлені); перенесення позитивного образу; невизначені вирази і натяки, що несуть негативне забарвлення; перенесення несхвалення і негативного образу; наклеювання ярликів; використання лякаючих тем і повідомлень; загострення уваги; пряме спростування; відволікаюча пропаганда; зменшення значущості теми; обмежувальні заходи; псевдологічні висновки; порушення логічних і часових зв'язків між подіями; заміна джерела повідомлення; зменшення значущості теми; вибірковий добір інформації. Не дивлячись на те, що за використання методів інформаційної війни в ринку, законодавством всіх країн передбачена

відповідальність, рекламні компанії в тій чи іншій мірі продовжують використовувати методи ведення інформаційних війн.

Проблема інформаційної війни не вивчена не до кінця. Незважаючи на високий ступінь соціальної небезпеки засобів її впливу, використовуваних у сучасній інформаційній боротьбі, багато наукових завданнь ще не вирішені. Тому необхідно більш докладне вивчення даного феномена з метою зниження ступеня соціальної так і економічної небезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Черешкин Д. С., Смолян Г. Л., Цыгичко В. Н. Реалии информационной войны. – Конфидент, 1996, № 4, с. 9-12.

2. Кузнецов П. А. Информационная война и бизнес. – Конфидент, 1996, № 4, с. 21-24.

3. Жарков Я. М., Петрик В. М., Присяжнюк М. М. Історія інформаційно-психологічного протиборства. Підручник за заг.ред. Є. Д. Скулиша, - Київ Науково-видавничий відділ Національної академії СБ України, 2012.

Левківський Казимир Михайлович, *к. іст. н., професор, в.о. директора,*
Івлєва Людмила Миколаївна, *нач.відділу,*
Інститут інноваційних технологій і змісту освіти МОН України

ЯКІСНА ОСВІТА – ЗАПОРУКА РОЗВИТКУ ЕКОНОМІЧНИХ І СОЦІАЛЬНИХ НОВАЦІЙ

Освіта в сучасних умовах є могутнім чинником розвитку духовної культури українського народу, відтворення інтелектуальних і продуктивних сил суспільства, запорукою громадянського миру і майбутніх успіхів у зміцненні й утвердженні авторитету України як суверенної, незалежної, демократичної, соціальної та правової держави – повноправного члена європейської та світової спільноти. Освіта і майбутнє – два ключові аспекти, із позицій яких слід розглядати стан справ, що склався в галузі та визначати її перспективи.

Обравши шлях у Європу, ми сьогодні маємо надзвичайно важливе завдання - це підготовка нашого суспільства, як конкурентноздатного.

І зробити це можливо лише шляхом піднесення якості освіти. Починаючи від кваліфікованого робітника, молодшого спеціаліста, молодшого бакалавра, бакалавра, закінчуючи магістром та доктором філософії - якість освіти на всіх цих щаблях проектує якість нашої економіки і якість нашого суспільства.

Питання забезпечення якості вищої освіти є одним з ключових європейської інтеграції української держави.

У показниках Глобального індексу конкурентоспроможності за період з 2010 до 2012 року зниження показників якості вищої освіти корелює зі зниженням інноваційної спроможності країни. З огляду на критичний стан вищої освіти в Україні, можна констатувати, що комплексне оновлення освітньої нормативно-правової бази та нещодавно прийнятий Закон України «Про вищу освіту» є чи не єдиною можливістю виходу вищої освіти із кризового стану і перетворення її на дієвий інструмент динамічного реагування на запити суспільства та економіки, забезпечення її конкурентоспроможності на європейському ринку освітніх послуг.

Зокрема, Закон України «Про вищу освіту» є документом стратегічного значення. Він визначає загальну філософію освіти, пріоритети і принципи, основні напрями і механізми розвитку на найближчі роки. Принциповими в ньому є положення про необхідність забезпечення рівного доступу до якісної освіти, утвердження новітніх інформаційних педагогічних технологій, мовних стратегій освіти.

Українська освіта має стати орієнтованою на особистість, демократичною, конкурентноздатною у світовому та освітньому просторі. Базуючись на національній ідеї українського державотворення вона спрямована на утвердження національних інтересів, має здійснюватись упродовж життя, відповідати потребам особистості та суспільства, які постійно змінюються.

Цей Закон впроваджується у три етапи. Перший етап - це етап напрацювання підзаконних актів (наказів, постанов, розпоряджень), етап вироблення тих документів, без яких не можна рухатися далі, починаючи вже від освітніх стандартів.

З першого вересня 2015 року запрацює Національне агентство з якості вищої освіти. Також, з цього часу відбудеться перехід на максимальне навантаження на викладачів - з 900 до 600 годин у рік. А кількість годин в кредиті має бути не 36, а 30. Це означає, що мають бути зміни в розподілі часу на навчальні курси відповідно до нових освітніх стандартів. Крім того, студентам надається можливість вибору - до 25% курсів. Це також важливо, адже посилює конкуренцію між викладачами.

Третій етап почнеться з 1 січня 2016 року. З цього часу мають вступити в дію статті, які потребують додаткового фінансування.

Крок за кроком ми досягаємо того, що хочемо змінити, а це — фінансова, академічна, організаційна автономія університетів. Ми йдемо шляхом дерегуляції та децентралізації.

На порядку денному Міністерства освіти і науки - Закон «Про наукову та науково-технічну діяльність», де будуть передбачені зміни в організації наукових досліджень. Передусім необхідно інтегрувати науку і вищу освіту. Головний критерій якості освіти — це наукові дослідження.

Закон України «Про вищу освіту» визначив головний напрям перетворень, має значний потенціал, разом з тим, потребує активної підтримки та пильності керівників освітянської галузі і суспільства.

Мельник Сергій Вікторович, *к.е.н., доцент,*
директор Державної установи НДІ соціально-трудових відносин Мінсоцполітики України, м. Київ

РЕФОРМУВАННЯ ПРОФЕСІЙНИХ ТА ОСВІТНЬО-КВАЛІФІКАЦІЙНИХ СТАНДАРТИЗОВАНИХ СИСТЕМ УКРАЇНИ: ЗИСКИ ТА РИЗИКИ

За останні 10 місяців в Україні на теренах сфери підготовки кадрів відбуваються суттєві зміни, перш за все, шляхом закріплення нових іноваційних підходів законодавчо-нормативними актами. Серед них виділимо:

- Закон України „Про вищу освіту”, який, окрім іншого, відходить від регулювання (як правило) професійних кваліфікацій. У подальшому, навчальні заклади вищої освіти визнаватимуть виключно загальні (далі-академічні) кваліфікації (бакалавр (інженерна механіка), магістр (соціологія), а професійні кваліфікації – визнаватимуться через новоутворені кваліфікаційні центри, практика діяльності яких за єдиними принципами в Україні відсутня;
- відмова від галузевих стандартів вищої освіти (ОКХ, ОПП, варіативна частина, засоби оцінювання) та запровадження стандартів освіти та стандартів освітньої діяльності, які як і більшість інновацій Закону, будуть формуватися та регулюватися Національним агенством з оцінювання якості вищої освіти, які за станом на сьогоднішній день, окрім „розподілу портфелів та повноважень” не оформлюються інституційно, втрачає до свого „відкриття” (01.10.2015) статус незалежного;
- автономізація ВНЗів щодо підготовки за спеціалізаціями, в т.ч. стосовно підготовки за професійно-орієнтованими програмами. Існує велика ймовірність розширення

„кваліфікаційного безладу та хаосу” до безкінечності через відсутність практики зовнішнього оцінювання та наявності на ринку освітніх послуг „ринку дипломів”, а на ринку праці - „ринку професій”, але не „ринку професійних кваліфікацій”;

- прийняття Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти (Постанова КМУ від 29.04.2015 р. за № 266). Це подія, з одного боку, наближає підготовку до норм Міжнародного стандарту освіти (МСКО – 2011, 2012), укрупнює в 5 разів кількість спеціальностей, а з іншого – ставить ВНЗи у скрутне становище через відрив документу від „регульованих” професійних кваліфікацій, які визначатимуться державою та зацікавленими сторонами під час формування державного замовлення на підготовку кадрів;
- запровадження в Україні системи видавання ваучерів незайнятому населенню у віці, старше 45 років для навчання за визначеними Урядом (тепер Мінсоцполітики України) робітничими професіями та спеціальностями, започаткування процесу визнання результатів неформальної освіти (Постанова КМУ „Про затвердження переліку підтвердження результатів неформальної освіти громадян за робітничими професіями” (від 15.05.2015, № 340).

Слід зазначити, що ці та багато інших підходів щодо оновлення законодавчо-нормативного забезпечення сфери підготовки кадрів мають багато нарікань та застережень, у т. ч. від міжнародної спільноти, насамперед, стосовно:

- несистемності у трактуванні норм та положень, кулуарності в прийнятті рішень, норм, перш за все, з боку МОН України;
- відсутності підготовчої роботи стосовно створення механізмів запровадження на практиці законодавчо задекларованих інновацій;
- украй слабка роз’яснювально-інформаційна та консультаційно-інформаційна робота із зацікавленими сторонами, відсутність мережі з підготовки розробників нормативної бази відповідного спрямування, стандартів освіти, освітньої діяльності, професійних стандартів нового типу, оцінювачів професійних кваліфікацій;
- намагання максимального запозичення зарубіжно-міжнародних підходів без урахування вітчизняних надбань, традицій та специфіки;
- відірваності більшості освітніх інновацій від реалій, що формуються в суспільстві, економіці, на ринку праці та на виробництві;
- розбалансованість терміно – понятійного апарату сфери підготовки кадрів, незрозумілість більшості запозичених термінів пересічних користувачів (молодший бакалавр, інформальне навчання, неформальна освіта, ваучер, регульовані професії, тощо):
- закритість закладів вищої освіти, „буксування” у реалізації державної політики використання трудового потенціалу з боку Мінсоцполіитики, різновекторність діяльності відповідного спрямування серед соціальних партнерів національного рівня.

Сухарніков Юрій Васильович, *к. т. н ., доцент, нач. відділу,*
Інститут інноваційних технологій і змісту освіти МОН України

ОБРАЗОВАТЕЛЬНОЕ ЗАКОНОДАТЕЛЬСТВО УКРАИНЫ в контексте глобализационного процесса

Верховна Рада 28 червня 1996 року приняла новую Конституцию Украины, которая должна была привести в соответствие изменения в организации государства и общества и наладить качественно новую систему права в Украине. Новая статья 53 Конституции Украины должна дать импульс развитию системы образования с учётом мировых тенденций развития образовательного законодательства, т.е. приобрести *интеграционный* характер,

формировать европейский менталитет общества и личную ответственность учащейся молодежи, как **субъекта образовательных отношений.** Следует учитывать статью 9 Конституции Украины, в которой признается приоритет международных договоров и принципов международного права перед национальным законодательством.

– Нужно также подчеркнуть, что из статьи 53 изъята норма «*…на основі зв'язку навчання з життям, з виробництвом*». Это концептуальное, очень важное действие, потому что оно послужило причиной значительных неурядиц в современном высшем образовании Украины. Эта примитивная «операция» Верховной Рады 1996 года перерезала «пуповину», которая де-юре связывала в советские времена сферу образования и рынок труда. Государственная политика в сфере образования должна быть ориентирована на формирование человеческого потенциала общества и содействие реализации прав граждан на полную, продуктивную и свободно избранную занятость. В статье 15 Закона Украины «Про зайнятість населення» от 05.07.2012 г. № 5067-VI (редакция от 27.03.2015 р.) [1] наведено принципи государственной политики занятости населения.

Закон Украины «Про вищу освіту» от 01.07.2014 г. не согласуется с законом «Про зайнятість населення», изолирует систему высшего образования от рынка труда и формирует её, по сути, как организационно-управленческую «вещь в себе», а не систему "для нас", т.е. призванную выражать интересы гражданского общества, главной ценностью которого является человек.

В Меморандуме об учении в течение всей жизни [2] подчёркивается тот факт, что "… люди являются главным достоянием Европы и должны быть в центре политики Союза". Из этого делается вывод, что системы образования и профессиональной подготовки должны адаптироваться к новым реалиям XXI столетия и что "Учение в течение всей жизни (LifeLong Learning) – необходимая политика для развития гражданства, социальной сплочённости и занятости".

В этом смысле важно вспомнить рекомендации Комитета министров Совета Европы от 16 мая 2007 г. относительно вопроса «какое образование нам нужно?». Высшее образование должно учитывать и сбалансировать четыре основных цели, выявленные в процессе работы Совета Европы по общественной ответственности за высшее образование и научные исследования – «…все они являются основными[3]: подготовка к рынку труда; подготовка к жизни активных граждан демократического общества; личностное развитие; формирование и поддержка путем преподавания, учения и исследований, всеобъемлющей и разнообразной базы знаний».

В этом контексте, сотрудничая с ЕС в области высшего образования Украина должна провести работу в сфере образовательного законодательства «…с целью: «перестройки» и «осовременивания» систем высшего образования; содействия сближению в сфере высшего образования. повышение качества и релевантности высшего образования …».

Терминологическая релевантность определит:

a) траекторию «перестройки» и «осовременивания» системы образования и профессиональной подготовки Украины на многие годы в будущем;

b) будут ли признаваться результаты деятельности системы образования и профессиональной подготовки Украины на рынке труда (т.е. влияние на судьбы будущих выпускников);

---

[1] ЗАКОН УКРАЇНИ «Про зайнятість населення» від 05.07.2012 № **5067-VI**
URL: http://zakon0.rada.gov.ua/laws/show/5067-17

[2] **A Memorandum on Lifelong Learning:** COMMISSION STAFF WORKING PAPER, Brussels, 30.10.2000 SEC (2000) 1832. – URL: http://www.eaea.org/doc/MemoEN.doc

[3] Recommendation CM/Rec (2007) 6 of the Committee of Ministers to member states on the public responsibility for higher education and research (Adopted by the Committee of Ministers on 16 May 2007 at the 995th meeting of the Ministers' Deputies) [El. resource] / Council of Europe. — URL: https://wcd.coe.int/ViewDoc.jsp?Ref=CM/Rec(2007)6&Sector=secCM&Language=lanEnglish&Ver=original&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75#RelatedDocuments.

c) удастся ли сертифицировать Национальную Рамку Квалификаций Украины и обеспечить признание результатов деятельности системы образования и профессиональной

d) подготовки Украины за рубежом.

Терминологическая релевантность обусловливает методологический «шлейф» перестройки и осовременивания, потому что за каждым термином, который вводится должны стоять (опосредованно) нормативно-правовые документы.

В частности, **Высшая школа** (в Законе Украины «Про вищу освіту» от 01.07.2014 г., редакция от 01.05.2015 г.) рассматривается как организационно-управленческая система, «***принципы функционирования***» которой *устанавливает* Закон. В этом контексте понятие Высшая школа определяется как «вещь в себе», а это означает, что высшее учебное заведение де-юре имеет право: 1) разрабатывать образовательную программу (на основе «*переліку навчальних дисциплін»)*; 2) организовывать учебный процесс; 3) назначать аттестационный орган; 4) проводить аттестацию; 5) присуждать степень и квалификацию – т.е. оно является «изолированной системой», которая де-факто не несет ответственности за результаты своей деятельности с точки зрения пригодности выпускника к трудоустройству (в Законе этот термин даже не упоминается) и, как следствие, с точки зрения «**реалізації політики держави у сфері зайнятості населення**».

Определение понятия «профессиональная подготовка» в качестве ключа к разрешению вопроса о соотношении рассматриваемых понятий было дано в прецедентном праве Сообщества. Этой проблеме посвящено несколько решений Европейского суда юстиции. Основным из них является Решение суда от 13 февраля 1985 года – **Франсуаза Гравье** (Gravier) **против города Льеж**. Суд определил, что «*любая форма образования, которая подготавливает к получению квалификации по конкретной профессии, ремеслу или занятию или которая обеспечивает необходимые умения (мастерство – англ. SKILLS) для такой профессии, ремесла или занятия, является профессиональной подготовкой независимо от возраста и уровня подготовки ученика или студента, даже если программа подготовки включает элемент общего образования*». В 1988 году, по **делу Блейзо** (Blaizot) **против университета Льежа**, Европейский суд юстиции в обосновании своего решения зафиксировал, что *«Единообразное применение законодательства сообщества не даёт полномочия действовать таким образом, чтобы исключить вообще приобретение знаний в университете из концепции профессиональной подготовки»*. В национальных реалиях это означает:

1. важность ***отработки терминологии***, которая формирует совокупность однозначных профессиональных терминов как в сфере образовательного законодательства, так и в преподавательской деятельности. Проблема терминологии – одна из важнейших в праве, поскольку применение терминов, не имеющих четких правовых критериев, может обусловить возникновение правовых коллизий в реализации права на образование (в данном вопросе недопустима «вкусовщина);

2. поскольку любая форма университетского образования, которая подготавливает к получению квалификации по конкретной профессии (см. ст. 5. «Рівні та ступені вищої освіти» Закона Украины «Про вищу освіту» от 28.12.2014 г.) является профессиональной подготовкой, то академические квалификации, по сути, должны ***сопрягаться*** с профессиональными квалификациями по предметной области специализации мастерства (англ. - *Skill specialisation*) и уровня мастерства (англ. - *Skill level*);

3. **Право человека на образование** (в соответствии со статьёй 53 Конституции) обусловливает необходимость вступления в ***образовательное правоотношение***, которое выступает как механизм осуществления субъективного права **в интересах правообладателя**. В соответствии с мировой практикой законы (как и другие нормативно-правовые акты) в Украине принимаются на основании **Конституции Украины** и должны отвечать ей. Поэтому формирование образовательного законодательства необходимо начинать с трансформации основного закона – в нашем случае, статьи 53 Конституции.

Белоусов Вячеслав Владимирович, *д.т.н., профессор*

СВОЕОБРАЗИЕ ОБРАЗОВАТЕЛЬНЫХ ПОЛОЖЕНИЙ В УКРАИНЕ И США

1 июля Верховная Рада приняла новый Закон « О высшем образовании» (далее - Закон), вступающий в силу 6 сентября 2014 года. Закон определяет принципы и пути реализации государственной политики в сфере высшего образования, уровни и степени высшего образования, органы управления в области высшего образования и их полномочия, стандарты образовательной деятельности, порядок лицензирования высших учебных заведений и аккредитации специальностей, основы создания Единой государственной электронной базы по вопросам образования. Закон предусматривает ликвидацию уровней аккредитации высших учебных заведений, введение академической и первой научной степени - доктор философии, создание Национального агентства по качеству высшего образования и независимых учреждений оценки и обеспечения качества высшего образования.

Деньги, которые заработают государственные вузы, будут изначально храниться не в казначействе, а в государственных банках на специальных депозитных счетах.

Новым понятием является термин эндаумены, по своей сути являющиеся целевым капиталом неприбыльной организации, формируемым за счет пожертвований, доход от использования которого предназначается для реализации уставных целей.

Институт эндаумента широко используется в мировой практике. К примеру, наибольшими эндаументами владеют университеты США и Великобритании. Так, эндаумент Гарвардского университета составляет более 32 миллиардов долларов США. Весомыми по величине являются также эндаументы Йельского, Стенфордского, Принстонского университетов США. Более 80 ВУЗов мира владеют эндаументами объемом более 1 миллиарда долларов США. Чаще всего объектом инвестирования средств из эндаументов являются ценные бумаги, реже - реальные активы.

Эндаумент также является стимулом повышения качества образования и репутации ВУЗов, т. к., основываясь на зарубежном опыте, можно говорить о том, что жертвователями подобных фондов в большинстве являются именно выпускники ВУЗов. Соответственно, нововведение может стать хорошей предпосылкой для качественной конкуренции ВУЗов.

Предлагается создание одноразовых спецсоветов по защите научных работ. Такая методика защит диссертаций имеет место в США. В отличие от украинской системы высшего образования система образования в США отличается своеобразием в том плане, что далеко не все специальности требуют университетского образования.

Университеты в США подразделяются на две группы: с преобладанием обучения (Teaching) и с преобладанием исследований (Research). В университетах очень большой конкурс для поступления на данные специальности и очень маленькая финансовая помощь. Американские студенты, изучающие данные специальности, обычно берут в банке ссуду на время учебы, которую возвращают после окончания учебной программы. Курс для студентов является четырехгодичным, и выпускники колледжей и университетов получают степень Bachelor of Arts (BA) или Bachelor of Sciences (BS), которая соответствует отечественному диплому о высшем образовании.

Вместе с тем, Более одного триллиона долларов, то есть 40 бюджетов Украины - столько денег задолжали Соединенным Штатам американские студенты. Стоимость высшего образования в США растет ежегодно. Сейчас год в частном университете стоит в среднем 25 тысяч долларов, в государственном - дешевле, но среди них меньше престижных. Поэтому выпускники оставляют колледже с многотысячными долгами, которые отдают половину жизни.

Герганов Леонід Дмитрович, *к.п.н, доцент,*
заступник начальника Навчального центру
«Українське Дунайське пароплавство»

ОСВІТНІ ПАРАДИГМИ СУЧАСНОЇ СИСТЕМИ ПРОФЕСІЙНОЇ ПІДГОТОВКИ ФАХІВЦІВ МОРСЬКОЇ ГАЛУЗІ

Інтеграція національної системи професійної освіти до світового освітнього простору вимагає підвищення вимог до професійної підготовки фахівців морської галузі. У документах ЄС обґрунтовано політику щодо професійного навчання, визначено цілі і завдання в цій галузі, зокрема:

-сприяння адаптації до змін в промисловості, особливо під час професійного навчання і перепідготовки;

-удосконалення початкового і подальшого професійного навчання з метою професійної інтеграції та реінтеграції в ринок праці;

-розширення доступності професійного навчання і заохочення мобільності викладачів та тих, хто навчається, особливо молоді;

-стимулювання співробітництва в навчанні між навчальними закладами або центрами професійної підготовки і фірмами;розвиток обміну інформацією та досвідом із загальних проблем для систем професійного навчання держав-членів.

З урахуванням інтеграційних процесів в умовах інформаційно-технологічного розвитку у XXI столітті, ці п’ять напрямків політики ЄС в галузі професійного навчання є актуальними для всіх пострадянських держав й України зокрема [1, с.6]. Аналіз потреб професійних навичок в Європі до 2020 року свідчить, що, наприклад, для 27 країн Європейського Союзу, у тому числі Норвегії й Швейцарії, можливості для працевлаштування будуть включати приблизно 80 млн. робочих місць, із яких майже 7 млн. будуть складати нові робочі місця. Більшість змін у зайнятості стосуватиметься професій, які потребуватимуть високої кваліфікації. Протягом 10 років частка зайнятих на таких робочих місцях збільшиться з 29% до 35%. При цьому, професії,які передбачають середню кваліфікацію,будуть складати половину усіх робочих місць, а частка малокваліфікованих професій скоротиться з 21% до 15% [2].

Серед найбільш дефіцитних якостей, якими мають володіти сучасні кваліфіковані робітники морського профілю для роботи на суднах сучасного покоління, є навички роботи в багатонаціональних екіпажах, професійні навички інформаційно-комунікативних технологій, навички розв’язання виробничих проблем у екстремальних та аварійних ситуаціях, навички пов’язані з безпекою праці та інші. Наприклад, у Великобританії роботодавці виділяють в якості ключових трудових навичок: здатність до комунікації, уміння будувати відношення з клієнтами, уміння працювати в колективі й вирішувати проблеми, а також грамотність, уміння рахувати, загальні навички в галузі інформації та технологій, яких не вистачає багатьом особам, зайнятих пошуком роботи, що є перепоною набору персоналу або слугує причиною зниження потенціальної продуктивності підприємств [3, с.25]. При цьому вони передбачають у своїх бюджетах кошти на навчання персоналу, підвищення його кваліфікації.

Проведене дослідження із забезпечення екіпажів морських суден кваліфікованими фахівцями в професійно-кваліфікаційному розрізі в ПрАТ «Українське Дунайське пароплавство» доводить, що 30% суден мають труднощі у комплектуванні екіпажів морських суден відповідним кваліфікованим персоналом. У зв’язку з цим, пріоритетними напрямками у підвищені ефективності формування професійної компетентності у членів екіпажу морських суден стає:

- формування та відслідкування ситуацій з потребою кваліфікованого персоналу на морських суднах компанії;
- перехід на нові парадигми підготовки кадрів, виходячи з досвіду вітчизняної та світової практиці у морській галузі з даного напрямку;

- запровадження сучасних підходів та організації системи навчання усіх ланках професійної освіти на основі впровадження системи якості;
- перегляд і уточнення кваліфікаційних вимог до робітників і спеціалістів з метою розширення їх професійної мобільності, конкурентоздатності підприємств;
- розробка і запровадження державних стандартів професійної освіти для морської галузі;
- розробка та впровадження у навчальних закладах сучасного навчально-методичного забезпечення професійного навчання з урахуванням змін у виробничому процесі і професійно-кваліфікаційному складі;
- підвищення кваліфікації педагогічних працівників зайнятих у професійному навчанні.

Саме тому зміни в освіті передбачають перехід на нові парадигми у професійній підготовці фахівців для морської галузі, а саме:

1. Перехід виробництва від «конвеєрного» випуску як студентів, так і слухачів курсів, до підготовки їх малими групами, конкретно під вимоги роботодавця. При цьому найважливішим є те, що професійна освіта стає більш гнучкою та здатною до переналагодження. Це стосується як самої системи професійного навчання, так і тих, хто навчається.
2. Перехід від засвоєння загальної інформації до формування якостей, необхідних для творчої діяльності і засвоєння інформації в купі з випуском необхідної продукції чи надання послуг. Основним орієнтиром професійного навчання стає формування творчої особистості, яка не тільки знає технологічний процес, але й володіє здатністю саморозвиватися.
3. Використання у процесі навчання сучасних інформаційних технологій, що кардинально перетворюють навчальний процес, надають йому елементи виробничого процесу, та наближають його до роботи на сучасному обладнанні з використанням усіх вимог, які необхідні роботодавцю.
4. Підвищення ролі професійного навчання фахівців завдяки поширенню її складових (курсів підвищення кваліфікації, курсів спеціальної і спеціалізованої підготовки та ін.), що значно впливає на весь процес підготовки кваліфікованих фахівців), особливо на підвищення їх професійної компетентності.
5. Підвищення витрат роботодавців на навчання фахівців з одночасним зростанням віддачі від неї. Навчання для виробництва стає однією з найприбутковіших галузей вкладення грошей, воно починає концентрувати навколо себе усі напрямки освіти (шкільної, професійно-технічної, вищої, післядипломної), як центр кадрових та інформаційних ресурсів і водночас перетворюється в особливий ресурс формування кадрового потенціалу, що забезпечує його відновлення на ключових етапах розвитку виробництва.
6. Професійне навчання фахівців концентрує в собі нововведення, які спонукають виробництво, формує інноваційний людський капітал для нього, стає головним елементом поповнення та оновлення персоналу.

Національна система підготовки та дипломування моряків відповідає мінімальним стандартам і вимогам Міжнародної конвенції з «Підготовки, дипломування моряків та несення вахти» 1978р. з поправками, на підставі яких рядовий склад флоту для отримання міжнародного підтвердження своєї робочої кваліфікації має пройти спеціальне навчання в навчально тренажерних центрах і отримати відповідний документ-сертифікат [4]. Для України, що втратила більшу частину торговельного флоту під своїм прапором, ці питання є особливо гострі. По-перше, колишні українські судна не зникли, а просто змінили прапор і власника та продовжують працювати. Отже, важливо, щоб на них працювали, по можливості, українські моряки. По-друге, морські навчальні заклади всіх відомств (кількість яких навіть збільшилась) продовжують підготовку кваліфікованих фахівців для морської галузі, роботи яким у рідній країні немає. При цьому на світовому ринку праці кількість вакансій для торговельного флоту обчислюється десятками тисяч, від того для наших моряків не тільки є високооплачувана робота з фаху за кордоном, а й для України зберігається «в гарячому стані» кадровий резерв, без якого реанімація українського торговельного флоту практично неможлива. По-третє, з радянських часів престиж

вітчизняної морської освіти настільки високий, що чимало іноземних держав і зараз надають перевагу морським кадрам з України, тим більше, що й їм, й нам це економічно вигідно.

Розуміючи серйозність, в якій знаходиться вся морська галузь України, коли посилюється роль якості підготовки кваліфікованих фахівців для морської галузі в суперництві країн світу у всіх сферах морської діяльності, чітко усвідомлюються судноплавними компаніями глобальні тенденції формування ефективної морської стратегії, яка орієнтована на використанні на суднах нової техніки, автоматизованих систем управління, інформаційних технологій, в [5] підкреслено, що «морський потенціал України – це сукупність природних ресурсів і надбань людини, які використовуються в процесі провадження морської діяльності в інтересах Українського народу в галузі морського транспорту і система підготовки та перепідготовки фахівців для морської галузі всієї світової спільноти».

Для вирішення завдань, які поставлені Доктриною, необхідно врахувати ряд проблем, які знижують ефективність роботи морського флоту. Окрім технічного стану суден, які у більшості знаходяться на межі технічного ресурсу (багатьом суднам вже за тридцять років) і вкладати кошти в їх ремонт вже не доцільно, вимагає серйозної уваги опрацювання кадрового питання забезпечення флоту. Потрібні нові парадигми професійного навчання фахівців для морської галузі на всіх ланках освіти, які несли в собі позитивні сторони старої, традиційної школи підготовки моряків і нові педагогічні технології в підготовці кваліфікованих фахівців, що чітко уявляють свою відповідальність за якість виконаної роботи, постійно удосконалюють професійну майстерність у швидкоплинному технічному оснащенні флоту і ясно уявляють, що безпека на морі, в першу чергу, залежить від професійної компетентності, професіоналізму і бездоганного виконання усіх вимог, вказаних в міжнародних конвенціях і національних стандартах. Проведені дослідження з навчання фахівців морської галузі в навчальних закладах різного рівня визначили ряд чинників, які негативно впливають на професійну підготовку моряків, такі як:

- відсутність чіткого механізму взаємовідносин між службою управління кадрів судноплавної компанії, і навчальним закладом в питаннях прогнозування підготовки, перепідготовки і підвищення кваліфікації кадрів з перспективою кар'єрного зростання моряків і необхідною ротації кадрів суднових екіпажів;

- нерозуміння своєї ролі в питаннях професійної підготовки моряків керівництвом судноплавних компаній і, як наслідок, недостатнє вникання в питання підготовки кадрів в навчальних закладах, відсутність спланованої кадрової політики без достатнього опрацювання впливу якості підготовки моряка на результати його професійної діяльності;

- низький рівень контролю за якістю підготовки членів екіпажів морських суден з боку командного складу суден, відсутність рекламацій і пропозицій до підготовки працівників морського профілю;

- формальна організація навчання членів екіпажа безпосередньо на судні, для підтримки кваліфікаційного рівня і відробітку дій в екстремальних і аварійних умовах, відсутності методичного забезпечення, методики проведення зайняття на борту судна і контролю з боку навчального закладу;

- відсутність критеріїв професійного відбору для роботи на суднах;

- відсутність матеріальної і моральної мотивацій в підвищенні кваліфікації і конкретних умов професійного зростання;

- недостатнє забезпечення навчальних закладів сучасним устаткуванням, необхідними тренажерними комплексами, відсутність сучасних педагогічних технологій в процесі професійної підготовки моряків, недостатня, у більшості випадків, формальна практична підготовка тих, що навчаються на суднах;

- відсутність постійного зв'язку і моніторингу за якістю самостійного підвищення професійного рівня моряків, які знаходяться у рейсі і навчальним закладом, через систему дистанційного навчання.

Виходячи з цих характерних недоліків, які були виявлені в процесі дослідження як у вищих державних навчальних закладах, так і учбово-тренажерних центрах при судноплавних компаніях, а також з урахуванням міжнародних вимог до професійної підготовки фахівців морської галузі, згідно Конвенції і Кодексу ПДНВ, інтеграції України в міжнародну економічну та освітню спільноту, були визначені наступні завдання:

- покласти на навчальні заклади повну відповідальність за організацію і якість професійної підготовки, перепідготовки і підвищення кваліфікації фахівців для морської галузі з урахуванням вимог міжнародних конвенцій, системи управління безпекою і системи стандартів якості ISO 9001 - 2009;
- розробити і затвердити "Концепцію професійної підготовки фахівців для морської галузі у вищих навчальних закладах", з урахуванням формування кадрового потенціалу судноплавних компаній і специфіки роботи на судах змішаного річка-море плавання;
- удосконалити систему атестації і контролю знань випускників навчальних закладів на сучасному рівні рейтингового відбору, передбачивши висновки комісії відносно їх подальшого професійного просування;
- розробити і впровадити в практику нормативно-правові акти з питань матеріального і морального стимулювання фахівців морської галузі за професійне вдосконалення;
- опрацювати питання матеріальної зацікавленості командного складу в підвищенні кваліфікації членів суднової команди, участі їх в процесі навчання і виховання кадрів;
- удосконалити рейтингово-модульну систему підготовки фахівців для морської галузі, передбачивши її на усіх східцях професійного навчання плавскладу;
- використовувати дистанційну технологію для професійного навчання усіх осіб, що знаходяться в довготривалому рейсі, з урахуванням постійного контролю за рівнем їх професійних знань, компетентності та можливості подальшого просування по службі;
- забезпечити навчальний процес сучасним тренажерним устаткуванням, мультимедійним устаткуванням, системами комп'ютерного контролю і оцінки знань;
- відпрацювати питання проходження практичної підготовки студентів і слухачів курсів на суднах з використанням можливостей національних та зарубіжних компаній;
- провести перевірку якості підготовки інструкторсько-викладацького складу в суворій відповідності з модулем IMO 6.09 Конвенцій ПДНВ мінімального стандарту компетентності інструктора-викладача, забезпечити його психолого-педагогічну підготовку для роботи в нових умовах професійного навчання моряків з використанням сучасних форм і методів навчання, методики проведення тренажерної підготовки, процедури використання тренінгу, спеціальних питань фонової базової професії;
- продовжити науково-дослідні роботи за усіма напрямами професійної підготовки, перепідготовки і підвищення кваліфікації фахівців для морської галузі з урахуванням вимог безпечної роботи на суднах морського флоту.

Література:

1. Ничкало Н.Г. Проблеми професійного навчання на виробництві у контексті педагогіки, психології праці й андрагогіки / Професійне навчання на виробництві: Зб.наук.праць: Вип. IV. – К.: Вид-во Інституту професійно-технічної освіти НАПН України, 2011. – С.6.

2. Квалифицированная рабочая сила – основа для интенсивного, устойчивого и сбалансированного экономического роста. – Женева: МОТ, 2010. – 70с.

3. Радкевич В.О. Сучасні чинники розвитку професійного навчання в умовах виробництва/ Професійне навчання на виробництві: Зб.наук.праць: Вип.IV.– К. : Вид-во Інституту професійно-технічної освіти НАПН України, 2011. –С.18-26.

4. Міжнародна конвенція про підготовку та дипломування моряків і несення вахти 1978 з поправками (ПДНВ) – 551с.

5. «Морська доктрина України на період до 2035 року» Постанова Кабінету Міністрів України від 07 жовтня 2012 року №1307.

Вільський Геннадій Борисович, *PhD, професор, ректор,*
Михалишин Богдан Євгенович, *к.т.н.,перший проректор,*
МТУ «Миколаївська політехніка»

ФОРМУВАННЯ КРИТЕРІЇВ ОЦІНЮВАННЯ НАУКОВОЇ ЗНАЧИМОСТІ СТУДЕНТСЬКИХ КОНКУРСНИХ ДОСЛІДЖЕНЬ

Наукова робота - це самостійно виконане наукове дослідження тієї чи іншої проблеми, яке відповідає науковим принципам, має певну структуру, містить результат власного дослідження і власні висновки [1], а його якість може бути визначена за встановленими критеріями. Тому очевидно, що цільова ефективність оцінювання студентських конкурсних наукових робіт у великій мірі залежить від чіткості формулювання запропонованих критеріїв і можливості їх достовірного, об'єктивного встановлення конкурсною комісією.

Так скажімо, критерії оцінки робіт ІІІ Всеукраїнського молодіжного конкурсу „Новітній інтелект України" [2] є достатньо чіткими, але не конкретними і містять, наприклад, пункт: «Наявність посилань на досвід інших країн, які вирішили аналогічні проблеми», який навряд чи можна об'єктивно оцінити. Критерії оцінювання учнівських робіт в МАН [3] є не такими чіткими, але в них конкретно вказані максимальні кількості балів по кожному запропонованому критерію. В «Положенні про обласний конкурс робіт молодих учених Миколаївської області» взагалі віддається перевага практично-реалізованим, впровадженим дослідженням, які мають розраховану економічну ефективність (75 % балів), а теоретичні дослідження оцінюються за доволі суб'єктивною шкалою «актуальності». В «Положенні про проведення Всеукраїнських конкурсів студентських наукових робіт» взагалі відсутні методичні вказівки до формування критеріїв оцінювання досліджень. Тому кожен базовий вищий навчальний заклад формує власні непрозорі критерії оцінювання, які стають відомими лише після оприлюднення результатів конкурсу. Це приводить до того, що переможцями конкурсу стають роботи, які не відповідають встановленим вимогам до представлених робіт, про що свідчать результати конкурсу, наприклад у провідних вишах України. В Національному університеті імені Т.Г. Шевченка в конкурсі по спеціальності «Менеджмент» переможцями стали роботи, в яких шифрування не відповідало вимогам «Положення», тобто використовувалися не слова, а набір букв і цифр. Позитивним моментом слід відзначити, що на сайті університету оголошено кількість балів кожної роботи – переможця заочного етапу (з максимальних 200 балів, які складалися з оцінювання 2 науковими експертами), проте загальні критерії оцінювання робіт невідомі (відомо тільки що з 100 балів експерт вираховував бали за недоліки, одному йому зрозумілі). У Вінницькому національному технічному університеті в конкурсі зі спеціальності «Інформатика, обчислювальна техніка, автоматизація» переможцями стали 5 учасників з цього університету (всього було 31 переможців), критерії оцінювання взагалі відсутні, а при оголошенні підсумків конкурсу висвітлені лише рекомендації для представлення презентації. Як приклад некоректності оцінювання є диплом 4 ступеня (який не передбачується «Положенням»), отриманий студентом нашого університету Владиславом Шумиком, хоча результати його дослідження запатентовано і впроваджено при діагностуванні біля 200 працівників ДП «Морський торгівельний порт «Южний». Разом с цим переможцями стали деякі чисто теоретичні роботи. В Національному медичному університеті імені О.О. Богомольця в конкурсі по спеціальності «Профілактична медицина» ІІ місце зайняло дослідження студента Дніпропетровської медичної академії А.Р. Лі «Внесок видатних земських санітарних лікарів Катеринославщини кінця XIX – початку XX століття у справу збереження громадського здоров'я», зроблене на англійській мові. Виникає сумнів в об'єктивності оцінювання даної роботи, адже в оцінці її якості передбачалося 3 критерія: актуальність, новизна і практичне значення для сучасної медицини.

Тому цілком зрозуміло, що необхідна розробка прозорих й об'єктивних критеріїв оцінювання. За багаторічним досвідом проведення конкурсів студентських наукових (творчих) робіт підсумкова оцінка (ПО) дослідження конкурсанта може розраховуватися за формулою:

$$ПО = \sum_{i=1}^{3} \frac{ПО_i}{3} = \frac{1}{3} \sum_{i=1}^{3} \left(\sum_{к=1}^{6} Б_к B_к + \sum_{n=1}^{3} K_n T_n \right),$$

де $ПО_i$ – оцінка роботи конкурсанта *i*-им членом журі;

$Б_к$ – оцінки відповідно до критеріїв для заочних етапів конкурсу ($Б_{к max} = 20$);

$B_к$ –вагові коефіцієнти критеріїв оцінювання робіт заочного представлення;

K_n – оцінки згідно з критеріями для очних етапів конкурсу ($K_{n max} = 10$);

T_n – вагові коефіцієнти критеріїв оцінювання презентацій.

В якості критеріїв для заочного розгляду робіт доцільно вибрати наступні:

1. актуальність (B_1=0,5);
2. науковість (B_2=1,0);
3. достовірність та обґрунтованість результатів (B_3=0,25);
4. логічність та повнота викладу (B_4=0,25);
5. оригінальність та інноваційність (B_5=0,75);
6. практичне (теоретичне) значення, практична реалізація (B_6=1,0).

Для оцінки презентацій потрібно враховувати:

1. якість представлення (T_1=0,5);
2. ступінь самостійності роботи (T_2=1,5);
3. вміння відповідати на поставлені запитання (T_3=0,5).

Надзвичайно важливим та відповідальним моментом у написанні наукової роботи є вибір теми дослідження. Правильно обрати тему роботи - це майже наполовину забезпечити її успішне виконання. Назва теми повинна бути простою, відповідати пропонованому секційному напряму та галузі гуманітарних або технічних знань, по можливості короткою і оригінальною (не більше 7-8 слів). У назвах необхідно уникати ускладненої термінології, особливо так званого псевдонаукового характеру, як, наприклад, "Дослідження питання...", "Деякі питання...", "Дослідження деяких шляхів...". Від правильності формулювання теми дослідження залежить і кінцевий результат. Необхідно чітко сформулювати мету роботи та окреслити ряд конкретних завдань, розкрити наукову новизну та його актуальність. Під актуальністю насамперед розуміють доцільність даної роботи для розвитку відповідної вітчизняної галузі економіки. Зміст роботи має відповідати меті. Особливої уваги необхідно надати логічності викладу та плавності переходу від викладу одного питання до іншого. Не потрібно зловживати цитуванням, але принципові для змісту роботи думки науковців потрібно процитувати. Знижує рівень роботи переобтяженість її матеріалами, які взагалі не стосуються теми дослідження. Висновки мають відповідати меті та завданням дослідження, про які було повідомлено у вступі та сформульованим відповідно до опису основної частини. Варто наголосити на важливості отриманого наукового здобутку для науки, при потребі можна сказати про перспективу даного дослідження, викласти рекомендації щодо використання одержаних результатів. У висновках не повинно бути нових узагальнень порівняно з попереднім текстом.

Науково-дослідницька робота повинна засвідчити самостійність висновків та узагальнень оригінального наукового характеру. Мова науково-дослідницької роботи повинна бути позбавленою подвійного тлумачення. Крім того потрібно не допустити використання в роботах відомих результатів інших досліджень, що з врахуванням сучасних ІКТ-технологій надзвичайно легко відсліджується. Як показує досвід роботи, типовими недоліками багатьох студентських наукових досліджень є їх реферативно-описовий характер; неповнота розкриття теми (це часто трапляється через те, що сама тема сформульована занадто широко й просто фізично неможливо її осягнути й дослідити); відхилення від теми дослідження; не визначення завдань дослідження, які потрібно виконати

задля досягнення мети; не дотримання наукового стилю викладу: відсутність власних висновків, які б логічно випливали з проведеного дослідження тощо.

Безумовно запропоновані нами вимоги та критерії щодо оцінки наукової значимості дуже високі і важкі для студентів, проте в обов'язковому порядку про них потрібно пам'ятати і проявляти прагнення до їх досягнення. Слід також вважати що тільки за умови ознайомлення студентської молоді з особливостями наукової діяльності та запропонованими відкритими, прозорими критеріями оцінювання робіт, які нададуть можливість їм цілеспрямовано працювати та розвинути креативне мислення, при обов'язковій умові об'єктивної оцінки експертами всіх 9 критеріїв, можна досягти необхідних результатів у підвищенні цільової ефективності студентських наукових досліджень, а відповідно і покращити якість вищої освіти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Артемчук Г.П. Методика організації науково-дослідницької роботи: Навчальний посібник. - К.: Форум, 2000. – 271 с.
2. [Електронний ресурс]. – Режим доступу: http://www.novi.org.ua/projects/ novi/ 3rd/ part/
3. [Електронний ресурс]. – Режим доступу: http://matematukrschko. 3dn.ru/ news/ vimogi_do_oformlennja_konkursnikh_robit_man/2011-11-10-55

Манькусь Ірина Володимирівна, *к.п.н., доцент,*
Недбаєвська Людмила Степанівна, *к.п.н., доцент,*
МНУ імені В.О. Сухомлинського

ОСВІТНІЙ ПРОЕКТ «ПОВЕРТАЄМОСЬ ДО РЕАЛЬНОСТІ» ЯК ШЛЯХ ЗАПОБІГАННЯ КОМП'ЮТЕРНОЇ ЗАЛЕЖНОСТІ

У Концепції розвитку освіти України на період 2015-2025 років визначені численні проблеми системного характеру, які накопичувалися в освітньому секторі країни протягом усього періоду існування незалежної України. Серед них особливо гострими для системи вищої освіти є: зниження якості освіти та падіння рівня знань і вмінь студентів; моральне старіння методів і методик навчання; повільне і безсистемне оновлення змісту освіти; зниження якості педагогічних кадрів і криза педагогічної освіти; зниження якості навчальної літератури; критичний брак передових технологій в освітньому просторі [1]. Комп'ютерна залежність виникла і поширилась наприкінці XX століття. За результатами дослідження, проведеного в ході реалізації проекту, встановлено, що сетеголізм (залежність від Інтернету) і кіберадикція (залежність від комп'ютерних ігор). Найгостріші проблеми у 75% випускників ЗОШ. Зазвичай це молодь віком до 17 років із сильно завищеною або заниженою самооцінкою, у яких захворювання призводить до роздвоєння особистості.

Робота над проектом дає можливість визначення причин комп'ютерної залежності, серед яких домінують: брак спілкування з однолітками, бажання бути як усі, невпевненість в своїх силах, брак уваги з боку батьків. Визначені нами загальні ознаки залежності: зневага до важливих речей в житті, руйнування стосунків залежної людини зі значимими людьми, роздратування та скритність у відносинах з оточуючими, які дозволили визначити небезпеки комп'ютерної залежності, головна з яких, втрата зв'язку з реальністю.

З метою запобігання комп'ютерної залежності в рамках освітнього проекту нами розроблено і впроваджено в освітні середовища навчальний центр профілактики кіберзалежності «Enter to reality» (Повернення до реальності). Такі центри сьогодні функціонують з метою пошуку молоді, якій потрібна допомога, перевірка рівня залежності, бесід з батьками та вивчення захоплень молодих людей і організації їхнього дозвілля без комп'ютера. Основним освітнім продуктом проекту є його учасники, які самі починають

розуміти: комп'ютерна залежність – це реальність, із якою необхідно боротися, а ще краще – запобігати.

Список використаних джерел:

1. http://mon.gov.ua/ (Проект Концепції розвитку освіти України на період 2015–2025 років).
2. Вербицкий А. А. Активное обучение в высшей школе: контекстный подход / А. А. Вербицкий. – М. : Высш. шк., 1991. – 207 с.
3. Освітні технології: вчитель фізики. Навчально-методичний посібник / О.М. Пєхота, І.В. Манькусь. – Миколаїв : Іліон, 2011. – 247с.
4. Педагогічні технології в шкільній освіті. Навчальний посібник / С. П. Бондар, Л. Л. Момот, Л. А. Липова, М. І. Головко ; за заг. ред. С. П. Бондар. – Рівне : Ред. видав. центр «Теніс» Міжнар. ун-ту «РЕГІ» ім. акад. С. П. Дем'янчука, 2003. – 200 с.
5. Підготовка майбутнього вчителя до впровадження педагогічних технологій: Навч. посібн. / За ред. І.А.Зязюна, О.М. Пєхоти . – К. : А.С.К., 2003. – 240 с.

Голубев Владимир Александрович, *к. юр. н., доцент,*
директор Департамента противодействия киберпреступности «Cyber Safety Unit»

СОЦИАЛЬНЫЕ СЕТИ КАК ПОЛЕ БОЯ В ИНФОРМАЦИОННОЙ ВОЙНЕ

Уже больше года Украина ведет активную фазу необъявленной войны с Российской Федерацией. Это противостояние — вопрос не года-двух, а, очевидно, более длительного периода. При этом именно ближайшие годы могут стать решающими. Как вы знаете, войну России против Украины называют гибридной. Все потому, что война настоящая, а информация о ней лживая. Против нас открыто много фронтов, и один из особенно важных – информационный.

Вот почему киберпространство как поле ведения противоборства двух или более сторон приобретает все большее значение. Уже сегодня бюджеты ведомств безопасности развитых стран, задействованных в системе кибербезопасности государства, составляют миллиарды долларов, и ни одна из стран еще не уменьшала расходов по этим статьям. Не стоит обманываться, что эти средства вкладываются исключительно в системы «обороны» и «защиты», — неформально почти все государства занимаются разработкой и наступательных кибервооружений. Большинство последних активных вооруженных противостояний, так или иначе, сопровождались и противостоянием в киберпространстве.

Это было характерно для недавней войны в Ливии, частично — в Сирии, а кибершпионаж и кибердиверсии вообще являются постоянным фоном международных отношений. Работа вируса Stuxnet, разоблачение шпионских вирусов и сетей Duqu, Flame, Gauss, Miniduke, Red October, Wiper — вот лишь неполный перечень известных кибершпионских или кибердиверсионных акций, выявленных с 2011 г., и с каждым следующим годом их становится все больше. И это без учета целенаправленных кибершпионских действий против конкретных государственных или промышленных объектов, цель которых — получить информацию о закрытых разработках (в том числе — новейших исследованихя в сфере ВПК). Известный вирус Stuxnet, целью которого была ядерная программа Ирана, его разработчики позиционировали именно как асимметричный ответ на эту программу. То есть развитые государства четко осознают, что кибероружие может оказаться реальным асимметричным инструментом противодействия странам, ставящим под угрозу существующий международный порядок в сфере безопасности [1].

С развитием мобильного интернета социальные сети стали серьезным элементом ведения информационной войны. Сегодня большинство СМИ активно используют

информацию из интернета, в том числе и из социальных сетей. И, на мой взгляд, это серьезно угрожает информационной безопасности. Что такое информационная безопасность в данном контексте – это защита от ложной информации, на основе которой может быть приняты неверные решения. Т.е. любая непроверяемая информация несет в себе потенциальную опасность информационной безопасности.

Если традиционные СМИ имеют какую-то верификацию и дорожат соей репутацией, то участник соцсети полностью избавлен от этого. Т.е. вы не можете проверить каждый источник в сети, который утверждает, что является очевидцем событий. Особенно остро этот вопрос встал в связи с событиями на Украине. Если собрать все источники, которые выдают себя за очевидцев, а также съемки фото и видео с мобильных телефонов, - то, мне кажется, там людей-то столько нет, сколько этих источников.

Так в марте 2015 г. СБУ выявлено около 600 антиукраинских групп в соцсетях. Около 80% подобных групп были созданы и администрируются с территории РФ или «ДНР» и «ЛНР». Соцсети Facebook, Вконтакте и Одноклассниках, с одной стороны, – цифровой вариант сарафанного радио для более продвинутой публики. С другой, – мощная информационная площадка для СМИ и поле боя для российских ботов и “диванной сотни”. И здесь проще проверить, где действительно в Донецке взорвалось и сколько человек погибло. А патриотам разных мастей обменяться “Репостами!” о распятых мальчиках и удельном весе чеченцев в рядах боевиков.

Есть четкий раздел среди пользователей: ВК и ОК – пространство, завешанное георгиевскими лентами, фанаты “Новороссии” здесь абсолютно в собственной среде. В Facebook ситуация радикально отличается. Местные украинские форумы абсолютно не уступают противнику по качеству, разве что в количестве пользователей могут проиграть. Все-таки, среди выехавших из “ДНР/ЛНР” людей весьма значительная часть настроена проукраински, а вот ряды патриотично настроенных украинцев в зоне АТО постепенно пустеют. Слишком много забот у выехавших на украинский материк. Многие ветки обсуждений в соцсетях, помимо перемывания костей политикам и проверки новостных ресурсов на адекватность, ориентированы, прежде всего, на взаимопомощь. Здесь первой появляется информация о ситуации на блокпостах с пропусками или кассах супермаркетов, принимающих оплату банковской картой. Все посты “проверены на практике”, а боты отправляются в “вечный бан”. Но тут ресурсы Украины не могут сравниться с ресурсами, которые выделяет Российская Федерация на войну с Украиной. Поэтому в информационном противостоянии, на сегодня надежды на негосударственный ИТ-сектор [2].

Проведенное нами анализ показал, что Украина входила и пока входит в число стран, где российские социальные сети по числу пользователей вне конкуренции. На начало 2014 по данным Яндекс в стране было более 7,47 млн. аккаунтов «В контакте», 1,57 млн. «Одноклассники». Фейсбук мог похвалиться всего лишь 857 тысячами участников. Причём картина была одинаковой в большинстве регионов. За исключением Луганской области с достаточно большим охватом сетью «Одноклассники» — она хоть и осталась на втором месте, но имела значительно большее число подписчиков в расчёте на 1 пользователя интернет. Вторым исключением стала Одесская область, у жителей которой на втором месте Фейсбук.Древняя китайская поговорка подсказывает нам, что адекватная оценка ситуации – это половина решения проблемы. Украинскому государству и украинскому обществу следует понять, что они находятся в ситуации войны, международный информационный аспект которой является одним из решающих факторов и основных фронтов. В этот фронт Россия инвестирует очень много и, в отличии от Украины, проводит систематическую информационную политику, имеющую существенный дезинформационный эффект. Одним из ответов на такие вызовы стало создание под эгидой Министерства информационной политики Украины “Информационных войск” [3], которые начали сражаться с российскими ботами и фейками.

ИСТОЧНИКИ:
1. Владимир Горбулин «Гибридная война как ключевой инструмент российской геостратегии реванша»: http://gazeta.zn.ua/internal/gibridnaya-voyna-kak-klyuchevoy-instrument-rossiyskoy-geostrategii-revansha-_.html
2. Информационная война: определения и базовые понятия: http://psyfactor.org/psyops/infowar25.htm
3. "Информационные войска" будут сражаться с российскими ботами и фейками: http://cybersafetyunit.com/informatsionnyie-voyska-budut-srazhatsya-s-rossiyskimi-botami-i-feykami/

Шипилов Владимир Андреевич, *к.фил.н.,*
директор Николаевской ОШ I-III ступеней № 61

ПРОБЛЕМЫ ИНФОРМАЦИОННО-ЛИЧНОСТНОЙ БЕЗОПАСНОСТИ ПРИ ОБУЧЕНИИ МОЛОДЕЖИ

Одним из важнейших компонентов, формирующих современное общество, является информация, которая всё больше и больше заполняет современный мир.

«В современном социуме информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т.п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью» [1].

Современный мир полон разного рода опасностей, среди которых наибольшую угрозу несут в себе опасности социального характера (порнография, ложь, клевета, дезинформация, национализм, терроризм, массовые беспорядки и т.д.). Молодёжь бесконтрольно черпает из Интернета информацию, которая заключает в себя элементы насилия, жестокости, агрессии, формирует соответственно моральные качества и эстетические вкусы, моделирующие поведение подрастающего поколения.

Это наиболее значимые, но не единственные проблемы, связанные с использованием Интернета несовершеннолетними. Серьезной проблемой является игровая зависимость у детей и подростков, которая вызывает у них значительные психологические проблемы, трудно поддающиеся лечению (т.н. компьютерная зависимость).

Особо следует выделить проблему воздействия Интернета на формирование суицидальных склонностей у детей и подростков.

Постоянное и беспрерывное использование всемирной паутины подростками, молодёжью оказывает негативное влияние на их внутренний мир, развивая в них дух пессимизма, конфликтности, саморазрушения, страха. Не склонные к объективному и глубокому анализу, они становятся вспыльчивыми, раздражительными, агрессивными.

Чувство низкой самооценки, стресс и социофобия угнетают врожденные творческие способности ребенка, существенно тормозят процесс его социализации. Молодёжь становится наиболее уязвимой, неспособной должным образом противостоять жизненным трудностям.

Изменения, происходящие в их психическом состоянии, развивают депрессивные настроения, которые порой и доводят до самоубийства.

Зависимость от Интернета сужает духовные горизонты молодёжи, т.к. их Интернет-поиски сосредоточены главным образом на играх и бессмысленных действиях, лишённых познавательного интереса.

Постоянное и непрерывное использование ребенком Интернета и указанные выше виды деятельности, бесполезные и даже вредные с точки зрения педагогики, влияют и на язык современной молодёжи, усугубляя бедность их словарного запаса.

Бедный словарный запас, широкое использование ненормативной лексики не способствует развитию цельной и сформированной личности человека.

Существует немало сторонников свободы слова, свободы средств массовой информации в Украине, которые отстаивают вседозволенность как в традиционных, так и компьютерных масс-медиа.

Но если у взрослого человека хоть как-то выработаны механизмы защитных реакций, то дети и молодёжь наиболее уязвимы к информационным угрозам.

А ведь общеизвестно, что эстетические вкусы, моральные качества молодёжи формируются прежде всего под влиянием стихийных факторов общественной жизни.

Обеспечение государством информационной безопасности детей, защита физического, умственного и нравственного развития несовершеннолетних, а также человеческого достоинства во всех аудиовизуальных медиа-услугах и электронных СМИ – требование международного права. Международные стандарты в области информационной безопасности молодого поколения находят отражение и в украинском законодательстве.

Для сведения информационных угроз к минимуму – нужно прежде всего снизить уровень риска.

В наше время особенно актуальна проблема формирования у школьников, студентов и молодёжи общеучебных умений безопасной работы с различными источниками информации, их готовности и способности регулировать информационные угрозы.

Несмотря на то, что в большинстве случаев молодёжь находится под постоянным контролем (родители, учителя, преподаватели и т.д.), все же она наиболее подвержена риску, связанному с информационным взаимодействием.

Мне как директору общеобразовательной школы подробнее хотелось бы остановиться на формировании информационно-личностной безопасности школьника, которая включает в себя два аспекта:

- защищённость информационной среды общеобразовательных учреждений через создание системы контентной фильтрации: программного комплекса, позволяющего ограничивать учащимся доступ к интернет-ресурсам на основании анализа их содержимого.
- создание внутренних условий безопасности личности подростка через формирование у учащихся способности к распознаванию, уклонению, преодолению опасностей.

Подростковый возраст характеризуется проявлением возросших возможностей развития познавательной деятельности, интеллектуальной рефлексии, повышенной активности.

Именно поэтому, запретительно-ограничительными мерами проблему информационной безопасности личности не решить. **Информационная безопасность может быть обеспечена только через формирование способности распознавать информационные опасности.**

На мой взгляд, наиболее эффективными направлениями в решении обозначенной проблемы являются следующие направления:

- развитие умений критически осмысливать информацию, конструктивно её преобразовывать;
- формирование нравственно устойчивой личности, обладающей иммунитетом к воздействиям различных взглядов и убеждений, противоречащим его личностным установкам;
- воспитание у подростков избирательного отношения к внешним влияниям;
- развитие умений сопоставлять собственные умения и поступки с усвоенными обществом нормами и принципами.

Педагогический аспект проблемы развития у подростков способности преодолевать информационно-психологические опасности заключается в обучении их защите от манипулятивных воздействий в различных коммуникативных ситуациях.

Важнейшим условием эффективности такого вида обучения выступает опора на имеющийся у школьников небольшой жизненный опыт. В педагогике его принято называть витагенным обучением, сущность которого состоит в актуализации жизненного опыта личности, ее интеллектуально-психологического потенциала в образовательных целях [2].

Отбор различных коммуникативных ситуаций и организация учебной деятельности должны базироваться на логике перехода опыта жизни в жизненный опыт подростка: от недифференцированной стадии первичного восприятия витагенной информации через оценочно-фильтрующую стадию,

Самоуправление информационными опасностями в предложенных коммуникативных ситуациях, следовательно, представляет собой алгоритм следующих действий и соответствующих им умений:

- ориентация в ситуации,
- оценка потенциала влияния,
- выявление признаков скрытого психологического принуждения,
- выбор тактики и способов защиты,
- организация защитного поведения.

Витагенная технология формирования информационно-личностной безопасности подростков, таким образом, направлена на развитие способности распознавать, предвидеть, противостоять информационным опасностям и угрозам, негативным информационным воздействиям, базируется на умениях самосохранительного поведения [3].

В процессе формирования информационно-личностной безопасности подростка в качестве источников информации используются средства массовой информации, Интернет, научная, техническая и художественная литература, социальное, деловое и бытовое общение, образовательный процесс, что, к сожалению, недостаточно предусмотрено школьными методиками предметов.

Но существует серьёзная проблема, связанная с противоречием между существующей необходимостью обеспечения информационной безопасности молодёжи, использующей Интернет в образовательном процессе, и отсутствием механизма ее реализации в образовательном пространстве. Проблемность ситуации состоит в отсутствии единой научно разработанной теории информационной безопасности, несоответствии потенциальных возможностей информатизации образования и получаемыми в настоящее время результатами. Отсутствие законодательных и нормативно-правовых документов, определяющих уровень нравственности данных, циркулирующих в информационных электронных сетях, обостряет проблему воспитания подрастающего поколения, использующего ресурсы Глобальной Сети.

Информационная безопасность в учебном учреждении может быть достигнута реализацией воспитательной функции образования на основе приобщения учащихся к информации культурного, этического, гуманистического характера; обеспечением мотивированного включения молодёжи в разнообразные виды деятельности в информационной сфере; реализацией практической направленности отбора содержания образовательных ресурсов Интернета и применения интерактивной технологии фильтрации поступающей информации.

Решая задачи построения информационного образовательного пространства, многие учебные заведения приобретают различные программные продукты, интегрирующие в себе многие функции информационных систем («КМ-Школа», «Net-School», «Школьный офис», TeachPro и др.) [4].

Инновационный продукт компании «Кирилл и Мефодий» - «КМ-Школа <#"justify">·хранение личных дел учащихся и учителей в электронном виде (БД);

- обеспечение коммуникации всех участников образовательного процесса (библиотека, методический кабинет, сайт школы);

- наличие большого объема цифровых образовательных ресурсов (готовые уроки, Медиатека КМ-Школы, портал «Школьный клуб»);

- доступность и открытость результатов учебного процесса (интеграция ИИП «КМ-Школа)

Новые возможности сети Интернет для образования требуют их учета при построении информационного образовательного пространства, которое сегодня не может ограничиваться стенами учебного учреждения. Необходима поддержка дополнительного обучения дома, подготовки учителей и преподавателей к занятиям.

Только информационная компетенция учащейся молодёжи, сформированная на принципах витагенной технологии обучения, и выстроенное информационное пространство для молодёжи может обеспечить информационно-личностную безопасность учащихся.

Использованные источники:

1. Электронный ресурс: https://ru.wikipedia.org/wiki
2. Электронный ресурс: http://sociosphera.com/publication/conference/2014/243/tehnologiya_vitagennogo_obucheniya_v_shkole/
3. Грачев Г. Г. Личность и общество: информационно-психологическая безопасность и психологическая защита. М., 2003.
4. Электронный ресурс: http://www.bibliofond.ru/view.aspx?id=563232

Юдін Олександр Костянтинович, *д.т.н., професор,*
Весельська Ольга Михайлівна, *аспірант,*
Національний авіаційний університет

АНАЛІЗ ПАРАМЕТРІВ ОЦІНКИ ЯКОСТІ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОЇ СИСТЕМИ ДЕРЖАВНОГО ПРИЗНАЧЕННЯ

Ключовою складовою технічного забезпечення інформаційних систем державного призначення є інформаційно-комунікаційна система та мережа (ІКС), головна функція якої полягає в організації оперативного й конференційного обміну інформаційними потоками між користувачами державних інформаційних ресурсів (ДІР) та оптимізацією витрат на передачу даних. Найважливішим показниками ефективності функціонування ІКСМ державного призначення є стійкість ДІР до дешифрування (порушення властивостей конфіденційності) та час і обсяги оперативної доставки інформації. Данні властивості інформаційних ресурсів та ІКСМ залежать від:

1) особливостей ІКСМ, а саме від типу та технічних характеристик каналів зв'язку;

2) формату та обсягів оброблюваних і переданих даних;

3) ефективності алгоритмів стиску та шифрування ДІР, тощо.

Найбільш повна інформація для систем прийняття і підтримки рішень (СППР) в автоматизованих системах управління (АСУ) ДІР доставляється на основі відеоданих й графіки. Обсяги відеопотоків для сучасних систем формування й знімання інформації змінюються в межах від десятків Мбіт до сотні Гбіт. Частка відеоінформаційного потоку займає до 90% від загального потоку інформації, оброблюваної, переданої й аналізованої в інформаційних системах (ІС).

Тому для зниження часу доставки даних розробляються спеціальні стандарти, протоколи й методи обробки даних, які є складовими інформаційних і програмно-математичних забезпечень функціонування інформаційних систем державного призначення.

Основними причинами тимчасових затримок є, з одного боку, обмежені характеристики технічного забезпечення функціонування ІКС ДІР, а з іншого боку, обсяги оброблюваних і переданих цифрованих зображень, а також час на реалізацію процедури шифрування інформаційного потоку.

Модернізація й установка більш сучасних програмно-апаратних комплексів, або більш сучасного телекомунікаційногообладнання є дорогим і не завжди можливим напрямом підвищення ефективності функціонування інформаційних систем ДІР. Тому, поряд з розвитком технічної бази, необхідно здійснювати модернізацію інформаційного забезпечення ІКС ДІР. Один із напрямів такої модернізації полягає в скороченні обсягів відеоданих за рахунок інтегрування в інформаційні системи інтегрованих технологій крипто-стиску зображень.

Великий внесок у побудову теорії й методів стиску даних зробили багато вчених. Серед них Зубарєв Ю.М., Корольов А.В., Красильников Н.Н., Поляков П.Ф., Юдін О.К., Бараннік В.В., Рябко Б.Я., Свириденко В.А. та ін. Із закордонних дослідників значний внесок зробили Зив Дж., Претт У.К., Шеннон К., Хартлі Р.Л., Хаффман Д.А. та ін.

Проведений аналіз існуючих технологій компресії показує, що забезпечувані ними ступені стиску та час і стійкість методів шифрування не задовольняють необхіднимумовам сучасних ІКС ДІР. Так, для методів без втрати якості середнє значення ступеня стиску при обробці середньокогерентних зображень не перевищує 2 разів. Для методів із втратами якості середнє значення ступеня стиску не перевищує 3 разів для пікового відношення сигнал/шум на рівні 60дб і не перевищує 20 разів для пікового відношення сигнал/шум на рівні 30дб. Дані характеристики в середньому на 30 - 50% нижче необхідних значень за ступенем стиску для забезпечення передачі зображень у реальному часі. При цьому, процеси стиску ДІР та їх шифрування, виконуються відокремлено. Даний стандартний підхід до обробки ДІР значно підвищує час обробки даних.

Таким чином, існуючі технології компресії та шифрування не дозволяють здійснювати доставку інформації в реальному часі в ІКС державного призначення. Звідси виходить, що існує *науково-прикладне завдання*, яке полягає в необхідності підвищення ступеня стиску зображень із регульованою втратою їхньої якості та інтеграції даних методів з алгоритмами і процедурами шифрування ДІР одночасно.

Отже, для підвищення ефективності функціонування ІКС державного призначення необхідно розробити технологію крипто-стискуДІРна основіметодів компактного подання та шифрування даних цифрових зображень з урахуванням їх інтеграції. Тому *тематика*дослідження є *актуальною*.

Мета і завдання дослідження. Мета роботи полягає в аналізі параметрів ефективності функціонування ІКС державного призначення з урахуванням методів компактного подання та шифрування ДІР, а також їх інтеграції в ІКС державного призначення.

Наукова новизна одержаних результатівповинна бути обумовлена рішенням завдань щодо зменшення сумарного часу обробки й передачі відеоінформації в ІКС ДІР без втрати якості (або з регульованою якістю) за рахунок скорочення структурної й статистичної надмірностей зображень та інтеграції з алгоритмами та методами шифрування відео потоків даних.

Новизна отриманих результатів буде підтверджена всебічним аналізом положень теорії інформації й кодування (шифрування), а також відсутністю аналогів серед методів і технологій стиску цифрованих зображень.

У роботі проводиться аналіз характеристик технічного й інформаційного забезпечення функціонування інформаційних систем ДІР щодо скорочення часу доставки та шифрування даних. Показано роль і місце технологій компресії зображень для підвищення ефективності функціонування ІС з урахуванням алгоритмів шифрування. Виявлено необхідність підвищення ступеня стиску відеоданих з регульованою якістю їхньої реконструкції та інтеграції даних процедур з процедурами шифрування. Обґрунтовано підхід до підвищення

ступеня стиску, заснований на подальшому розвитку технологій компресії з регульованою втратою якості.

Найважливішим показником ефективності функціонування ІКСМ є час доставки інформації τ_{deliv}, що формується на основі часу τ_{oprt} обробки й часу τ_{trans} передачі $\tau_{deliv} = \tau_{oprt} + \tau_{trans}$. Показано, що істотний вплив на збільшення часу доставки даних роблять з одного боку обмежені характеристики технічного забезпечення функціонування ІС, а, з іншого боку, - обсяги оброблюваних і переданих цифрованих зображень. Для скорочення обсягів відеоданих в інформаційні системи інтегруються технології компресії зображень з урахуванням методів шифрування. Встановлено, що показниками якості функціонування технологій компресії цифрованих зображень є коефіцієнт стиску C_r відеоданих; кількість типових операцій на стиск та шифрування υ_{com} і на відновлення з дешифруванням ν_{ren} цифрового зображення, на основі яких визначається час на стиск і шифрування τ_{com} та на подальшу реконструкцію τ_{ren} зображень (відкритий текст або відкрите зображення). З застосуванням технологій компресії і шифрування зображень час $\tau_{d.comp}$ їх доставки в ІКСМ визначається на основі співвідношення

$$\tau_{d.com} = \nu_{com} / S_c + \nu_{ren} / S_c + W_{init} / C_r S_{trans} \quad (1)$$

де ν_{com} – кількість типових операцій на стиск і шифрування;

S_c – швидкість виконання машинних операцій у секунду на обчислювальній системі;

ν_{ren} – кількість типових операцій на відновлення і дешифрування відкритого тексту зображень;

W_{init} – обсяг зображення в бітах;

C_r – коефіцієнт стиску відеоданих;

S_{trans} – швидкість передачі даних по ІКСМ.

Встановлено, що найбільш кращою буде та технологія компресії крипто-шифрування, для якої

$$C_r \to max \text{ для } \nu_{oprt} = \nu_{com} + \nu_{ren} \le \nu'_{oprt} \text{ й } \delta_{ren} \ge \delta'_{ren}, \quad (2)$$

де ν'_{oprt}, δ'_{ren} – задані значення відповідно для кількості операцій на обробку й для пікового відношення сигнал/шум.

Аналіз існуючих технологій компресії показує, що забезпечувані ними ступені стиску не задовольняють необхідному рівню компресії. Дані характеристики в середньому на 30 - 50% нижче необхідних значень за ступенем стиску для забезпечення передачі зображень у реальному часі.

Висновки. Проведено аналіз параметрів та характеристик ефективності функціонування ІКС державного призначення з урахуванням методів компактного подання та шифрування ДІР, а також їх інтеграції в ІКС державного призначення.

Представлений набір показників оцінки якості функціонування ІКС повинен забезпечити визначення важливих властивостей інформаційно-комунікаційної системи державних ресурсів в процесі її розробки та експлуатації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1.Бараннік В.В. Методологічні основи криптосемантичного представлення відеозображень в інформаційних комунікаціях / В.В. Бараннік, С.О. Сідченко, В.В. Ларін // Наукоємні технології. – К., 2012 р. – № 3(15). – С. 78-82.

2.Юдін О.К. Інформаційна безпека держави / О.К.Юдін, В.М.Богуш // – К.: МК-Прес, 2005. – С.245-259.

3.Юдін О.К. Інформаційна безпека / О.К.Юдін, В.М.Богуш // – К.: НАУ, 2012 р. – С.468-490.

Одарченко Роман Сергійович, *к.т.н., доцент,*
заступник директора Інституту аеронавігації,
Мачалін Ігор Олексійович, *д.т.н., професор,*
Ткаліч Олег Петрович, *к.т.н., доцент,*
заступник директора Інституту комп'ютерних інформаційних технологій,
Національний авіаційний університет

УДОСКОНАЛЕННЯ СИСТЕМ БЕЗПЕКИ БЕЗПРОВОДОВИХ МЕРЕЖ НОВИХ ПОКОЛІНЬ

У зв'язку з розвитком технологій, а також з появою нових, більш вдосконалених мобільних пристроїв, які надають користувачам більше можливостей, з'являється необхідність у наявності високошвидкісного бездротового інтернет з'єднання [1, 2]. Сучасні смартфони, планшетні ПК, ноутбуки та інші «розумні» пристрої надають користувачам нові можливості. Завдяки цьому з'являється попит на більш швидкісний зв'язок. Так, завдяки цьому, сучасні оператори мобільного зв'язку починають впроваджувати у свої мережі нові технології, які здатні надати абонентам необхідну швидкість з'єднання і якість зв'язку. Однією з таких технологій є LTE (англ. Long Term Evolution – «довготерміновий розвиток»). На даному етапі свого розвитку існує більше трьохсот комерційних мереж LTE. Але, не дивлячись на всі переваги, аналітики розуміють, що на зміну LTE за оцінками експертів після 2020 року мають прийти мережі 5-го покоління – 5G [2]. Вони повинні будуть врахувати всі недоліки мереж попередніх поколінь, в тому числі і систем безпеки. Кожен користувач будь-якої мережі (в тому числі і 4G та 5G) прагне забезпечити конфіденційність передаваних даних та унеможливити спроби мережевих атак на мобільні пристрої.

На рисунку 1 представлені основні напрямки розвитку безпроводових мереж, які відображають як побажання користувачів, так і операторів стільникового зв'язку [2].

Як видно з рис. 1, мережі 5G будуть багато в чому представляти безпроводову глобальну мережу, в якій кожен абонент може бути завжди он-лайн. Тому в цих умовах важливо забезпечити такий рівень захисту самих мереж та даних, які передаються по їх каналам, який задовольнить усіх абонентів стільникових мереж нового покоління.

Таким чином можна сформулювати *мету дослідження*: по-перше необхідно провести аналіз систем безпеки стільникових мереж останнього покоління, які використовується у всьому світі, а по-друге визначити їх недоліки та запропонувати шляхи їх удосконалення.

Об'єктом дослідження є процес захисту передаваних даних в мережах нових поколінь. *Предметом дослідження* є методи удосконалення систем безпеки безпроводових мереж нових поколінь.

Аналіз існуючих проблем систем безпеки мереж 4G. У роботі [2] була наведена порівняльна характеристика систем безпеки безпроводових мереж 4-го покоління, зокрема LTE та WiMAX [3]. Не дивлячись на значну насиченість цих систем захисту, вони мають і деякі свої вразливості. В [2] пропонується розділити можливі атаки на користувачів мереж 4G на ті, які безпосередньо можливі через вразливість систем захисту, та ті, які можливі в мережі Інтернет.

Отже, до першого класу вразливостей відносять [2]:

- Атаки фізичного рівня, такі як глушіння передачі сигналу, що веде до відмови доступу або лавинний наплив кадрів (flooding), що має метою виснажити батарею станції.
- Самозвані базові станції, що пов'язане з відсутністю сертифіката базової станції.
- Уразливість, пов'язана з невипадковістю генерації базовою станцією ключів авторизації.
- Можливість повторно використовувати ключі TEK, чий строк життя вже минув.
- Проблема зв'язана, з небезпекою використання шифрування DES в мережах WiMAX.

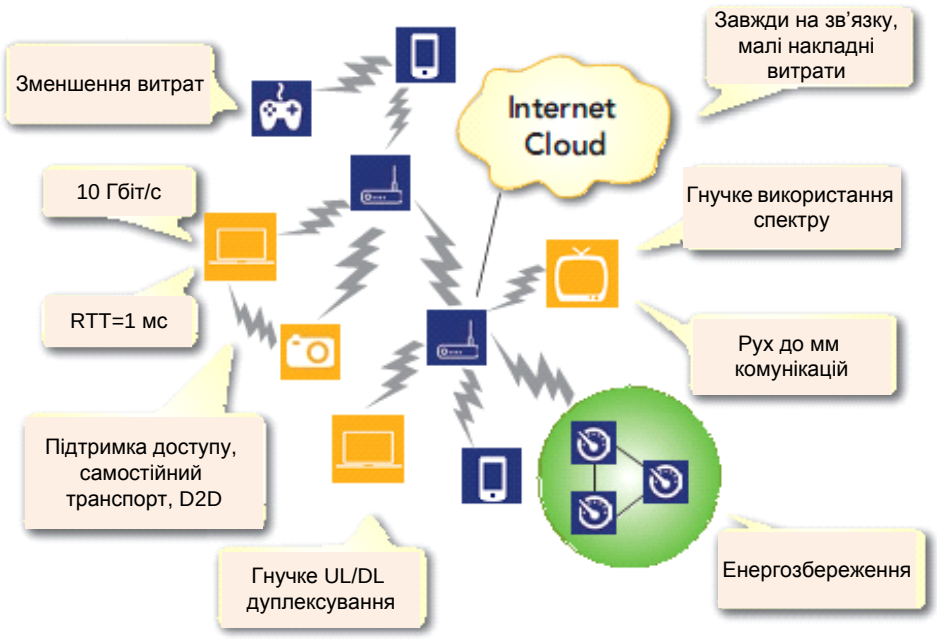


Рис. 1. Шляхи розвитку безпроводових мереж зв'язку

До другого класу вразливостей користувачів мереж 4G слід віднести всі можливі види атак через мережу Internet, адже вона буде одним із основних середовищ спілкування та обміну данними [4]: фрагментація даних; атака Ping flooding; нестандартні протоколи, інкапсульовані в IP; атака smurf; атака DNS spoofing; атака IP spoofing; нав'язування пакетів; Sniffing - прослуховування каналу; Перехоплення пакетів на маршрутизаторі; нав'язування хосту хибного маршруту за допомогою протоколу ICMP; WinNuke; підміна довіреної хоста; Fishing; Whaling.

Наданий перелік зовсім не є вичерпним і постійно оновлюється. Це ще більше актуалізує питання удосконалення систем безпеки безпроводових мереж нових поколінь. На даний момент доволі успішно працює система безпеки мереж LTE. Архітектура системи безпеки в мережах LTE – це структура мережі стандарту LTE, описана в технічних специфікаціях 3GPP TS 33.401 [5] і 3GPP TS 33.402 [6], яка включає набір методів, що дозволяють забезпечити безпечний зв'язок між вузлами мережі, конфіденційність і цілісність даних користувача. Дана архітектура запропонована консорціумом 3GPP в 2008 році [7], а поточною версією є Realease 11.

Основні принципи перевірки достовірності користувачів і шифрування для стільникових мереж були сформульовані ще при розробці мереж GSM. Архітектура мереж наступного покоління UMTS зберегла найкращі параметри безпеки, які використовувалися в GSM і ввела нові. Архітектура мереж LTE сильно відрізняється від схеми, використовуваної в існуючих мережах 3G [8]. Ця відмінність породжує необхідність адаптувати і покращувати механізми забезпечення безпеки. Найбільш важливою вимогою до механізмів безпеки залишається гарантія принаймні того ж рівня безпеки, який вже існує в мережах стандарту 3G [9]. Основні зміни і доповнення, призначені для задоволення нових вимог, були сформульовані наступним чином [10]:

- Ієрархічна ключова інфраструктура, в рамках якої для вирішення різних завдань використовуються різні ключі;
- Поділ механізмів безпеки для шару без доступу, на якому здійснюється підтримка зв'язку між вузлами мережі і мобільним терміналом, і механізмів безпеки для шару з доступом, що забезпечує взаємодію між кінцевим мережевим обладнанням (включаючи набір базових станцій і мобільними терміналами;

- Концепція превентивної безпеки, яка здатна знизити масштаби шкоди, що завдається при компрометації ключів;
- Додавання механізмів безпеки для обміну даними між мережами 3G і LTE.

Таким чином були сформульовані чотири основні вимоги до механізмів безпеки технології LTE [11]:

- Забезпечення такого ж, або більшого рівня безпеки, як в мережах типу 3G, при цьому не доставляючи незручностей користувачам;
- Забезпечення захист від будь-якого типу Інтернет-атак;

- Механізми безпеки для мереж LTE не повинен створювати перешкод для переходу зі стандарту 3G на стандарт LTE;
- Забезпечення можливості подальшого використання програмно-апаратного модуля USIM (універсальна сім-карта).

Таким чином, підсумовуючи вищесказане, можна констатувати, що однією із основних тенденцій розвитку безпроводових мереж є поступовий рух до мереж 5G, запуск яких планується вже до 2020 року. При цьому важливим питанням залишається забезпечення достатнього рівня конфіденційності, доступності та цілісності передаваних даних. Тому необхідно було сформувати основні вимоги до архітектури систем безпеки мереж 5G, які би включили до етапів удосконалення архітектури мереж 4G. Проте, як вже відзначалось, остаточні вимоги та концепція мереж 5G не є до кінця погодженим документом, відповідно до якого слід проводити удосконалення систем безпеки. Тому в роботі були наведені лише вимоги до систем безпеки сучасних стільникових мереж LTE, які займають лідируючі позиції на всьому світовому телекомунікаційному ринку. Саме цих вимог планується дотримуватись та розширювати при удосконаленні систем безпеки стільникових мереж на шляху до 5G. Таким чином, в майбутньому необхідно притримуватись цього основного напрямку досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Одарченко Р.С., Ткаліч О.П. Використання концепції мереж SDN для розподілу трафіку між мережами LTE та Wi-Fi // Наукоємні технології. Науковий журнал НАУ – К.:НАУ, 2014 – Випуск №4 (24)– С.432-437.
2. Одарченко Р.С., Даков С.В. Основні тренди в розвитку безпроводових стільникових мереж // Тези доповідей VIII Міжнародної науково-технічної конференції «Комп'ютерні системи і мережні технології». – К.: НАУ, 2015. – С. 34.
3. Одарченко Р.С., Беженар Ю.В., Ксендзенко А.О. Аналіз вразливостей систем захисту інформації в мережах Wi-MAX та методів їх усунення // Защита информации: Сб. науч. трудов: Випуск 18. − К.:НАУ, 2011. − С. 39 − 44.
4. Офіційний сайт Лабораторії Касперського // www.kaspersky.ru
5. 3GPP System Architecture Evolution (SAE). Security architecture: http://www.3gpp.org/ftp/Specs/html-info/33401.htm
6. 3GPP System Architecture Evolution (SAE). Security aspects of non-3GPP accesses: http://www.3gpp.org/ftp/Specs/html-info/33402.htm
7. SP-39 1.0.0 2008-03-20: http://www.3gpp.org/ftp/Specs/html-info/33401.htm
8. LTE and the Evolution to 4G Wireless. Design and Measurement Challenges, 2010.
9. Security in the Evolved Packet System, Ericsson review no.2/2010pp.4-9.
10. Аналитический обзор защиты данных в сетях LTE По материалам NTT DOCOMO Technical Journal Vol. 11 No. 3: http:// advancedmonitoring.ru/ article/detail. php? ELEMENT_ID=56
11. Security in the Evolved Packet System, Ericsson review no.2/2010. – P. 7. – К.: НАУ, 2012. – С.468-490.

Василиу Евгений Викторович, *д. т. н., профессор,*
Лимарь Игорь Валериевич, *аспирант,*
Одесская национальная академия связи им. А. С. Попова

КВАНТОВАЯ КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА СИСТЕМЫ ЭЛЕКТРОННОГО ГОЛОСОВАНИЯ С ИСПОЛЬЗОВАНИЕМ СХЕМЫ «НЕПРЕРЫВНЫХ ПЕРЕМЕННЫХ»

В недавней публикации [1] была изложена концепция интегрированной системы криптографической защиты процедуры электронного голосования. Это решение основано на совместном использовании квантовых технологий разделения секрета и битового обязательства. Хотя указанная работа основана на самом известном способе квантового разделения секрета – использовании состояний Гринбергера-Хорна-Цайлингера (ГЦХ), предложенная в ней схема имеет значимое ограничение при практической реализации. Это ограничение обусловлено существующим на сегодняшний день техническим ограничением на количество фотонов, способных одновременно находиться в искусственно созданном запутанном состоянии (состоянии ГЦХ). Наибольшее количество таких фотонов, согласно экспериментальным данным [2], равно восьми. С учетом того, что один фотон в схеме разделения секрета должен принадлежать «дилеру» [1], количество членов избирательной комиссии не может превышать семи. Представляется возможным реализовать схему разделения секрета с небольшим (не более 8) числом запутанных фотонов [3]. Однако, такие схемы не обладают рядом преимуществ, отмеченных для схем разделения секрета, основанных на так называемых «непрерывных переменных» [4]. Главным таким преимуществом является возможность необходимого масштабирования схемы разделения секрета без, зачастую, имеющего место при таком масштабировании неприемлемого повышения сложности системы. Эта сложность технических средств при инженерной реализации сопряжена с необходимостью существенного увеличения числа специальных оптических элементов. Построение схем разделения секрета не требующих большого числа связанных квантовой сцепленностью фотонов нередко наталкивается на проблему криптографической стойкости [5]. В тоже время, недавно опубликованное [6] успешное масштабирование системы на основе непрерывных переменных призвано решить указанные выше проблемы ограничения количества сцепленных фотонов и является одним из перспективных направлений исследований.

Ещё одним аспектом, обуславливающим необходимость усовершенствования схемы [1] является непрактичность изначальной идеальной концепции той её части, которая представлена битовым обязательством. Хотя процедура битового обязательства, изложенная в работе [1], полностью соответствует классическим канонам релятивисткой схемы, реализация её в условиях реального избирательного участка сопряжено с рядом технологических сложностей из-за масштабов расстояний. Преодоление этой трудности наряду с реализацией разделения секрета на основе непрерывных переменных приведено ниже.

Также, как и в описанном в работе [1] случае, автоматическое устройство «Алиса» направляет на другое находящееся на избирательном участке устройство «Боб» группу фотонов каждый из которых – в одном из состояний BB84 (Рис. 1). Причём эти состояния формируются случайным образом. Алиса в обязательном порядке фиксирует состояния отправляемых ею Бобу фотонов. Расстояние между устройствами Алиса и Боб не должно превышать 1 м., а сами устройства контролируются независимыми наблюдателями процесса выборов. Каждая группа фотонов соответствует голосованию за каждого отдельного кандидата. Отправка должна быть организована таким образом, чтобы все фотоны отдельной группы достигли Боба одновременно.

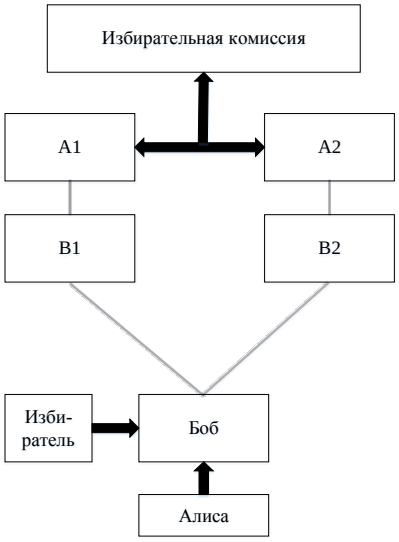


Рис. 1. Общая схема обеспечения информационной безопасности электронного голосования

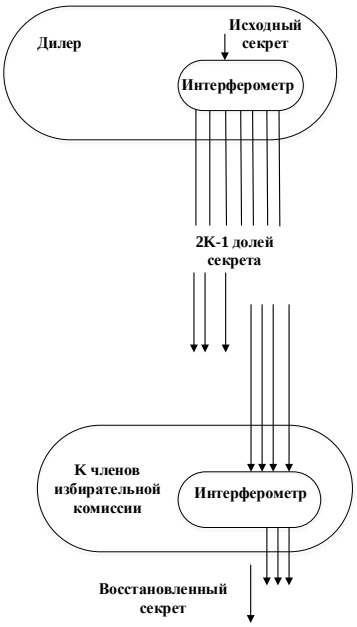


Рис. 2. Общая схема разделения секрета в системе электронного голосования

Однако, в отличие от схемы описанной в работе [1] выбор Бобом измерительного базиса осуществляется не в зависимости от результата голосования («за» или «против»), а – случайным образом [7] и обозначается b. Боб может осуществить измерение либо в базисе $\{|0\rangle,|1\rangle\}$, либо $\{|+\rangle,|-\rangle\}$, где $|\pm\rangle=(|0\rangle\pm|1\rangle)/\sqrt{2}$. Измерение осуществляется одновременно для всех фотонов группы и сразу же после их получения. Данная процедура должна осуществляться для каждого кандидата из списка голосования. То есть – Алиса должна направить Бобу столько групп фотонов сколько кандидатов значится в списке. После осуществления измерения в каждой группе частиц Боб немедленно и одновременно после завершения измерений и предварительного завершения отдельным избирателем голосования, со скоростью света в зашифрованном виде направляет двум своим агентам B_1 и B_2 как сами группы фотонов так и результат голосования отдельного избирателя. Также в обязательном порядке при отправке каждой порции информации Боб должен сообщить Алисе который по счёту кубит он направил своим агентам. Располагаться агенты B_1 и B_2 должны симметрично от Боба. Расстояние между ними обозначается как d. По истечении отведенного для голосования всеми избирателями времени осуществляется взятие на себя агентами B_1 и B_2 обязательств соответствующих результатам голосования каждым отдельным избирателем за каждого кандидата и отправка их агентам Алисы A_1 и A_2 соответственно. Для этого в фиксированный момент времени t_c агенты B_1 и B_2 одновременно направляют агентам A_1 и A_2 (агент B_1 агенту A_1, а агент B_2 агенту A_2 соответственно) набор битов каждый из которых соответствует голосованию каждым избирателем за каждого отдельного кандидата $b'=b\oplus a$. Здесь a - бит взятого обязательства соответствующий результату голосования, а b - случайно переданный бит. Отметим, что каждый из агентов A_1 или A_2 должен находится на расстоянии не более 1 м. от агента B_1 или B_2 соответственно. Поскольку b', по сути, представляет из себя шифр Вернама, Алиса до раскрытия агентами Боба бита a определить его из b' не может. В то же время Боб и его агенты после передачи информации агентам Алисы уже не имеют возможности отказаться от взятого ими на себя обязательства. В момент времени $t_c+d/2c$, где c - скорость света агенты B_1 и B_2 одновременно раскрывают агентам A_1 и A_2 (каждый своему парному агенту соответственно) как значения a , так и результаты квантовых измерений полученных ими ранее от Боба. Агенты A_1 и A_2 проверяют – совместимы ли результаты квантовых измерений с b. Комплекс агентов A_1 и A_2 и B_1 и B_2 при необходимости также может выполняться в

виде автоматических устройств контролируемых независимыми наблюдателями процесса выборов.

После получения агентами Алисы информации о взятом на себя Бобом обязательстве осуществляется процедура разделения секрета. Используем для этого схему описанную в работе [4]. При использовании схемы разделения секрета на основе решения изложенного в работе [4] число долей на которое делится секрет не соответствует числу членов избирательной комиссии и значимо отличается от такового. А именно – используется пороговая схема (k, $2k$-1), где k – число членов избирательной комиссии, а $2k$-1 – число долей на которое осуществляется разделение секрета (рис. 2.).

Для восстановления секрета каждый из участников процедуры разделения должен иметь доступ к соответствующему порту интерферометра. При этом, для возможности работы с минимально допустимым количеством оптических элементов в целях технологической осуществимости квантово-оптических преобразований подбираются параметры матрицы в уравнении:

$$T = \begin{pmatrix} \alpha & \beta & 0 & \cdots & 0 \\ 0 & \gamma & 0 & \cdots & 0 \\ 0 & 0 & & & \\ \vdots & \vdots & & I & \\ 0 & 0 & & & \end{pmatrix} W \quad (1)$$

где W – оператор состояния луча в интерферометре, α , β и γ - параметры характеризующие настройки интерферометра [4]. При этом вычисляется «минимальная общая сумма сжатия» R_{min} и соответствующий ей параметр γ_0 при котором R принимает минимальное значение. На основе этого осуществляется настройка интерферометра позволяющего восстановить секрет. Параметры α и β изначально известны. Для расчёта необходим параметр κ который выражается как $\kappa \equiv \left(1-\alpha^2-\beta^2\right)/(1-\alpha^2)$. Возможны две ситуации:

1) $\alpha^2+\beta^2<1$ и $\alpha^2+\beta^2<\kappa$

$\alpha^2+\beta^2>1+\beta^2/\alpha^2$ и $\alpha^2+\beta^2>\kappa$

В этом случае R_{min} рассчитывается как $R_{\min}=\left|\ln\left(\kappa\alpha\right)\right|$, а $\gamma_0=\sqrt{k}$.

2) $1\le\alpha^2+\beta^2\le 1+\beta^2/\alpha^2$

$\kappa\le\alpha^2+\beta^2\le 1$

$1+\beta^2/\alpha^2\le\alpha^2+\beta^2\le\kappa$

В этом случае $R_{\min}=\ln\left[\left(\sqrt{\alpha^2+\beta^2}+\left|\beta\right|\right)/\left|\alpha\right|\right]$ и $\gamma_0=\sqrt{\alpha^2+\beta^2}$

Список литературы

1. Василиу Е.В. Схема криптографической защиты системы электронного голосования с использованием протоколов квантовой криптографии / Е.В. Василиу // Міжнародний науково-технічний журнал "Вимірювальна та обчислювальна техніка в технологічних процесах". – 2015. – № 1. – С. 232–236.
2. Yao X.C. Observation of Eight-Photon Entanglement / X.C. Yao, T.X. Wang, P. Xu at al. // Nature Photonics.-2012.-V.6, issue 4.-P.225-228.

3. Bhatia P.S. Experimental Tripartite Quantum State Sharing and Perfect Teleportation of the Two-Qubit Photonic State Using Genuinely Entangled Multipartite States / P.S. Bhatia // Journal of the Optical Society of America B.-2014.-V.31, issue 1.-P.154-163.
4. Tyc T. Efficient Sharing of a Continuous-Variable Quantum Secret / T. Tyc, D.J. Rowe, B.C. Sanders // Journal of Physics A: Mathematical and General.-2003.-V.36, issue 27.-7625.
5. Liu F. Eavesdropping on Multiparty Quantum Secret Sharing Scheme Based on the Phase Shift Operations / F. Liu, Q. Su, Q. Wen // International Journal of Theoretical Physics.-2014.-V.53, issue 5.-P.1730-1737.
6. Yokoyama S. Ultra-Large-Scale Continuous-Variable Cluster States Multiplexed in the Time Domain / S. Yokoyama, R. Ukai, S.C. Armstrong at al. // Nature Photonics.-2013.-V.7, issue 12.-P.982-986.
7. Lunghi, T. Experimental Bit Commitment Based on Quantum Communication and Special Relativity / T. Lunghi, J. Kaniewski, F. Bussieres at al. // Physical Review Letters. – 2013. – Vol. 111.-180504.

Корченко Анна Александровна, *к.т.н., доцент.*
Национальный авиационный университет

ФОРМИРОВАНИЕ ЛИНГВИСТИЧЕСКИХ ЭТАЛОНОВ НА ОСНОВЕ КОРТЕЖНОЙ МОДЕЛИ ДЛЯ СИСТЕМ ВЫЯВЛЕНИЯ ВТОРЖЕНИЙ

Одним из решений обеспечения информационной безопасности являются системы выявления вторжений, основанные на аномальном принципе. Для построения такого рода систем используется метод выявления аномалий, порожденных кибератаками в информационных системах [1]. В этом методе процесс формирования различных эталонов достаточно трудоемкий и практически не формализован, что понижает эффективность его использования.

В связи с этим, целью работы является разработка метода формирования лингвистических эталонов на базе кортежной модели базовых компонент [2], позволяющего формализовать процесс получения эталонов параметров для заданных групп лингвистических переменных конкретной среды окружения при решении задач выявления атак в компьютерных системах.

Метод базируется на кортежной модели формирования набора базовых компонент для выявления кибератак [2, 3], в которой для формализации процесса их формирования вводится множество возможных кибератак $\mathbf{CA}$, которые могут воздействовать на ресурсы информационных систем за определенный временной промежуток τ_f, т.е.: $\mathbf{CA}^{\tau_f} = \{\bigcup_{i=1}^{n} \mathbf{CA_i^{\tau_f}}\} = \{\mathbf{CA_1^{\tau_f}}, \mathbf{CA_2^{\tau_f}}, \ldots, \mathbf{CA_n^{\tau_f}}\}$, n определяет количество возможных кибератак, каждая из которых отображается обобщенным кортежем $\mathbf{CA_i^{\tau_f}} = < CA_i, \mathbf{P_i}, \mathbf{T_i^e}, \mathbf{P_i^{\tau_f}}, \mathbf{DR_i} >$, а формирование лингвистических эталонов реализуется посредством шести базовых этапов.

Этап 1. Формирование подмножеств идентификаторов лингвистических оценок. На этом этапе вводится множество всех возможных идентификаторов лингвистических оценок эксперта $\mathbf{LE} = \{\bigcup_{l=1}^{c} LE_l\} = \{LE_1, LE_2, \ldots, LE_c\}$, $(l = \overline{1,c})$ и подмножества таких идентификаторов $\mathbf{LE_{ij}} \in \mathbf{LE}$, которые отображают используемые им суждения для

характеристики состояния параметров $\mathbf{P_i}$ [2, 3] при их наблюдении в определенной среде окружения. Таким образом, относительно *j*-го параметра эксперт может применить набор из r_j высказываний (лингвистических оценок), отображаемый подмножеством $\mathbf{LE_{ij}}=\{\bigcup_{k=1}^{r_j} LE_{ijk}\}=\{LE_{ij1}, LE_{ij2}, \ldots, LE_{ijr_j}\}, (k=\overline{1,r_j})$.

Этап 2. Формирование базовой матрицы частот. Для получения такой матрицы вводится множество идентификаторов интервалов **N** и подмножество таких идентификаторов $\mathbf{N_{ij}} \in \mathbf{N}$, которые отображаются как $\mathbf{N_{ij}}=\{\bigcup_{k=1}^{r_j} N_{ijk}\}=\{N_{ij1}, N_{ij2}, \ldots, N_{ijr_j}\}$, $(k=\overline{1,r_j})$. На основе элементов подмножеств $\mathbf{LE_{ij}}$ и $\mathbf{N_{ij}}$ формируется обобщенная таблица оценок, содержимое которой основывается на текущем фиксировании свидетельств (суждений, оценок) эксперта. Далее с использованием обобщенной таблицы оценок по элементам подмножества $\mathbf{LE_{ij}}$ формируется базовая матрица частот.

Этап 3. Формирование производной матрицы частот. На этом этапе создается вектор сумм VS_{ij} по соответствующим столбцам матрицы частот $VS_{ij}=\|vs_{ijq}\|=\|vs_{ij1}, vs_{ij2}, \ldots, vs_{ijr_j}\|=\left\|\sum_{s=1}^{r_j} f_{ijs1}, \sum_{s=1}^{r_j} f_{ijs2}, \ldots, \sum_{s=1}^{r_j} f_{ijsr_j}\right\|=\left\|\bigcup_{q=1}^{r_j}\sum_{s=1}^{r_j} f_{ijsq}\right\|$. Далее из членов VS_{ij} определяем максимальное значение по формуле $vsm_{ij}=\bigvee_{q=1}^{r_j} vs_{ijq}$, которое используется для формирования производной матрицы частот $F_{ij}^{'}=\|f_{ijsq}^{'}\|=(vsm_{ij}/vs_{ijq})\|f_{ijsq}\|, (s,q=\overline{1,r_j})$.

Этап 4 – формирование нечетких термов. На этом этапе вводится множество всех возможных нечетких термов **T** и подмножество таких термов $\mathbf{T_{ij}} \subseteq \mathbf{T}$, которые отображаются как $\mathbf{T_{ij}}=\{\bigcup_{s=1}^{r_j} \underset{\sim}{T}_{ijs}\}=\{\underset{\sim}{T}_{ij1}, \underset{\sim}{T}_{ij2}, \ldots, \underset{\sim}{T}_{ijr_j}\}, (s=\overline{1,r_j})$. Далее необходимо сформировать значения компонент $\underset{\sim}{T}_{ijs}$, для этого по элементам матрицы $F_{ij}^{'}$ строится вектор максимумов $FM_{ij}=\|fm_{ijq}\|=\|fm_{ij1}, fm_{ij2}, \ldots, fm_{ijr_j}\|=\left\|\bigvee_{s=1}^{r_j} f_{ijs1}^{'}, \bigvee_{s=1}^{r_j} f_{ijs2}^{'}, \ldots, \bigvee_{s=1}^{r_j} f_{ijsr_j}^{'}\right\|=\left\|\bigcup_{q=1}^{r_j}\bigvee_{s=1}^{r_j} f_{ijsq}^{'}\right\|$, $(s,q=\overline{1,r_j})$. На основании FM_{ij} сформируем матрицу функций принадлежности $M_{ij}=\|\mu_{ijsq}\|$, каждый элемент которой вычисляется по выражению $\mu_{ijsq}=f_{ijsq}^{'}/fm_{ijs}$. Используя матрицу, определим наборы нечетких термов (чисел) $\underset{\sim}{T}_{ijs}$ на основе выражения

$$\underset{\sim}{T}_{ijs}=\{\bigcup_{q=1}^{r_j} \mu_{ijsq}/x_{ijsq}\}=\{\mu_{ijs1}/x_{ijs1}, \mu_{ijs2}/x_{ijs2}, \ldots, \mu_{ijsr_j}/x_{ijsr_j}\}, \quad (1)$$

где $x_{ijsq} = N_{ijq}^{max} / N_{ijr_j}^{max}$ $(q = \overline{1,r_j})$. Отметим что, нечеткие числа (НЧ) $\underset{\sim}{T}_{ijs}$ $(s = \overline{1,r_j})$ соответственно являются интерпретацией лингвистических высказываний экспертов LE_{ijk} $(k = \overline{1,r_j})$, отображаемых элементами подмножества $\mathbf{LE_{ij}} \subseteq \mathbf{LE}$.

Этап 5 – формирование эталонных НЧ. Для реализации этого этапа воспользуемся подмножеством нечетких (лингвистических) эталонов $\mathbf{T_{ij}^e}$ (см. (13) в [2]), каждое из которых отображает характерные суждения эксперта (см. этап 1) относительно аномальности состояния параметра P_{ij}. Формирование нечетких эталонов основывается на преобразовании соответствующих НЧ (1) из подмножества $\mathbf{T_{ij}} \subseteq \mathbf{T}$ и реализуется посредством трех шагов.

Шаг 1. Преобразование нечетких термов (1) таким образом, чтобы для всех $\underset{\sim}{T}_{ijs}$ было справедливо отношение порядка, т.е. $\forall x_{ijsq}: x_{ijsq} < x_{ijsq+1}$ $(q = \overline{1,r_j - 1})$.

Шаг 2. В каждом $\underset{\sim}{T}_{ijs}$ осуществляется поглощение компонентом $0/x_{ijs}^{min}$ и $0/x_{ijs}^{max}$ соответственно ряда других компонентов согласно выражений $x_{ijs}^{min} = \bigvee\limits_{\substack{q=1 \\ при\ U1}}^{M-1} x_{ijsq}$ и $x_{ijs}^{max} = \bigwedge\limits_{\substack{q=M \\ при\ U2}}^{r_j} x_{ijsq}$, где U_1 ≝ $\forall x_{ijsq} < x_{ijsM} : \mu_{ijsq} = 0$, U_2 ≝ $\forall x_{ijsq} > x_{ijsM} : \mu_{ijsq} = 0$, а x_{ijsM} и M – соответственно мода $\underset{\sim}{T}_{ijs}$ и ее порядковый номер. Далее, с учетом этих преобразований и выражения (1), определим набор промежуточных термов в виде

$$\underset{\sim}{T}'_{ijs} = \{ \mu_{ijs\beta} / x_{ijs\beta}, ..., \bigcup_{q=\beta+1}^{r_j-\gamma} \mu_{ijsq} / x_{ijsq}, ..., \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1} \} =$$

$$\{ \mu_{ijs\beta} / x_{ijs\beta}, \mu_{ijs\beta+1} / x_{ijs\beta+1}, ..., \mu_{ijsr_j-\gamma} / x_{ijsr_j-\gamma}, \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1} \}, \quad (2)$$

где $\mu_{ijs\beta} / x_{ijs\beta} = 0 / x_{ijs\beta} = 0/x_{ijs}^{min}$ и $\mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1} = 0 / x_{ijsr_j-\gamma+1} = 0/x_{ijs}^{max}$, а β и γ – количество поглощенных $0 / x_{ijsq}$ соответственно слева и справа от $x_{ijs(M)}$.

Таким образом, формируются подмножества эталонов

$$\underset{\sim}{T}^e_{ijs} = \{ \bigcup_{q=1}^{r_{js}} \mu^e_{ijsq} / x^e_{ijsq} \} =$$

$$\{ \mu^e_{ijs1} / x^e_{ijs1}, \mu^e_{ijs2} / x^e_{ijs2}, ..., \mu^e_{ijsr_{js}-1} / x^e_{ijsr_{js}-1}, \mu^e_{ijsr_{js}} / x^e_{ijsr_{js}} \} \ (q = \overline{1,r_{js}}), \quad (3)$$

где $\mu^e_{ijs1} / x^e_{ijs1} = \mu_{ijs\beta} / x_{ijs\beta}$, $\mu^e_{ijs2} / x^e_{ijs2} = \mu_{ijs\beta+1} / x_{ijs\beta+1}$, …, $\mu^e_{ijsr_{js}-1} / x^e_{ijsr_{js}-1} = \mu_{ijsr_j-\gamma} / x_{ijsr_j-\gamma}$, $\mu^e_{ijsr_{js}} / x^e_{ijsr_{js}} = \mu_{ijsr_j-\gamma+1} / x_{ijsr_j-\gamma+1}$, r_{js} $(s = \overline{1,r_j})$ – количество компонент в $\underset{\sim}{T}^e_{ijs}$.

Шаг 3. Если при реализации второго шага для выражения (2) $\exists \underset{\sim}{T}'_{ijs}: \{0/x_{ijs}^{min}\} \in \varnothing$ или $\exists \underset{\sim}{T}'_{ijs}: \{0/x_{ijs}^{max}\} \in \varnothing$ (т.е. $\mu_{ijs\beta} \neq 0$, $\mu_{ijsr_j-\gamma+1} \neq 0$), то для таких термов дальнейшее формирование подмножества $\underset{\sim}{T}^e_{ijs}$ осуществляется путем расширения $\underset{\sim}{T}'_{ijs}$ посредством введения дополнительных $\mu_{ijs\beta-1} / x_{ijs\beta-1}$ и $\mu_{ijsr_j-\gamma+2} / x_{ijsr_j-\gamma+2}$ после чего компоненты НЧ

заново индексируются, начиная с $q=1$. С учетом этого, наборы промежуточных термов будут иметь следующий вид:

$$\underset{\sim}{T}'_{ijs}=\{\mu_{ijs\beta-1}/x_{ijs\beta-1},\mu_{ijs\beta}/x_{ijs\beta},...,\bigcup_{q=\beta+1}^{r_j-\gamma}\mu_{ijsq}/x_{ijsq},...,$$

$$\mu_{ijsr_j-\gamma+1}/x_{ijsr_j-\gamma+1},\mu_{ijsr_j-\gamma+2}/x_{ijsr_j-\gamma+2}\}=$$

$$\{\mu_{ijs\beta-1}/x_{ijs\beta-1},\mu_{ijs\beta}/x_{ijs\beta},...,\mu_{ijsr_j-\gamma+1}/x_{ijsr_j-\gamma+1},\mu_{ijsr_j-\gamma+2}/x_{ijsr_j-\gamma+2}\},$$

где $x_{ijs\beta-1}=x_{ijs\beta}$, $x_{ijsr_j-\gamma+2}=x_{ijsr_j-\gamma+1}$, а $\mu_{ijs\beta-1}=\mu_{ijsr_j-\gamma+2}=0$.

Таким образом, компоненты подмножества эталонов $\underset{\sim}{T}^e_{ijs}$ в выражении (3) будут определятся как $\mu^e_{ijs1}/x^e_{ijs1}=\mu_{ijs\beta-1}/x_{ijs\beta-1}$, $\mu^e_{ijs2}/x^e_{ijs2}=\mu_{ijs\beta}/x_{ijs\beta}$,…, $\mu^e_{ijsr_{js}-1}/x^e_{ijsr_{js}-1}=\mu_{ijsr_j-\gamma+1}/x_{ijsr_j-\gamma+1}$, $\mu^e_{ijsr_{js}}/x^e_{ijsr_{js}}=\mu_{ijsr_j-\gamma+2}/x_{ijsr_j-\gamma+2}$.

Этап 6. Визуализация лингвистических эталонов. Реализация этого этапа основывается на построении геометрического образа всех эталонных НЧ (3) принадлежащих подмножеству $\mathbf{T^e_{ij}}$. Геометрическое место точек на плоскости определяется посредством ломаной соединяющей точки, отображающие компоненты НЧ $\underset{\sim}{T}^e_{ijs}$ в порядке возрастания их суппортов.

Предложенный в работе метод формирования лингвистических эталонов на базе кортежной модели базовых компонент для систем выявления вторжений, за счет использования множеств идентификаторов лингвистических оценок и идентификаторов интервалов, базовой и производной матрицы частот, дает возможность отображать суждения эксперта для характеристики текущего состояния параметров относительно кибератаки, формировать на заданных интервалах частоты встречаемости экспертных оценок и построения подмножеств нечетких термов, что позволяет формализовать процесс получения эталонных значений параметров заданных групп лингвистических переменных, характеризующих конкретную среду окружения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Стасюк А.И. Метод выявления аномалий порожденных кибератаками в компьютерных сетях / А.И. Стасюк, А.А. Корченко // Захист інформації. – 2012. – №4 (57). – С. 129-134.

2. Корченко А.А. Кортежная модель формирования набора базовых компонент для выявления кибератак / А.А. Корченко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2014. – В.2 (28). – С. 29-36.

3. Корченко А.О. Модель базових компонент для виявлення кібератак на ресурси інформаційних систем / А.О. Корченко // Актуальні проблеми управління інформаційною безпекою держави: VI наук.-практ. конф. : Тези доп. – Київ: НА СБ України, 19 березня 2015 року – С. 274-275.

Кищенко Виталий Васильевич, *ассистент,*
Рябый Мирослав Александрович, *к.т.н.,*
Национальный авиационный университет

ОСОБЕНОСТИ ЗАЩИТЫ КРИТИЧЕСКИХ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОТ СПАМА: КЛАССИФИКАЦИОННЫЙ ПОДХОД

Информация является динамическим объектом, образующимся в момент взаимодействия объективных данных и субъективных методов. Как и всякий объект,

информация обладает свойствами. На свойства информации влияют как свойства данных, так и свойства методов, взаимодействующих с данными в ходе информационного процесса. По окончании свойства процесса свойства информации переносятся на свойства новых данных, то есть свойства методов могут переходить на свойства данных. Классификация критически важной информации в сетях, и в частности в сети Интернет, позволяет решать различные задачи, например: документооборот, автоматическое реферирование, машинный перевод, составление Интернет-каталогов, ограничение области поиска в поисковых системах, определение кодировки и языка текста, классификация новостей и т.д.

Иерархический метод. Учтя задаваемую определенным образом процедуру создания классификационной структуры, перед началом работы требуется знание признаков, при наличии которых объект относится к какому-то классу. Эти признаки и будут признаками классификации. Иерархический метод классификации подразумевает, что любой объект на каждом уровне относится к одному классу, характеризуемым конкретным значением своего классификационного признака.

Фасетный метод. В отличие от иерархического метода классификации, данный метод выбирает независимые друг от друга классификационные признаки, так и от семантических связей классифицируемых объектов. Такие классификационные признаки называют фасетами. В любом фасете имеется множество однородных значений конкретного признака классификации. Отметим, что они могут находится в фасете произвольным образом, но обычно их упорядочивают. Фасетная система классификации создается как массив (таблица). Имена столбцов назначают выбранным признакам классификации, или фасетам. В любом элементе таблицы содержится заданная величина фасета. Классификационная процедура выполняет присваивание всем элементам по отдельности конкретного значения из фасетов.

Дескрипторный метод. При проведении информационного поиска работая с тезаурусами (словарями), достаточно часто применяется дескрипторная (описательная) классификационная система. Это связано с тем, что ее языковые средства близки к языку описания информационных объектов. Наиболее часто этот метод применяют в библиотечной поисковой системе.

Многомерная классификация. Главным критерием корректности при создании систем классификации служит биективное отображение, заданное на множестве объектов и действующее на множество систем классификации. Другими словами, однозначное задание объекта (идентификация) и непротиворечивое задание множества свойств этого объекта. Решая эту задачу, мы зададим множество классифицируемых объектов классификации набором точек в конечномерном пространстве. Координатные оси будут соответствовать независимым классифицирующим признакам. Само пространство будет или дискретным, или частично непрерывным. В этом случае можно говорить о каких-то «непрерывных» свойствах. После этого, задав значения на координатных осях, получаем многомерный классификатор.

Одной из важнейших проблем, встающей практически перед каждым пользователем Интернет, является борьба со спамом, то есть задача фильтрации (классификации) поступающей информации. Кроме того, в связи с бурным ростом объема информации в сети Интернет поисковые машины стали основным средством для эффективного доступа к ней. Задача поисковой машины – на каждый поисковый запрос выдавать ранжированный набор страниц, наиболее соответствующих запросу. Мера соответствия страницы запросу, называемая релевантностью, вычисляется на основе характеристик страниц и запросов. Некоторые владельцы сайтов пытаются повлиять на работу поисковых машин, чтобы повысить релевантность страниц. Это явление получило название поискового спама. В настоящее время существуют технологии создания фильтров-сервисов отсекания навязываемой информации. Их принято разделять на два класса: настраиваемые вручную и автоматизированные.

Кроме этого, информация может быть классифицирована следующим образом: по объекту – показатели качества товара, его ресурсоемкость, параметры инфраструктуры рынка, организационно-технического уровня производства, социального развития коллектива, охраны окружающей среды и т.д.; по принадлежности к подсистеме системы – информация по целевой подсистеме, научному сопровождению системы, внешней среде системы, обеспечивающей, управляемой и управляющей подсистемам; по форме передачи – вербальная (словесная) информация и невербальная; по изменчивости во времени – условно-постоянная и условно-переменная (недолговечная); по способу передачи – спутниковая, электронная, телефонная, письменная и т.д.; по режиму передачи – в нерегламентные сроки, по запросу и принудительно в определенные сроки; по назначению – экономическая, техническая, социальная, организационная и т.д.; по стадиям жизненного цикла объекта – по стадии научно-исследовательских и опытно-конструкторских работ, организационно-технологической подготовке производства и т.д.; по отношению объекта управления к субъекту – между фирмой и внешней средой, между подразделениями внутри фирмы по вертикали и горизонтали, между руководителем и исполнителями, неформальные коммуникации.

Чернявський Олександр Сергійович,
МТУ «Миколаївська політехніка»

ЗАСТОСУВАННЯ ПАРОЛЬНИХ СИСТЕМ АУТЕНТИФІКАЦІЇ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ

Парольний захист, як найбільш поширений механізм аутентифікації [1], відзначається традиційністю та відносною простотою реалізації, оскільки механізми парольного захисту є звичними для більшості користувачів комп'ютерних систем (КС) і не викликають психологічного несприйняття – на відміну, наприклад, від сканерів малюнка сітківки ока, та їхня реалізація зазвичай не вимагає залучення додаткових апаратних засобів [2].

Для парольних систем захисту характерний парадокс, що ускладнює їх ефективну реалізацію: стійкі паролі мало придатні для використання людиною. Дійсно, стійкість пароля прямо пропорційна його складності. Однак чим складніший пароль, тим важче його запам'ятати, і у користувача з'являється спокуса записати незручний пароль, що створює додаткові канали для його дискредитації.

В загальному випадку, пароль може бути отриманий зловмисником:

1) ***За рахунок використання людського фактору*** при допомозі:
   - підглядування,
   - підслуховування,
   - шантажу,
   - загроз,
   - використання чужих облікових записів.
2) ***Шляхом підбору*** при застосуванні:
   - повного перебору, що дозволяє підібрати будь-який пароль незалежно від його складності, проте час, необхідний для реалізації даної атаки, для стійкого пароля буде досить значним і логічно припустити, що він буде суттєво перевищувати допустимі ресурси часу, наявного у зловмисника,
   - підбору по словнику, оскільки значна частина паролів, що використовуються на практиці, є осмисленими словами або виразами, крім того існують словники найпоширеніших паролів, які у багатьох випадках дозволяють обійтися без повного перебору.
3) ***Застосуванням інтелектуального методу підбору*** з використанням відомостей про користувача, який грунтується на тому факті, що якщо політика безпеки КС передбачає

самостійне призначення паролів користувачами, то в переважній більшості випадків у якості паролю буде обрана якась персональна інформація, пов'язана з системним користувачем. І хоча такою інформацією може бути вибрано що завгодно, від дати народження коханої людини і до прізвиська улюбленого песика, наявність певної інформації про користувача дозволяє перевірити найбільш поширені варіанти (дні народження, імена дітей, близьких родичів і т.д.).

4) ***Використанням недоліків реалізації парольних систем***, до яких відносяться експлуатовані уразливості мережевих сервісів, що реалізують певні компоненти парольної системи захисту або ж незадекларовані можливості відповідного програмного або апаратного забезпечень.

Очевидно, що при побудові системи парольного захисту необхідно враховувати специфіку КС, керуватися результатами проведеного аналізу ризиків та виконувати наступні практичні рекомендації:

- ***Встановлення мінімальної довжини пароля***. Очевидно, що регламентація мінімально допустимої довжини пароля суттєво ускладнює для зловмисника реалізацію підбору пароля шляхом повного перебору.
- ***Збільшення потужності алфавіту паролів***. За рахунок збільшення потужності (яке досягається, наприклад, шляхом обов'язкового використання спецсимволів) також можна ускладнити повний перебір.
- ***Перевірка і вибраковування паролів за словником***. Даний механізм дозволяє ускладнити підбір паролів за словником за рахунок вибраковування паролів, які можна явно підібрати.
- ***Встановлення максимального терміну дії пароля.*** Термін дії пароля обмежує проміжок часу, який зловмисник може затрачувати на підбір пароля. Тим самим, скорочення терміну дії пароля зменшує вірогідність його успішного підбору.
- ***Перевірка по журналу історії паролів.*** Механізм запобігає повторному використанню паролів–можливо, раніше скомпрометованих.
- ***Обмеження числа спроб введення пароля.*** Відповідний механізм ускладнює інтерактивний підбір паролів.
- ***Примусова зміна пароля при першому вході користувача в систему.*** У випадку якщо первинну генерацію паролів для всіх користувачів здійснює адміністратор, користувачу може бути запропоновано змінити первинний пароль при першому ж вході в систему – в цьому випадку новий пароль не буде відомий адміністратору.
- ***Затримка при введенні неправильного пароля.*** Механізм перешкоджає інтерактивному підбору паролів.
- ***Заборона вибору пароля користувачем і автоматична генерація пароля.*** Даний механізм дозволяє гарантувати стійкість згенерованих паролів, проте варто усвідомлювати, що в цьому випадку у користувачів можуть виникнути проблеми із запам'ятовуванням паролів.

Для оцінки елементарних взаємозв’язків між основними параметрами парольних систем справедливо наступне співвідношення [3]:

$$P = \frac{V * T}{S} \qquad (1)$$

- A – потужність алфавіту паролів;
- L – довжина пароля;
- $S=A^L$ – потужність простору паролів;
- V – швидкість підбору паролів;
- T – термін дії пароля;
- P – ймовірність підбору пароля протягом його терміну дії.

Зазвичай швидкість підбору паролів *V* і термін дії пароля *T* можна вважати відомими. В цьому випадку, задавши допустиме значення ймовірності *P* підбору пароля протягом його терміну дії, можна визначити необхідну потужність простору паролів *S*.

Слід відзначити, що зменшення швидкості підбору паролів *V* зменшує ймовірність підбору пароля. З цього, зокрема, витікає, що якщо підбір паролів здійснюється, наприклад шляхом обчислення хеш-функції і порівняння результату із заданим значенням, то значну стійкість парольної системи забезпечить застосування повільної хеш-функції.

Найбільш поширеними механізмами зберігання паролів в КС є наступні:

1) *У відкритому вигляді*. Безумовно, даний варіант не є оптимальним оскільки автоматично створює безліч каналів витоку парольної інформації. Реальна необхідність зберігання паролів у відкритому вигляді зустрічається вкрай рідко. Зазвичай подібне рішення є прийнятне для систем з низькими вимогами до безпеки і недопустиме в системах, що містять конфіденційну інформацію
2) ***У вигляді хеш-значення.*** Даний механізм зручний для перевірки паролів, оскільки хеш-значення однозначно пов'язані з паролем, але при цьому самі не представляють інтересу для зловмисника.
3) ***В зашифрованому вигляді.*** Паролі можуть бути зашифровані з використанням деякого криптографічного алгоритму, при цьому ключ шифрування може зберігатися:

   - на одному з постійних елементів системи;
   - на деякому носії (електронний ключ, смарт-карта і т.п.), що пред'являється при ініціалізації системи;
   - ключ може генеруватися з деяких інших параметрів безпеки КС – наприклад, з пароля адміністратора при ініціалізації системи.

Висновки.

1. Надано практичні рекомендації для побудови системи парольного захисту з метою забезпечення конфіденційності інформації.
2. Встановлено спосіб підвищення стійкості парольної системи.
3. Запропоновано механізми зберігання з найбільшою ефективністю паролів в КС.

Література.

1. Грушо А.А. Теоретические основы защиты информации/ А. А. Грушо, Е. Е. Тимонина.– М.: «Яхтсмен», 1996. – 187с.
2. Девянин П.Н. Теоретические основы компьютерной безопасности / П. Н. Девянин, О. О. Михальский, А. Ю. Щербаков. – М.: «Радио и связь», 2000. – 190с.
3. Столлингс В. Криптография и защита сетей. Принципы и практика / В. Столлингс, А.Г. Сивак, А.А. Шпак (пер.с англ.). – 2-е изд. – М.; СПб.; К.: Издательский дом "Вильямс", 2001. – 669с.

Обозная Алена Алексеевна, *к.эк.н., доцент,*
МТУ «Николаевская политехника»

ИНСТРУМЕНТЫ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В БАНКОВСКИХ УЧРЕЖДЕНИЯХ

Банковский бизнес неотделим от обработки электронных данных, значительная часть которых содержит конфиденциальную информацию – это данные о клиентах, финансовые отчеты, планы развития, интеллектуальная собственность и т.д. Однако доступ к такой информации, которая предоставляется сотрудникам в рамках утвержденных полномочий, не дает сотрудникам права на ее распространение внутри банка или за ее пределами среди неавторизованных получателей. Распространение сотрудниками конфиденциальной информации представляет серьезную угрозу для банковского бизнеса, так как может

привести к негативным юридическим и финансовым последствиям, а также нанести ущерб деловой репутации банковской компании.

Традиционным подходом к предотвращению утечек конфиденциальной информации является разграничение прав доступа на уровне сетевых файловых хранилищ, систем управления базами данных (СУБД) и других систем хранения информации. Кроме того, в трудовые договоры могут вноситься пункты о неразглашении информации, являющейся конфиденциальной. Тем не менее, утечки корпоративных данных происходят постоянно. Исследования аналитиков показывают, что более 98% инцидентов происходит не по злому умыслу сотрудников, а в процессе выполнения ими текущих стандартных бизнес-процессов, которые часто вступают в противоречие с требованиями политики информационной безопасности.

Для эффективного обнаружения и предотвращения утечек конфиденциальной информации банковским учреждениям требуется внедрение специализированных программных решений DLP (Data Loss Prevention). Особенность систем DLP в том, что они ориентированы не только на информационную безопасность (ИБ), но и на бизнес-требования соответствующих банковских сегментов [1].

По мере развития компьютерных технологий и услуг связи растет число возможных каналов утечки информации. В настоящее время основными каналами утечки являются: веб (веб-почта, форумы, блоги, ftp), электронная почта, печать, средства мгновенного обмена сообщениями (ICQ, Skype, MSN Messenger и т.п.), файлообменные сети, а также интерфейсы компьютеров пользователей. С рабочих мест данные могут передаваться за пределы банков с помощью сменных носителей: флэш-дисков, карт памяти, USB-накопителей, CD/DVD, а также через интерфейсы Bluetooth, Wi-Fi и инфракрасный порт. Сложность технического контроля утечек конфиденциальной информации обусловлена не только множеством каналов, но и разнообразием источников и способов преобразования данных в процессе ежедневной работы. Важные корпоративные данные хранятся в виде записей СУБД, текстовых и графических файлов, прайс-листов, схем, исходного программного кода, файловых архивов различных форматов и т.д. Содержимое файлов может дополняться, фрагменты текста перемещаться, а исходный текст видоизменяться.

Основа любого решения по предотвращению утечек – технология идентификации данных. Большинство известных систем класса DLP применяет лингвистические методы обнаружения и предотвращения утечек с использованием словарей ключевых слов и шаблонов регулярных выражений. На рабочих местах часто используются методы полной блокировки сменных носителей – USB-дисков, карт памяти, а также последовательных и параллельных портов. Также применяются решения на основе меток – все конфиденциальные документы маркируются невидимыми электронными ярлыками, после чего система принимает решение о статусе документа на основе этих ярлыков.

Реализация лингвистических методов контроля представляет собой сложную задачу: требуется проанализировать огромный объем данных и составить эффективные словари ключевых слов и шаблонов, по которым фильтры будут выявлять данные, содержащие конфиденциальную информацию. Словари необходимо проверять в работе и постоянно адаптировать под изменяющиеся данные, чтобы снизить вероятность ложных срабатываний и не перегружать штат сотрудников большим количеством ошибочных инцидентов. Внедрение решений класса DLP, основанных на применении лингвистических методов, является длительным, трудоемким и дорогим процессом и, что самое главное, оказывается в результате недостаточно эффективным, так как процент ложных срабатываний после окончания внедрения может составлять более 25%! Кроме того, с помощью лингвистических методов в принципе невозможно эффективно обнаруживать и предотвращать утечки конфиденциальной информации из баз данных, а также документов, не имеющих смыслового лингвистического содержания (изображения, исходный программный код и т.д.).

Использование меток для маркировки конфиденциальных документов не решает элементарную задачу идентификации содержимого: файл без метки, даже если содержит

важную информацию, будет пропущен анализатором. Например, в результате работы банковской компании создается конфиденциальный документ, снабжаемый меткой. Но в процессе его подготовки на рабочих местах сотрудников оседает множество копий, черновиков и фрагментов текстов, которые впоследствии перемещаются по сети без всякого контроля – технология меток «слепа» по отношению к содержимому. К числу прочих недостатков следует отнести принципиальную необходимость использования агентов на каждом рабочем месте.

Блокирование сменных носителей также может не принести необходимого эффекта. Во-первых, закрывая доступ к сменным носителям, организация теряет гибкость в банковских бизнес-процессах, так как часто сотрудникам требуются сменные носители для копирования информации, не являющейся конфиденциальной (например, презентации, открытые отчеты и т.д.). Во-вторых, сотрудникам, которым предоставляется доступ к конфиденциальной информации, часто разрешается использование сменных носителей. При этом рядовые сотрудники, на компьютерах которых заблокированы сменные носители, могут вообще не иметь доступа к конфиденциальной информации.

Поэтому, для эффективного выбора DLP-решения необходимо провести полнофункциональное тестирование в рамках автоматизированной системы банковского учреждения [2]. Внедряя DLP-систему в банковском учреждении необходимо учитывать:

- принципиальное отличие типов информации и требований к ее защите в зависимости от специфики банковских учреждений;
- инициативу BYOD (Bring Your Own Device);
- налаживание контактов и достижение результатов посредством обмена информацией в онлайн-пространстве неизбежно станет доминирующим видом коллективной работы.

В первую очередь, службам ИБ банков необходимо следовать принципу минимальной достаточности функциональных возможностей DLP-решения реальным требованиям по защите данных в учреждении. Хорошо сбалансированные технические требования позволят снизить полную стоимость владения выбранным решением и обеспечат надежное выполнение корпоративных требований по ИБ. Качественная оптимизация требований предполагает разработку профиля угроз, актуального для конкретной организации. И ко всему прочему, следует добавить момент, связанный с проактивной защитой. В этом могут помочь мониторинг и корреляция событий безопасности, как способ повышения эффективности ИБ.

Особый кумулятивный эффект достигается за счет применения совместно с DLP-системами таких решений, как Security Information and Event Management (SIEM) и Digital Rights Management (DRM). В таком симбиозе системы взаимно дополняют друг друга. Компоненты DLP-системы осуществляют поиск и классификацию защищаемой информации по установленным критериям. В свою очередь, DRM-решение накладывает политики доступа на выявленные файлы, что ограничивает набор операций с ними. А SIEM - формирует «единое окно» для администратора безопасности, в котором сводятся данные о выявленных файлах, подлежащих защите, попытках доступа к ним, а также увязывается технологическая информация, поступающая от операционных систем, СУБД, сетевого оборудования и других источников, формируя полную картину состояния ИБ в банке.

Успешно внедренные в банковских компаниях DLP-системы помогут обнаруживать каналы утечки информации, находить нарушителей, выявлять и корректировать небезопасные бизнес-процессы, получать подтверждения в соответствии со стандартами безопасности, видеть статистику по уменьшению количества инцидентов, укреплять доверие старых партнеров и получать доверие новых клиентов.

ЛИТЕРАТУРА:

1. Кузьмина А.Л. Актуальные направления информационной безопасности банков/ А.Л. Кузьмина // Информационные технологии для менеджмента. – 2014. - № 4-5. – С.52-53.

2. Захист інформації у банківській діяльності / М.М. Браїловський, Г.П. Лазарєв, В.О. Хорошко – К.: ТОВ «ПоліграфКонсалтінг», 2004. – 216 с.

Кошевой Виталий Михайлович, *д.т.н., профессор,*
Шишкин Александр Владимирович, *к.т.н., доцент,*
Одесская национальная морская академия

СОВЕРШЕНСТВОВАНИЕ МОРСКИХ СУДОВЫХ СИСТЕМ НАВИГАЦИИ И РАДИОСВЯЗИ В РАМКАХ РАЗВИТИЯ ЭЛЕКТРОННОЙ НАВИГАЦИИ

На сегодняшний день одним из основных инструментов морской навигации является электронная картографическая навигационная и информационная система (ЭКНИС). Приоритетная роль ЭКНИС в обеспечении безопасности судоходства стала возможной благодаря подключению разнообразных источников навигационной информации и созданию глобального банка электронных навигационных карт. Интеграция ЭКНИС с такими навигационными системами как автоматическая идентификационная система (АИС) и радиолокационная станция (РЛС) с функциями автоматической радиолокационной прокладки обеспечила синэргетический эффект, когда результирующий эффект от объединения превосходит простое сложение возможностей отдельных систем. Типовая схема судовой ЭКНИС с подключениями внешних датчиков представлена на рис. 1 [1, 2].

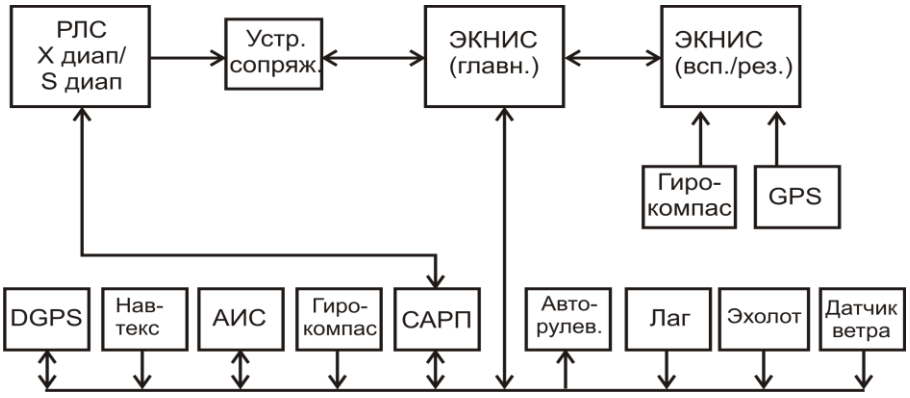


Рис. 1. Структурная схема ЭКНИС с подключениями внешних датчиков

Следующим шагом по нашему мнению в системной интеграции средств навигации и радиосвязи судна является разработка ЭКНИС с поддержкой двунаправленного обмена данными с аппаратурой УКВ ЦИВ. Реализация такого обмена позволяет создать удобный для судоводителя презентационный интерфейс, который в свою очередь устраняет недостатки применяемых в настоящее время средств радиосвязи с использованием аппаратуры ЦИВ. Интеграция систем и обрабатываемый данных является одним из ключевых направлений развития концепции е-навигации (e-navigation), развиваемой Международной морской организацией [3].

Современная ЭКНИС, учитывая ее возможности наложения на электронную карту АИС-отметок и радиолокационного изображения, бесспорно, является важнейшим навигационным инструментом судоводителя. Восприятие одновременно на одном экране АИС-отметок и радиолокационной информации позволяет компенсировать собственные недостатки АИС и РЛС при их раздельном использовании. Так, не все суда могут иметь АИС (или она может быть отключена) и тогда соответствующая реальная цель не будет зафиксирована. В то же время РЛС присущи мертвые и теневые зоны, невозможность наблюдать цели за препятствием или на фоне мешающих отражений. АИС же свободна от этих недостатков и позволяет получить АИС отметки судов, которые не «видит» РЛС.

АИС является судовой навигационной системой, так как ее основное предназначение – это решение именно навигационных задач. Однако принцип ее действия основан на методах и технологиях радиосвязи. Эта система использует УКВ диапазон, выделенный для морской подвижной службы связи (156 МГц – 174 МГц); применяются методы обмена данными, модуляция и кодирование информации, которые являются типичными для систем радиосвязи; в АИС предусмотрено использование режима ЦИВ на 70-канале для назначения рабочих каналов береговой станцией.

В УКВ радиосвязи цифровой избирательный вызов является одной из основных процедур, применяемых для радиосвязи со всеми приоритетами. Тем не менее, как показал многолетний практический опыт, аппаратура ЦИВ в ее сегодняшнем исполнении имеет существенные недостатки. Корректное применение ЦИВ вахтенным офицером-судоводителем сопряжено с выполнением большого числа ручных операций, требующих затрат времени и отвлекающих от решения основной задачи по навигационной безопасности. Причины нарушения процедур радиосвязи с ЦИВ и частое игнорирование его при установлении УКВ радиотелефонного обмена проанализированы в статьях [4, 5].

Интегрированная система УКВ ЦИВ – ЭКНИС/АИС [6-8] позволяет исключить ручную процедуру формирования вызова и заменить ее практически действием click-to-talk (кликни для разговора) АИС отметки судна на электронной карте. В существующих ЭКНИС взаимодействие с УКВ ЦИВ в таком виде не предусмотрено. Поэтому для осуществления двустороннего взаимодействия в ЭКНИС введены функции автоматического формирования вызова в формате ЦИВ и выделения АИС отметки вызывающего судна на электронной карте. Схема ЭКНИС с разработанными модулями (4 - 8) представлена на рис. 2.

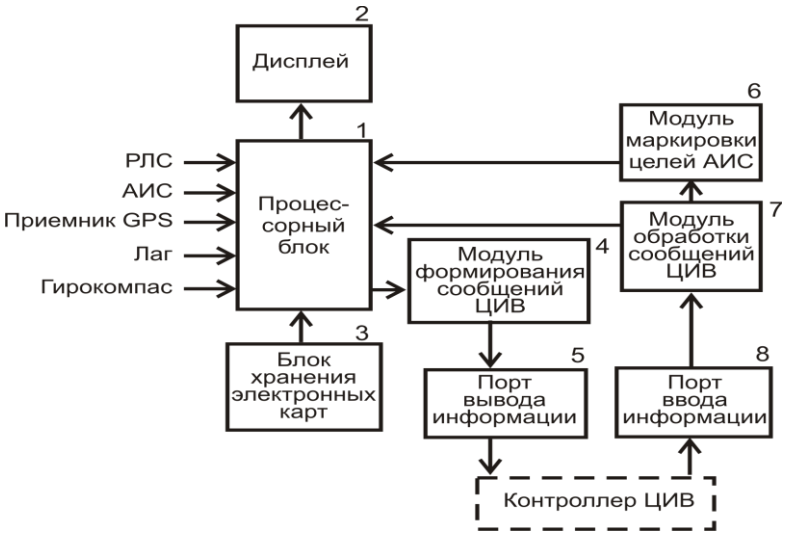


Рис. 2. Разработанная ЭКНИС интегрированной системы навигации - радиосвязи

Принцип двустороннего взаимодействия ЭКНИС – ЦИВ поясняется следующим образом. Вахтенный офицер при необходимости УКВ радиосвязи с каким-либо судном должен первоначально сделать вызов на 70-м канале ЦИВ. Для этого он должен набрать на контроллере ЦИВ как минимум 9-ти значний ИМПС вызываемого судна и номер рабочего канала для последующей голосовой связи, нажать другие функциональные кнопки. В целом вся процедура формирования вызова в существующей системе практически включает в себя три операции, каждая из которых требует определенных затрат времени и переработки рутинных данных. Одной из приоритетных задач е-навигации является представление навигационной информации в виде, удобном для непосредственного восприятия и применения судоводителем. Следует учитывать тенденцию соотношения картографической (chart) и оперативной (operational) информации. Это соотношение в ЭКНИС изменяется в пользу роста оперативной информации. При этом под информацией здесь следует понимать не набор сырых цифровых данных, а ясно воспринимаемые судоводителем представления о

текущей навигационной обстановке. Именно в таком представлении действует разработанная ЭКНИС, освобождая оператора от рутинного ввода данных, заменяя их простыми действиями на дисплее ЭКНИС.

Разработанные приложения к ЭКНИС не влияют на работу других функций системы. Также сохраняется выполнение всех функций управления контроллером ЦИВ в штатном режиме. При необходимости формирование вызова ЦИВ может быть выполнено вручную с его панели управления.

Все процедуры радиосвязи с использованием ЦИВ также сохраняются в полном объеме.

Таким образом, реализация ЭКНИС с поддержкой взаимодействия с контроллером УКВ ЦИВ требует по существу разработки только программного обеспечения и может быть осуществлена в рамках действующего конвенционного оборудования навигации и радиосвязи морского судна.

СПИСОК ЛИТЕРАТУРЫ

1. Вагущенко Л.Л. Интегрированные системы ходового мостика. – Одесса: Латстар, 2003. - 169 с.
2. Weintrit A. The Electronic Chart Display and Information System (ECDIS): An Operational Handbook. - CRC Press/Balkema, 2009. - 895 p.
3. Patraiko D., Wake P., Weintrit A.: e-Navigation and the Human Element. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 4, No. 1, pp. 11-16, 2010
4. Кошевой В.М., Шишкин А.В. Повышение эффективности УКВ радиосвязи в интегрированной судовой системе радиосвязи и навигации // Судовождение: Сб. научн. трудов / ОНМА, Вып. 21. – Одесса: «ИздатИнформ», 2012 – С. 129-137
5. M.V. Miyusov, V.M. Koshevoy & A.V. Shishkin “Increasing Maritime Safety: Integration of the Digital Selective Calling VHF Marine Radiocommunication System and ECDIS” / TransNav, International Journal on Marine Navigation and Safety of Sea Transportation, Volume 5 Number 2 June 2011, pp. 159 – 161.
6. Патент 78762 (Україна). Пристрій для цифрового вибіркового виклику з підвищеною оперативністю / Кошевий В.М., Шишкін О.В., Заічко В.С. Опубл. в бюл. № 5, 2007 р.
7. Патент 90497 (Україна). Інтегрована система цифрового вибіркового виклику / Шишкін О.В., Кошевий В.М., Заічко В.С. . Опубл. в бюл. №9, 2010 р.
8. Patent No. : DE 11 2007 003 617 T5 (Germany). Integriertes System eines digitalen Selektivrufs und einer elektronischen nautischen Seekartographie / Shishkin O., Koshevyy V., Zaichko V. Date of Patent : 03.12.2007.

Ткач Юлія Миколаївна, *к.п.н., доцент*
Чернігівський національний технологічний університет

ЯКІСНА ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВНИХ ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДІВ

Забезпечення інформаційної безпеки стало сьогодні стратегічним завданням держави та кожної окремої установи, зокрема державних вищих навчальних закладів. Виконати це завдання можна шляхом управління ризиками. Згідно з міжнародними стандартом ISO 27002:2010 *управління ризиками* передбачає оцінку ризику, оброблення ризику, прийняття і доведення ризику до відома. Виконання зазначених вище заходів дозволить знайти баланс між вартістю засобів захисту інформації й вимогами установи.

Зупинимось на оцінці ризику. Методологія оцінки ризику може бути якісною, кількісною або їх комбінацією. Проведемо якісну оцінку ризиків інформаційної безпеки державного ВНЗ, оскільки, у міжнародному стандарті ISO 27005:2008 зазначено, що саме з цього аспекту у більшості випадків розпочинається оцінка ризику.

Об’єктом дослідження було обрано державний вищий навчальний заклад, оскільки у сучасній літературі достатньо детально викладено різні підходи до дослідження, управління та оцінки ризиків різних галузей, але щодо державних вищих навчальних закладів таких досліджень проводилось недостатньо.

Зауважимо, що ВНЗ, як об’єкту, дослідження притаманний ряд особливостей. Наприклад, публічність, відкритість для відвідувачів, наявність великої кількості різноманітних інформаційних ресурсів, що циркулюють у ВНЗ, непостійність аудиторій (переміщення студентів між заняттями), широкий перелік заходів, що проводяться протягом року, застосування різноманітних інформаційно-комунікаційних технологій тощо. Всі ці процеси досить складно піддаються формалізації.

Пропонуємо застосувати когнітивного підходу до якісної оцінки ризику інформаційної безпеки державного вищого навчального закладу.

Когнітивний підхід дозволяє зрозуміти логіку розвитку системи за умови впливу на неї багатьох взаємозалежних факторів.

Когнітивне моделювання – це один із наукових методів когнітології. Когнітологія (когнітивна наука) [лат. cognitio - пізнання гр. logos - вчення] – міждисциплінарний науковий напрямок, який об'єднує теорію пізнання, когнітивну психологію, нейрофізіологію, когнітивну лінгвістику й теорію штучного інтелекту [3]. Когнітивне моделювання у свою чергу розглядається багатьма авторами як формалізація знань, прийняття рішень на основі образних знань, управління на рівні інтуїтивних знань.

В основі когнітивного моделювання лежить побудова когнітивної карти. Побудуємо модель оцінки ризику інформаційної безпеки діяльності державного вищого навчального закладу за допомогою нечіткої когнітивної карти. Термін «нечітка» означає, що можна визначити не тільки взаємозв’язки між елементами моделі, але і силу їх впливу один на одного.

Когнітивна карта – це знаковий орієнтований граф, у вершинах якого розміщені ключові фактори об’єкта моделювання (концепти), що пов’язані між собою дугами, тобто причинно-наслідковими зв’язками між ними). Ці зв’язки характеризуються ступенем впливу концептів один на одного. При цьому стан кожного концепта описується однією або декількома змінними станами.

У загальному випадку нечітка когнітивна карта являє собою множину:

$$НКК = \{C, F, W\},$$

де C - множина концептів, F - множина зв’язків між концептами, W - множина сили зв’язків.

Ефективність використання нечітких когнітивних карт у якості моделей слабоструктурованих систем обумовлена: можливістю наочного представлення системи або проблеми, що аналізується, відсутністю необхідності попередньої специфікації концептів та їх взаємозв’язків, конструктивністю, наочністю та відносною легкістю інтерпретації з їх допомогою причинно-наслідкових зв’язків (відношень) між концептами [2].

Процес побудови нечітких когнітивних карт для оцінки ризику діяльності вищого навчального закладу можна представити у вигляді послідовності наступних етапів:

- визначення мети,
- визначення списку концептів (факторів), що характеризують інформаційну безпеку вищого навчального закладу (системне дослідження вищого навчального закладу на предмет виявлення інформаційних активів, загроз, вразливостей, видів можливих збитків),
- встановлення взаємозв’язків між кожною парою концептів (факторів) вищого навчального закладу (також визначається сила впливу),
- побудова нечіткої когнітивної карти (побудова графової моделі),

Розглянемо кожен етап побудови когнітивної карти окремо.

Безпосередній список концептів та їх взаємозв’зків визначались шляхом узагальнення оцінок експертів кожного із запропонованих концептів та, як наслідок, відкидання

несуттєвих.

До переліку концептів ВНЗ ми включили наступні: інформаційні активи ВНЗ $\left\{C_m^S\right\}$, загрози інформаційній безпеці ВНЗ $\left\{C_n^L\right\}$, базисні фактори $\left\{C_k^U\right\}$, цільові активи $\left\{C_l^G\right\}$.

Інформаційні активи потребують захисту, оскільки їх втрата загрожує нанести значної шкоди. Ними можуть бути різноманітні бази данних $\left\{C_1^S\right\}$, документи $\left\{C_2^S\right\}$, програмне забезпечення $\left\{C_3^S\right\}$, апаратні ресурси $\left\{C_4^S\right\}$.

Основні загрози інформаційній безпеці - це крадіжка $\left\{C_1^L\right\}$, фальшування $\left\{C_2^L\right\}$, розголошення конфіденційної або комерційної інформації $\left\{C_3^L\right\}$, занесення вірусів $\left\{C_4^L\right\}$, апаратні та програмні збої $\left\{C_5^S\right\}$, корупція $\left\{C_6^S\right\}$.

Базисні фактори впливають на діяльність установи, тобто у ВНЗ, цими факторами може бути емоційно-психологічний стан колективу $\left\{C_1^U\right\}$, порушення графіку навчального процесу $\left\{C_2^U\right\}$, рівень успішності студентів $\left\{C_3^U\right\}$.

Цільові фактори визначають стан процесів, що відбуваються у ВНЗ, ці фактори є важливими для його успішного функціонування, вони також здійснюють стабілізуючий вплив на заклад та позитивний вплив на рівень інформаційної безпеки. А саме, репутація $\left\{C_1^G\right\}$, якість освіти $\left\{C_2^G\right\}$, матеріально-технічне забезпечення $\left\{C_3^G\right\}$, запитуваність випускників $\left\{C_4^G\right\}$, кваліфікація професорсько-викладацького складу $\left\{C_5^G\right\}$.

Під час побудови нечіткої когнітивної карти та оцінці ризиків ми використовували метод експертних оцінок. Експертів залучали до визначення списку концептів, встановлення причинно-наслідкових зв'язків та їх сили, а також до визначення переліку змінних, що входять до складу концепта. Експерти, що брали участь у нашому експерименті, мали різні рівні навченості та обізнаності у інформаційній безпеки, але всі добре орієнтувались у проблемах вищої школи. Тому ми обчислювали умовну оцінку значущості кожного експерта:

$$E_i = 0,4E_{сам} + 0,6\frac{\sum_{j=1}^{m} E_{взаєм}}{m-1},$$

де E_i - оцінка значущості i -го експерта, $E_{сам}$ - самооцінка експерта, $E_{взаєм}$ - взаємооцінювання i -го експерта j -м експертом, m - загальна кількість експертів.

З метою визначення сили зв'язку ми скористались методами нечіткої логіки [1]. Такі методи ґрунтуються на нечітких множинах і використовують лінгвістичні величини і висловлювання для опису стратегій прийняття рішень.

Для встановлення сили зв'язку між концептами ми запропонували експертам нечіткі відношення у вигляді лінгвістичних термінів: «сильний» вплив, «середній» вплив та «слабкий» вплив.

У результаті першого етапу формалізації отримаємо знакову когнітивну карту, а на другому етапі, після визначення сили взаємозв'язку між концептами, отримуємо нечітку когнітивну карту.

Таким чином, ми побудували нечітку когнітивні карту з оцінки ризику діяльності вищого навчального закладу (рис.1).

Когнітивна карта, яка представлена на рис. 1, являє собою граф, з множини концептів (вершини) та їх взаємозв'язків (дуги).

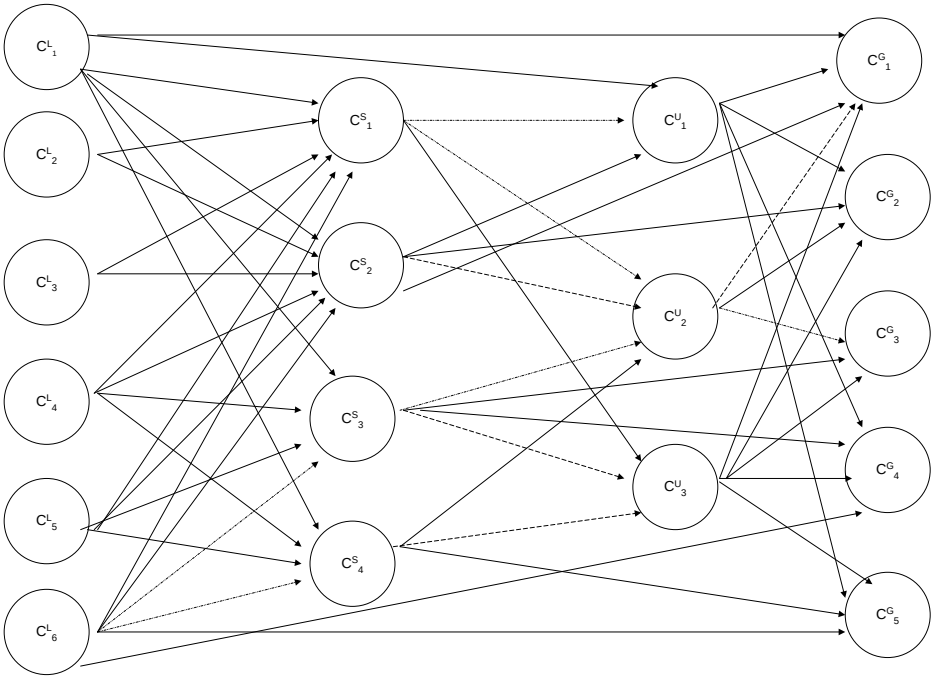


Рис.1. Нечітка когнітивна карта для оцінки ризику інформаційної безпеки державного вищого навчального закладу

Кожна дуга має свою силу зв'язку та відображає думку експертів про вплив концептів один на одного. На рис. 1 «сильний» зв'язок позначено суцільною лінією, «середній» - штриховою, «слабкий» - штриховою з крапочками.

Для того, щоб визначити вплив деякої загрози, наприклад, $\{C_2^L\}$ - фальсифікації на $\{C_2^G\}$ - якість освіти, треба визначити всі непрямі зв'язки між цими концептами. Таким чином,

$$\min(C_2^L \xrightarrow{\text{сильний}} C_1^S \xrightarrow{\text{слабкий}} C_1^U \xrightarrow{\text{сильний}} C_2^G) = "\textit{слабкий}";$$

$$\min(C_2^L \xrightarrow{\text{сильний}} C_2^S \xrightarrow{\text{середній}} C_2^U \xrightarrow{\text{сильний}} C_2^G) = "\textit{середній}";$$

$$\min(C_2^L \xrightarrow{\text{сильний}} C_2^S \xrightarrow{\text{сильний}} C_2^G) = "\textit{сильний}".$$

Отже, повний ефект від впливу фактору C_2^L на C_2^G буде наступним:

$$\max(\textit{слабкий}, \textit{середній}, \textit{сильний}) = "\textit{сильний}".$$

Аналогічно визначаємо силу впливу кожного концепта на інший. У результаті отримаємо матрицю сили впливів.

Отже, з метою якісної оцінки ризиків інформаційної безпеки державного вищого навального закладу можна застосувати когнітивне моделювання, зокрема нечіткі когнітивні карти, що дозволить у наочній формі представити загрози та оцінити ступінь їх вплив на різні сфери діяльності вузу. Використовуючи такий підхід, керівництво вищого навчального закладу отримує можливість мінімізувати втрати інформації шляхом здійснення своєчасних контрзаходів.

Список використаних джерел:

1. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: НАУ, 2005. – 336 с.

2. Нечеткая логика: алгебраические основы и приложения: Монография / С.Л. Блюмин, И.А. Шуйкова, П.В. Сараев, И.В. Черпаков. – Липецк: ЛЭГИ, 2002. – 113 с.

3. Раевнева Е.В., Берест Н.М. Когнитивное моделирование для решения задач управления слабоструктурированными системами (ситуациями) // Бизнесинформ. - №5 (2), 2010. – С. 40-43.

Мехед Дмитро Борисович, *к.п.н.,*
Базилевич Володимир Маркович,
Петренко Тарас Анатолійович,
Чернігівський національний технологічний університет

ОЦІНКА РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Захист комп'ютерних даних на підприємстві є однією із самих головних проблем при розробці та використанні сучасних інформаційно-обчислюваних систем. На сьогодні сформовано 3 основні принципи інформаційної безпеки, завдання котрих полягають у: цілісності даних – захист від збоїв, що ведуть до втрати інформації; конфіденційність інформації; доступність інформації для авторизованих користувачів. Сучасне підприємство будь-якого типу не може існувати без інформаційних технологій. Відомо, що біля 70% світового сукупного національного продукту залежать тим або іншим чином від інформації, що зберігаються в інформаційних системах [3].

До основних ризиків втрати інформації можна віднести наступні: несанкціонований доступ, копіювання або зміна інформації, випадкові або умисні дії, що призводять до знищення даних; некоректна робота програмного забезпечення, що призводить до втрати або псування даних пов'язані з помилками в прикладному або мережевому ПО, зараженням мереж вірусами; технічних збоїв систем; помилки обслуговуючого персоналу. Процес захисту інформації на підприємстві повинен включати: формування, управління, поширення і дотримання політики інформаційної безпеки і інших допоміжних політик, які мають відношення до інформаційної безпеки(політика інформаційної безпеки, це політика, що визначає підхід організації до управління інформаційною безпекою); розуміння погоджених поточних і майбутніх вимог бізнесу до безпеки; використання контролів безпеки для виконання політики інформаційної безпеки і управління ризиками пов'язаними з доступом до інформації, систем і послуг; документування переліку контролів безпеки, дій з їх експлуатації і управління, а також усіх пов'язаних з ним; управління постачальниками і контрактами, що потребують доступу до систем та ін [2]. В той же час, інформаційна безпека сьогодні, на більшості великих підприємств, по суті являє собою набір нормативних актів, в яких обмежуються майже всі дії персоналу підприємства, окрім тих, що пов'язані з виконанням їх прямих обов'язків. Робиться це здебільшого через невисоку компетентність працівників, діяльність яких пов'язана з забезпеченням безпеки: адміністратори, керівники служби безпеки, керівники. Така надлишковість заборон знімає з цих осіб відповідальність за порушення безпеки, перекладаючи її на персонал.

Таким чином виникає ситуація, коли всі процеси діяльності підприємства пов'язані з виконанням вимог інформаційної безпеки і ведуть до того, що інформаційна безпека стає вузьким місцем підприємства. В такому випадку негативна роль, яку несе інформаційна безпека може перевищити позитивну і нанести шкоду діяльності підприємства.

Проте, на нашу думку, створення якісної системи інформаційної безпеки допоможе досягти головної її мети – унеможливити доступ сторонніх осіб до не публічної інформації підприємства.

Основні завдання системи захисту інформаційної безпеки підприємства:

1.Унеможливлення несанкціонованого доступу до баз даних, серверів, серверних і інших приміщень. При чому тут йде мова як про програмний захист, так і про апаратний. Велика кількість програмного забезпечення та різноманітних пристроїв дозволяють створених для цих цілей дозволяють досягти цієї мети.

2.Обмеження несанкціонованого доступу з зовнішніх джерел. Знову ж таки йдеться як про захист локальної мережі підприємства так і про фізичний захист інформації.

3.Обмеження несанкціонованого доступу з внутрішніх джерел. Це одне з найважливіших завдань. Адже саме співробітники підприємства є однією з найбільших потенціальних загроз інформаційній безпеці.

Аналізуючи вищезазначене, можна стверджувати, що актуальною є задача визначення показника інформаційної безпеки з метою впровадження ефективних дій для захисту інформації. Нами було запропоновано алгоритм проведення оцінки ризиків на підприємствах малого та середнього бізнесу. Він полягає у наступному:

- ідентифікація активів;
- визначення ризику невідповідності вимогам законодавства;
- розробка моделі загроз;
- процедура кількісного визначення ризиків;
- визначення максимально допустимого рівня ризику.

В процесі ідентифікації активів експерти проводять інтерв'ю з персоналом кожного підрозділу або відділу з метою виявлення використовуваних активів. Активи системи інформаційних технологій є компонентом або частиною загальної системи, в яку підприємство безпосередньо вкладає кошти і які, відповідно, вимагає захисту з боку підприємства. При ідентифікації активів слід мати на увазі, що всяка система інформаційних технологій включає в себе не тільки апаратні засоби, але і програмне забезпечення. При визначенні ризику невідповідності вимогам законодавства слід враховувати, що будь-яка організація, що має інформаційні системи або робота якої пов'язана з використанням інформаційних технологій для ведення бізнесу, повинна дотримуватися державних законів в цій галузі. Невиконання даних вимог може спричинити за собою цивільну, кримінальну, адміністративну, дисциплінарну та іншу передбачену законодавством України відповідальність. Після завершення оцінки загроз складають перелік актуальних ідентифікованих загроз на кожен ідентифікований актив або групу активів, вразливих до цих загроз, а також визначають ймовірність їх реалізації. Весь процес складання переліку актуальних загроз проводиться з використанням теорії графів [5]. Для визначення кількісної оцінки ризиків інформаційної безпеки необхідно визначити актуальність загрози та встановити ймовірність її настання. Наступним кроком є встановлення цінності активу. У разі неможливості визначення точної вартості активів рекомендується визначати їх цінність в діапазоні від 0 до 1, яка буде показувати відношення вартості активу до загальної вартості бізнесу. Дана оцінка проводиться власником підприємства з експертом по оцінці ризиків. Можливість використання організаційних вразливостей проводиться експертним шляхом, аналізуючи застосовувані організаційні заходи захисту інформації. В ході проведення аналізу, усіх організаційних заходів, які виконуються, присвоюється значення «1», в іншому випадку - «0». Всі значення, яким присвоєно значення «1», підсумовуються, інші значення не враховуються. Процедура оцінки ризиків реалізації хоча б однієї загрози ґрунтується на взаємності декількох факторів - ймовірності події, а саме ймовірності реалізації хоча б однієї актуальної загрози, коефіцієнта цінності активу, середньоарифметичного значення коефіцієнтів можливості використання організаційних вразливостей і можливості використання технічних вразливостей і ризику невідповідності вимогам законодавства. Під коефіцієнтом цінності активу розуміють цінність або критичність активу по відношенню до всього бізнесу. Загальна формула визначення ризику реалізації хоча б однієї загрози з усього переліку актуальних загроз з урахуванням наявності вразливостей стосовно конкурентного активу матиме вигляд:

$$R = P_{угр} \cdot R_n \cdot C \cdot \frac{K_o + K_t}{2} \cdot 100\%,$$

де R - чисельна величина ризику реалізації загроз інформаційної безпеки; $P_{угр}$ - ймовірність реалізації хоча б однієї загрози з усього переліку актуальних загроз; R_n - ризик невідповідності вимогам законодавства; C - цінність активу; K_o - ймовірність використання організаційних вразливостей; K_t - ймовірність використання технічних вразливостей.

Допустимим ризиком прийнято вважати такий, який в даній ситуації вважають прийнятним при існуючих суспільних цінностях. Для підприємства малого та середнього

бізнесу рекомендоване значення ризику не повинно перевищувати 5%. Виконання всіх етапів проведення оцінки ризиків інформаційної безпеки підприємства повторюється для кожного типу активу. Отримане значення ризиків необхідно для вироблення рекомендацій щодо зниження їх рівня, а також впровадження ефективних заходів щодо забезпечення інформаційної безпеки підприємства. У разі якщо підсумкове значення ризику менше 5%, то робиться висновок про те, що на підприємстві виконані вимоги по інформаційній. Необхідно періодично проводити переоцінку отриманих результатів. У разі якщо підсумкове значення ризику більш або дорівнює 5%, то робиться висновок про те, що на підприємстві не виконуються вимоги забезпеченню інформаційної безпеки, а також що ризик оцінюваного типу активу підвищений і вимагає негайного прийняття управлінських та технічних рішень. Цього можна досягти за допомогою наступного:

1. Можливість прийняття ризиків керівником бізнес-підрозділу підприємства, який виконує певні комерційні операції, які залежать від дотримання вимог інформаційної безпеки.

Дуже часто виникають задачі, які потрібно швидко вирішити. В такій ситуації зволікання та бюрократична тяганина можуть нанести не тільки фінансовий збиток підприємству, але й погіршити репутацію. В даному контексті можливість прийняття ризиків керівником є вкрай важливою.

2. Побудова списку критичних ресурсів підприємства і побудова додатково захищеного прошарку між ними та усіма іншими елементами системи.

Тут мова йде в першу чергу про захист локальної мережі підприємства від зовнішніх впливів та створення так званої «демілітаризованої зони» із використанням брандмауерів та іншого програмного забезпечення. Решту ж системи достатньо обмежити штатними засобами антивірусів, політик доменної безпеки, але без зменшення функціональності, що дозволить усім співробітникам в повному обсязі виконувати свої функції без можливості нанести шкоду системі інформаційної безпеки підприємства. До списку критичних ресурсів можуть входити: сервер електронної пошти, файловий сервер, сервера бухгалтерії, веб-сервер підприємства, тощо.

3. Спрощення погодження діяльності працівників підприємства пов’язаних із порушенням обмежень встановлених інформаційної безпеки підприємства.

Список використаних джерел:

1. Корченко А. Г. Анализ и оценивание рисков информационной безопасности / Корченко А.Г., Архипов А.Е., Казимирчук С.В. – К.:ООО «Лазурит-Полиграф», 2013.– 275 с.
2. Мехед Д. Б. Захист інформації на підприємстві / Д. Б. Мехед // Вісник Чернігівського державного технологічного університету. Серія : «Технічні науки» : науковий збірник / Черніг. нац. технол. ун-т. – Чернігів : Черніг. нац. технол. ун-т, 2014. – No 2 (73). – С. 143 – 149.
3. Інформаційна безпека підприємства як елемент економічної безпеки Третя науково-практична конференція з міжнародною участю «Актуальні питання організації та управління діяльністю підприємств у сучасних умовах господарювання», 22 листопада 2013 р. – Харків, 2013. – С.21-23
4. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. — Харків: Вид. ХНЕУ, 2009. — 352 с.
5. Ткач Ю. М. Побудова нечітких когнітивних карт для оцінки інформаційних ризиків вищого навчального закладу. / Ю. М. Ткач // Вісник Чернігівського державного технологічного університету. Серія : «Технічні науки» : науковий збірник / Черніг. нац. технол. ун-т. – Чернігів : Черніг. нац. технол. ун-т, 2014. – No 2 (73). – С. 149-153.

Козловський Валерій Валерійович, *д.т.н., професор,*
Міщенко Андрій Віталійович, *к.т.н., професор,*
Національний авіаційний університет

МЕТОДОЛОГІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В АВІАТРАНСПОРТНОМУ КОМПЛЕКСІ

В сучасному світі постає проблема інформаційної безпеки в авіатранспортному комплексі. Такі проблеми відносять до основних задач менеджменту та економіки інформаційної безпеки - наукової організації складних процесів по критерію максимально ефективного функціонування системи за призначенням та тендерних задач ресурсної оптимізації процесів поточного типу. На кожному етапі цих процесів існує імовірність порушення інформаційної безпеки тому і постає необхідність у пошуку оптимальних рішень для захисту. До процесів «поточного» типу відносять неперервну послідовність (комплекс) різнорідних операцій «обробки» потоку однорідних одиниць основного ресурсу («засобу») для переведення кожної з початкового у потрібний стан – це так званий «конвеєрний» процес.

Головне завдання будь-якої авіатранспортної інфраструктури – прийняти адекватне рішення щодо необхідності і захищеності в конкретних мінливих умовах. Сьогодні це стало дедалі складніше, оскільки все важче стало спрогнозувати, оцінити, яким чином Ваше рішення вплине на розвиток усієї проблемної системи. Тому сьогодні науковці знаходяться в пошуці методології, яка б адекватно оцінювала слабкоструктуровані системи та ОПР як особистість: зі своїм світобаченням, досвідом та інтуїцією. Аналізуючи багатосторонню полеміку щодо питання формування інформаційної безпеки АТК, можна стверджувати, що його суть полягає в тому, щоб найскладніші проблеми і тенденції розвитку системи відобразити в спрощеному вигляді в моделі, досліджувати можливі сценарії виникнення кризових ситуацій, знайти шляхи та умови їх вирішення завдяки роз’язку задач економіки інформаційної безпеки. В першу чергу це забезпечує розумне використання ресурсів, які задіюються в організації комплексної безпеки.

Основною ціллю формування інформаційної безпеки АТК є формування та уточнення гіпотези щодо функціонування досліджуваного об’єкту, що розглядається як слабкоструктурована система, яка складається з окремих внутрішніх і зовнішніх елементів, підсистем, що взаємодіють одне з одним, на основі структурної схеми причинно-наслідкових зв’язків.

Для формування інформаційної безпеки авіатранспортного комплексу необхідно знайти всі можливі способи нападу та можливості їх усунення. Тому для зручності розрахунків потрібно розділити його на етапи, для яких можливе використання основних задач менеджменту та економіки інформаційної безпеки.

Для початку розглянемо можливі варіанти нападу на АТ комплекс. На початковому етапі підготовки засобів до акту застосування можливі втрати інформації про вантаж, його кількість, важливість та можливі засоби його захисту. Також інформація про маршрут, можливі зупинки та способи передбачення і анулювання можливих нападів. На етапі регламентного обслуговування силами забезпечення можливі втрати саме завдяки некомпетентності можливого керівництва. Такий тип втрат інформації зменшується завдяки збільшенню фінансування цього етапу для використання більш висококваліфікованих робітників. Третій етап повністю залежить від фінансування АТ комплексу. Модернізація і відновлення основних засобів захисту та поновлення ресурсів – основні завдання третього етапу.

Проілюструємо застосування елементів методології інформаційної безпеки для оцінки рівня інформаційної інфраструктури в системі, в якій повинні прийматися певні управлінські рішення, щодо розподілу коштів на інформаційну безпеку інфраструктури. Задача побудована на принципі групового характеру підготовки і прийняття управлінських рішень,

необхідно зрозуміти, чим вони зумовлені і наскільки на ті рішення впливають внутрішні уявлення і знання кожного з команди. Велика частина інформації для прийняття управлінських рішень у цій ситуації є невідомою, а частина потребує прогнозу. Команди знають про ціль гри, але важко уявляють, механізм її досягнення. Внаслідок складності процесу підготовки та прийняття рішень в задачах захисту цієї системи, не можливості його обмеження виключно раціональним вибором, вважаємо доцільним використовувати методологію когнітивного моделювання.

Кожний етап потребує багато фінансових вливань, а наша задача пов'язана з необхідністю мінімізувати витрати на кожному етапі життєвого циклу АТ комплексу.Умовою ефективного захисту ресурсу забезпечення є відсутність його простою між «сусідніми» операціями процесу; це означає, що тривалість кожної операції «поточного» процесу (як їх послідовності) при даному ресурсі забезпечення повинна бути однаковою, тобто –

$$\tau_j(y_j)=(\omega_j / y_j)=\tau, j=\overline{1,n}, \quad (1)$$

де n – кількість послідовних операцій процесу для одинці основного ресурсу;

τ_j – тривалість j-ї операції;

ω_j – трудомісткість j-ї операції;

y_j – кількість одиниць спеціалізованого ресурсу забезпечення для захисту j-ї операції;

τ – потрібна тривалість кожної операції поточного процесу.

Для кожного виду ресурсу, наприклад, пасажирських ПС різного класу (різної місткості, дальності та швидкості польоту) визначається потрібність захисту одиниць кожного виду із n –

$$A=\left\langle A_j, j=\overline{1,n}\right\rangle,\ AS=\sum_{j=1}^{n} A_j . \quad (2)$$

З формули бачимо, що для забезпечення кращого захисту ми можемо або зменшити кількість одиниць для захисту, що для нас є небажаним, або проводити модернізацію для укріплення основних пунктів захисту і розширення можливих варіантів спроб нападу, для кращого захисту. Це робить можливим знаходження більш зручних і ефективних способів захисту.

Обстеження ринку m постачальників способів модернізації дає можливість проаналізувати всі можливі варіанти розширення та відтворення інформації:

$$B=\left\langle B_i, i=\overline{1,m}\right\rangle,\ BS=\sum_{i=1}^{m} B_i \quad (3)$$

та ціни на продукцію –

$$C=\left\| c_{ij} \right\|_{m\times n}, \quad (4)$$

де c_{ij} – ціна одиниці ресурсу j-го класу у i-го постачальника .

Планом нападів і захисту є матриця

$$X=\left\| x_{ij} \right\|_{m\times n}, \quad (5)$$

елементом якої x_{ij} є кількість одиниць ресурсу j-го класу, що захищається. Вартість даного плану X –

$$CS(X)=\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}x_{ij} . \quad (6)$$

Виникає наступна («тендерна») задача нападів і захисту даного виду ресурсу – на множині планів *{X}* нападів (стовпчики матриці *X*) і захисту (стрічки матриці *X*), кожний котрих (5) задовольняє умову на можливий об'єм поставок –

$$WS(X) = \sum_{i=1}^{m}\sum_{j=1}^{n} x_{ij} \geq WS, \tag{7}$$

Постає завдання знайти такий (оптимальний) план :

$$X^o = \left\| x_{ij}^o \right\|_{m\times n}, \tag{8}$$

який мінімізує загальну вартість плану (захисту) –

$$CS(X^o) = \min_{\{X\}} CS(X) = \sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij} x_{ij}^o . \tag{9}$$

Це – задача лінійного програмування (ЛП) з матричним аргументом, яка належить до класу «транспортних» задач (ТЗ) ЛП і звичайно вирішується методом «потенціалів» чи симплексним методом. Недоліком симплексного методу для ТЗ є необхідність «розгортання» матричного аргументу у векторний (по стрічкам матриці) [5], що тягне за собою нетривіальні і громіздкі процедури «пере-нумерації» змінних і констант обмежень і цільової функції, породжує розширену матрицю системи з розмірністю на декілька порядків більшою, а ніж у вихідної матриці плану, та з більшістю «нульових» елементів.

Згідно (1), при відомій «трудомісткості» (чи «трудовитратах») операцій процесу –

$$\Omega = \left\langle \omega_j = (y_j \tau_j), j = \overline{1,n} \right\rangle \tag{10}$$

потрібний ресурс захисту для кожної операції (компонента плану розподілу *Y*) знаходиться з очевидного рівняння – обмеження

$$\frac{\omega_j}{y_j} = \tau, j = \overline{1,n}. \tag{11}$$

Остаточно –

$$Y^o = \left\langle y_j^o = (\omega_j / \tau), j = \overline{1,n} \right\rangle. \tag{12}$$

Для обмеження «оберненої» задачі –

$$TS(Y) = \sum_{j=1}^{n} \frac{\omega_j}{y_j} \leq TS^{прип} = (\tau n), \tag{13}$$

тобто для

$$\tau = (TS^{прип} / n), \tag{14}$$

Недоліком як симплексного методу, так і методу «потенціалів» є необхідність введення «фіктивних» постачальників чи замовників при незбалансованості задач по ресурсах, коли не всі нерівності (7) виконуються. Крім того, ітераційна процедура симплексного методу й методу «потенціалів» є повним перебором можливих варіантів покращення поточного плану, тобто не має «градієнтної» евристики.

Тому для вирішення даної задачі ЛП з матричним аргументом найбільш ефективним є ітераційний метод «динамічної ефективності» поточного рішення («динамічної ефективності» ДЕ), який вільний від усіх недоліків відомих методів.

Зміст «питомої ефективності» визначається виразом (19) – це очікувана (умовна для *k*-ої ітерації) продуктивність витрат (при відповідній ціни) на постачання одиниці ресурсу для матриці можливих об'ємів (18). Зрозуміло, що ітераційна процедура методу дозволяє вирішувати задачі з системою (декількома матрицями, як у задачі оптимального

розташування) обмежень; «приріст» значення надається змінній є глобально (по усіх обмеженнях) максимальною ДЕ. Отже, розроблено ітераційну задачу для пошуку і вирішення завдань інформаційної безпеки, яка відрізняється від відомих тим, що зв'язок між факторами АТК розкривається до відповідного рівняння, яке може містити як кількісні (вимірювані) змінні, так і якісні (не вимірюються) змінні, що дає можливість використовувати для аналізу неповну, нечітку і навіть суперечливу інформацію. Набула подальшого розвитку дана ітеративна система аналізу неструктурованих даних, яка на відміну від відомих враховує вплив помилок експерта за допомогою спеціальних програмних модулів і підсистем, що враховують особливості організації людської системи вимірювання, оцінки та переробки суб'єктивної інформації, що дозволило побудувати систему концептуального моделювання і запропонувати технічне рішення, яке може здійснювати безперервний моніторинг стану інформаційної безпеки, породження і перевірки гіпотез механізмів розвитку та механізмів управління інформаційною безпекою.

Таким чином, розглянуті способи знаходження оптимальних рішень для захисту та ресурсної оптимізації процесів поточного типу функціонування авіатранспортного комплексу. Оптимальне рішення прямих й обернених задач надається єдиною аналітичною розрахунковою формулою (5) при обчисленні відповідного значення параметра τ для кожної задачі. Алгоритмічна реалізація наданого методу ресурсної оптимізації процесу даного класу є очевидною (розрахунок по формулах) і тому докладно не розглядається. Окремо відмітимо, що засобом «градієнтного спрямування» наданої ітераційної процедури є саме евристика про динамічну ефективність ДЕ; ітерація потребує перерахування стрічки й стовпчику матриці ДЕ, на відзнаку від повного перерахування симплекс-таблиці. Даний метод не потребує ніяких спеціальних процедур приведення задачі до «регулярної» при будь-яких варіантах незбалансованості по запасах і замовленнях ресурсу і має абсолютну збіжність. Кількість ітерації дорівнює загальної кількості одиниць ресурсу, яка розподіляється, тобто на кожній ітерації розподіляється *1* ресурсу найкращім чином для загального значення цільової функції.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Качинський А.Б. Безпека, загрози, ризик. Наукові концепції та математичні методи. Інститут проблем національної безпеки. Національна академія служби безпеки України. Київ, 2004. – 470 с.

2. Самарский А.А. Гулин А.В. Численные методы. М: "Наука" 1989. – 432с.

3. Справочно - информационный портал: http://www.dic.academic.ru

Корченко Александр Григорьевич, *д.т.н., профессор,*
Казмирчук Светлана Владимировна, *к.т.н., доцент,*
Гололобов Андрей Юрьевич, *аспирант,*
Национальный авиационный университет
Ахметов Бахытжан Сражатдинович, *д.т.н., профессор,*
директор Института информационных и телекоммуникационных технологий,
Казахский национальный технический университет им. К.И. Сатпаева

МЕТОД ИНКРЕМЕНТИРОВАНИЯ ЭТАЛОНОВ ПАРАМЕТРОВ ДЛЯ СИСТЕМ АНАЛИЗА И ОЦЕНИВАНИЯ РИСКОВ

Существующие средства анализа и оценивания рисков информационной безопасности (ИБ), которые основываются на нечеткой логике [1], используют лингвистические переменные (ЛП) с фиксированным количеством терм-множеств, определенных экспертами

на этапе инициализации базовых величин при настройке системы. Для повышения эффективности таких средств в работах [2, 3] были представлены методы n-кратного декрементирования (понижения) числа термов ЛП для трапециевидных и треугольных нечетких чисел (НЧ), которые позволяют уменьшать порядок ЛП без привлечения экспертов соответствующей предметной области. При практическом использовании данных систем возникает необходимость трансформировать эталонны ЛП таким образом, чтобы область их определения расширилась на большее количество термов. В связи с этим актуальным является решение задачи инкрементирования (повышения) числа термов ЛП на основе оценок экспертов, которые использовались на этапе настойки системы. Исходя из актуальности, целью данной работы, является разработка метода трансформирования эталонов посредством однократного инкрементирования (увеличение на один порядок) числа термов ЛП.

Для решения поставленной задачи в качестве ЛП воспользуемся ***DR*** – «СТЕПЕНЬ РИСКА» [1]. Пусть исходная ЛП имеет вид: $\boldsymbol{DR}^{(m)}(\underset{\sim}{T}_{DR_1}^{(m)} = (a_1^{(m)}; b_{11}^{(m)}; b_{21}^{(m)}; c_1^{(m)})_{LR}, \ldots, \underset{\sim}{T}_{DR_j}^{(m)} = (a_j^{(m)}; b_{ij}^{(m)}; b_{ij}^{(m)}; c_j^{(m)})_{LR}, \ldots, \underset{\sim}{T}_{DR_m}^{(m)} = (a_m^{(m)}; b_{im}^{(m)}; b_{im}^{(m)}; c_m^{(m)})_{LR})$, а преобразованная – $\boldsymbol{DR}^{(m+1)}(\underset{\sim}{T}_{DR_1}^{(m+1)} = (a_1^{(m+1)}; b_{11}^{(m+1)}; b_{21}^{(m+1)}; c^{(m+1)})_{LR}, \ldots, \underset{\sim}{T}_{DR_j}^{(m+1)} = (a_j^{(m+1)}; b_{ij}^{(m+1)}; b_{ij}^{(m+1)}; c_j^{(m+1)})_{LR}, \ldots, \underset{\sim}{T}_{DR_{m+1}}^{(m+1)} = (a_{m+1}^{(m+1)}; b_{im+1}^{(m+1)}; b_{im+1}^{(m+1)}; c_{m+1}^{(m+1)})_{LR})$ ($j=\overline{1,m}$, $i=\overline{1,2}$), тогда функцию трансформирования ЛП на плюс один порядок (инкрементирование) обозначим через $FT^{+1}(\boldsymbol{ЛП})$. Например, повышение $\boldsymbol{DR}^{(m)}$ на один порядок позволит расширить возможности использования указанной функции [2] посредством реализации операции трансформирования на +1 порядок:

$$\boldsymbol{DR}^{(m+1)} = FT^{+1}(\boldsymbol{DR}^{(m)}). \quad (1)$$

Так как, ЛП $\boldsymbol{DR}^{(m)}$ представляется НЧ с различными функциями принадлежности (ФП) $\mu(dr)$ [1], а для целей компактного описания такие ФП удобно отображать трапециевидными НЧ вида $\underset{\approx}{X}_{DR_j} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$, где a_j, c_j и b_{1j}, b_{2j} соответственно абсциссы нижнего и верхнего основания трапеции [1] (при $j=\overline{1,m}$), то выражение (1) представим в виде:

$$\begin{gathered}\boldsymbol{DR}^{(m+1)}((a_1,b_{11},b_{21},c_1),(a_2,b_{12},b_{22},c_2),\ldots,(a_m,b_{1m},b_{2m},c_m),(a_{m+1},b_{1m+1},b_{2m+1},c_{m+1})) = \\ FT^{+1}(\boldsymbol{DR}^{(m)}((a_1,b_{11},b_{21},c_1),(a_2,b_{12},b_{22},c_2),\ldots,(a_m,b_{1m},b_{2m},c_m))).\end{gathered} \quad (2)$$

Для реализации заданной функции (2) предлагается метод, который позволяет трансформировать эталоны за счет встраивания дополнительного терма. Метод содержит 4 этапа.

Этап 1. Поиск корректирующих параметров. Для реализации однократного инкрементирования числа термов, которое было ранее установлено экспертным путем, необходимо, соответственно для абсцисс верхнего и нижнего оснований, определить корректирующие параметры по следующим выражениям:

$$\begin{gathered}k_1^{(m+1)} = \frac{\sum_{j=1}^{m}\left(b_{2j}^{(m)} - b_{1j}^{(m)}\right)}{m},\ k_2^{(m+1)} = \frac{\sum_{j=2}^{m}\left(b_{1j}^{(m)} - b_{2\,j-1}^{(m)}\right)}{m-1},\ k^{(m+1)} = k_1^{(m+1)} + k_2^{(m+1)},\ j=\overline{1,m}; \\ l_1^{(m+1)} = \frac{a_2^{(m)} - a_1^{(m)} + \sum_{j=3}^{m}\left(a_j^{(m)} - c_{j-2}^{(m)}\right) + c_m^{(m)} - c_{m-1}^{(m)}}{m},\ l_2^{(m+1)} = \frac{\sum_{j=2}^{m}\left(c_{j-1}^{(m)} - a_j^{(m)}\right)}{m-1},\ l^{(m+1)} = l_1^{(m+1)} + l_2^{(m+1)},\end{gathered} \quad (3)$$

где $k_1^{(m+1)}$, $k_2^{(m+1)}$, $k^{(m+1)}$ и $l_1^{(m+1)}$, $l_2^{(m+1)}$, $l^{(m+1)}$ - корректирующие параметры соответственно для абсцисс верхнего и нижнего основания трапеции, а m - количество исходных терм-множеств.

Этап 2. Определение номера расширяющей вершины. Здесь, необходимо найти расширяющую вершину т.е. такое x_j $(j=\overline{1,m})$ по которому определяется позиция встраивания дополнительного терма. Реализация этого этапа осуществляется с помощью выражения определения расширяющей вершины $x_j = b_{2j}^{(m)} - b_{1j}^{(m)}$ $(j=\overline{1,m})$, номер которой (j) будет отображаться переменной s. Таким образом, поиск номера расширяющей вершины осуществляется посредством определения значения s согласно выражения (4):

$$s = j \; при \left(x_j \le k_1^{(m+1)} \le x_{j+1} \right) или \left(x_j \ge k_1^{(m+1)} \ge x_{j+1} \right), \tag{4}$$

где $k_1^{(m+1)}$ - корректирующий параметр, определяемый посредством (3).

Этап 3. Вычисление значений абсцисс. После нахождения номера расширяющей вершины необходимо определить значения абсцисс нижнего a_j, c_j и верхнего b_{1j}, b_{2j} основания трапециевидных НЧ вида $\underset{\sim}{X}_{DR_j} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$, при $j=\overline{1,m+1}$, т.е. осуществить их переопределение с учетом дополнительного терма. Реализацию этого этапа будем осуществлять с помощью следующих выражений:

$$b_{1j}^{(m+1)'} = \begin{cases} b_{1j}^{(m)} \; при \; j < s+1; \\ b_{2\,j-1}^{(m)} + k_2^{(m+1)} \; при \; j = s+1; \\ b_{1\,j-1}^{(m)} + k^{(m+1)} \; при \; j > s+1, \end{cases} \quad b_{2j}^{(m+1)'} = \begin{cases} b_{2j}^{(m)} \; при \; j < s+1; \\ b_{1j}^{(m+1)'} + k_1^{(m+1)} \; при \; j = s+1; \\ b_{2\,j-1}^{(m)} + k^{(m+1)} \; при \; j > s+1, \end{cases} \quad j=\overline{1,m}, \tag{5}$$

$$a_j^{(m+1)'} = \begin{cases} a_j^{(m)} \; при \; j < s+2; \\ c_{j-2}^{(m+1)'} + l_1^{(m+1)} \; при \; j = s+2; \\ a_{j-1}^{(m)} + l^{(m+1)} \; при \; j > s+2, \end{cases} \quad c_j^{(m+1)'} = \begin{cases} c_j^{(m)} \; при \; j < s \\ a_{j+1}^{(m)} + l_2^{(m+1)} \; при \; j = s; \\ c_{j-1}^{(m)} + l^{(m+1)} \; при \; j > s, \end{cases} \quad j=\overline{1,m}, \tag{6}$$

где m – количество исходных терм-множеств.

Этап 4. Нормирование эталонов. Для завершения процесса однократного инкрементирования, необходимо осуществить нормирование полученных на этапе 3 эталонных значений. Данный этап выполняется посредством 2-х шагов. Отметим, что после реализации этапов 1 и 2 абсциссы верхнего и нижнего основания трапеции были переопределены с помощью выражений (5) и (6). В результате этого они вышли за границы определения эталонов. Для нормирования полученных результатов, необходимо определить соответствующие коэффициенты.

Шаг 1. Формирование нормирующих коэффициентов осуществляется по выражениям (7) и (8), т.е.:

$$k_3^{(m+1)} = \frac{b_{dr}}{b_{2m+1}^{(m+1)'}}, \; l_3^{(m+1)} = \frac{c_{dr}}{c_{m+1}^{(m+1)'}}, \tag{7)-(8}$$

где b_{dr} и c_{dr} соответственно максимальные значения абсцисс верхнего и нижнего основания трапеции.

Шаг 2. Нормирование абсцисс эталонных значений осуществляется с помощью $k_3^{(m+1)}$ и $l_3^{(m+1)}$ по выражениям (9) и (10), т.е.:

$$b_{ij}^{(m+1)} = b_{ij}^{(m+1)'} \times k_3^{(m+1)}; \; a_j^{(m+1)} = a_j^{(m+1)'} \times l_3^{(m+1)}, \; c_j^{(m+1)} = c_j^{(m+1)'} \times l_3^{(m+1)}, \; i=\overline{1,2}, \; j=\overline{1,m} \tag{9)-(10}$$

Для иллюстрации работы метода воспользуемся конкретным примером, где в качестве исходных данных, с учетом возможности дальнейшей верификации, будем использовать эталонные трапециевидные НЧ с равномерным, неравномерным, возрастающим и убывающим типом распределения при m=4. С учетом этого выражение (1) принимает вид: $\boldsymbol{DR}^{(5)}(T_{DR_1}, T_{DR_2}, T_{DR_3}, T_{DR_4}, T_{DR_5}) = FT^{+1}(\boldsymbol{DR}^{(4)}(T_{DR_1}, T_{DR_2}, T_{DR_3}, T_{DR_4}))$,

где $\underset{\sim}{T}_{DR}^{(4)} = \left\{ \bigcup_{j=1}^{4} \underset{\sim}{T}_{DR_j} \right\} = \left\{ \underset{\sim}{T}_{DR_1}, \underset{\sim}{T}_{DR_2}, \underset{\sim}{T}_{DR_3}, \underset{\sim}{T}_{DR_4} \right\} = \left\{ \underset{\sim}{НР}, \underset{\sim}{РС}, \underset{\sim}{РВ}, \underset{\sim}{ПР} \right\}$, $j = \overline{1,4}$, а НР - «Незначительный риск нарушения ИБ», РС - «Степень риска нарушения ИБ средняя», РВ - «Степень риска нарушения ИБ высокая», ПР - «Предельный риск нарушения ИБ» и

$$\underset{\sim}{T}_{DR}^{(5)} = \left\{ \bigcup_{j=1}^{5} \underset{\sim}{T}_{DR_j} \right\} = \left\{ \underset{\sim}{T}_{DR_1}, \underset{\sim}{T}_{DR_2}, \underset{\sim}{T}_{DR_3}, \underset{\sim}{T}_{DR_4}, \underset{\sim}{T}_{DR_5} \right\} = \left\{ \underset{\sim}{НР}, \underset{\sim}{РН}, \underset{\sim}{РС}, \underset{\sim}{РВ}, \underset{\sim}{ПР} \right\}, \quad (11)$$

а НР - «Незначительный риск нарушения информационной безопасности (ИБ)», РН - Степень риска нарушения ИБ низкая», РС - «Степень риска нарушения ИБ средняя», РВ - «Степень риска нарушения ИБ высокая», ПР - «Предельный риск нарушения ИБ».

Как видно при однократном инкрементировании переопределяются не только числовые, а и лингвистические эквиваленты. В примере видно, что добавилось значение РН (см. (11)). Так, как трапециевидные НЧ удобно описывать в виде $\underset{\sim}{X}_{DR_j} = (a_j, b_{1j}, b_{2j}, c_j)_{LR}$, где a_j, c_j и b_{1j}, b_{2j} соответственно абсциссы нижнего и верхнего основания трапеции [1] (при $j = \overline{1,m}$), то выражение (2) представим в виде:

$$DR^{(5)}((a_1,b_{11},b_{21},c_1),(a_2,b_{12},b_{22},c_2),(a_3,b_{13},b_{23},c_3),(a_4,b_{14},b_{24},c_4),(a_5,b_{15},b_{25},c_5) =$$
$$FT^{+1}(DR^{(4)}((a_1,b_{11},b_{21},c_1),(a_2,b_{12},b_{22},c_2),(a_3,b_{13},b_{23},c_3),(a_4,b_{14},b_{24},c_4))).$$

Графическая интерпретация исходных и преобразованных эталонов равномерно распределенных НЧ $\underset{\sim}{T}_{DR}^{(4)}$ и $\underset{\sim}{T}_{DR}^{(5)}$ приведена на рис.

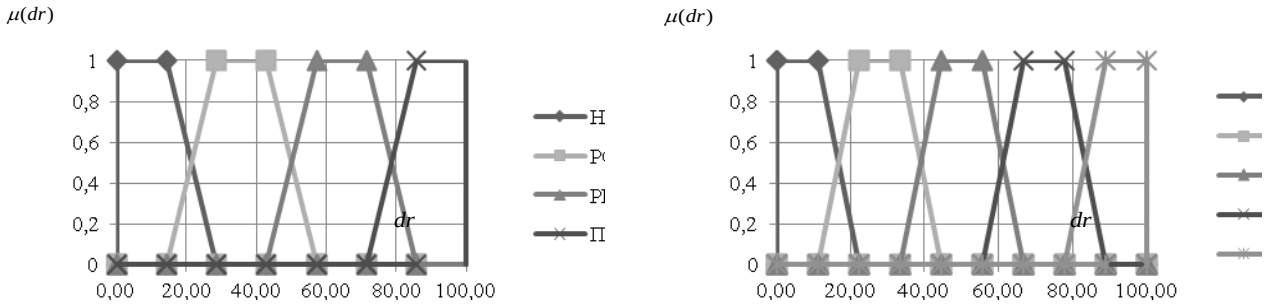


Рис. Термы эталонных значений равномерно распределенных НЧ для ЛП ***DR*** при $\underset{\sim}{T}_{DR}^{(4)}$ и $\underset{\sim}{T}_{DR}^{(5)}$

Таким образом, представленный метод реализации функции трансформирования эталонов ЛП позволяет повысить эффективность работы системы анализа и оценивания рисков ИБ. Это осуществляется посредством решения задачи инкрементирования числа термов трапециевидных НЧ без привлечения экспертов соответствующей предметной области. Для расширения возможностей функции по реализации процесса трансформирования термов, нужно осуществить разработку соответствующих методов, использующих другие классы параметрических НЧ, например, треугольных.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1.Корченко А.Г. Анализ и оценивание рисков информационной безопасности / А.Г. Корченко, А.Е. Архипов, С.В. Казмирчук // Монография. – К.: ООО «Лазурит-Полиграф», 2013. – 275 с.

2.Корченко А.Г. Метод n-кратного понижения числа термов лингвистических переменных в задачах анализа и оценивания рисков / А.Г. Корченко, С.В. Казмирчук, Б.С. Ахметов, А.Ю. Гололобов, Н.А. Сейлова // Защита информации– 2014.– Т.16.– №4, жовтень-грудень.– С.284-291.

3.Казмирчук С.В. Метод n-кратного понижения порядка лингвистических переменных на основе частного расширения базы / С.В. Казмирчук, Б.С. Ахметов, А.Ю. Гололобов, С.А. Гнатюк, Н.А. Сейлова // Безпека інформації. – 2014. – Т.20. –№3. – С. 306-311.

Дудатьєв Андрій Веніамінович, *к.т.н., доцент,*
Дудатьєва Валентина Миколаївна, *асистент,*
Коротаєв Дмитро Олександрович, *аспірант,*
Вінницький національний технічний університет

МЕТОД УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Забезпечення інформаційної безпеки і надійності інформаційної системи, безпеки інформаційних ресурсів , а також всіх інших ресурсів є одним із пріоритетних завдань будь-якого підприємства. Існування інформаційного середовища, у якому відбувається життєдіяльність підприємства і у якому можуть проводитись спеціальні інформаційно-психологічні операції з боку потенційних конкурентів, метою яких є мінімізація впливу або знищення опонентів, говорить про необхідність організації комплексного захисту. При цьому під комплексним захистом маємо на увазі рішення двоєдиного завдання: захисту власних інформаційних ресурсів і захисту від негативного інформаційного впливу конкурентів. Невирішеною проблемою залишається алгоритмізація процесу початку і закінчення інформаційної війни, що накладає певні труднощі при побудові ефективного захисту від негативних інформаційно-психологічних впливів. Крім цього, процес організації комплексного захисту інформаційних ресурсів та процес ведення інформаційної війни супроводжується численними неточностями і невизначеностями, що також впливає на побудову і реалізацію ефективного комплексного захисту.

Для рішення даної проблеми авторами пропонується комплексний комбінований метод управління інформаційною безпекою, який дозволить врахувати зазначені труднощі. Специфіка досліджуваної області така, що запропонований метод повинен бути практично реалізований у вигляді комплексної системи захисту інформації (КСЗІ). Фактично необхідно синтезувати оптимальну і адаптивну КСЗІ, здатну реагувати на зміни як внутрішніх, так і зовнішніх загроз. З метою ефективного оцінювання і забезпечення комплексної інформаційної безпеки доцільно цей процес розглядати на етапах проектування та експлуатації КСЗІ. Створення комплексних систем захисту інформації регламентується відомим переліком нормативних документів, таких як: НД ТЗІ 3.7-003 – 2005 ”Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі”, НД ТЗ 3.7-001-99 “Методичні вказівки щодо розробки технічного завдання на стоворення комплексної системи захисту інформації в автоматизованій системі”, НД ТЗІ 1.4-001 “Типове положення про службу захисту інформації в автоматизованій системі”. Виконання цих нормативних документів, безумовно, гарантує побудову ефективної КСЗІ. Однак, такий підхід дасть нам рішея тільки 1-го завдання, тобто захист власних інформаційних ресурсів, рішення іншого завдання – захист від негативного інформаційно-психологічного впливу – залишається практично невирішеним. Запропонований метод поєднує в собі можливості забезпечення комплексної інформаційної безпеки на етапі проектування і на етапі експлуатації КСЗІ. При цьому на етапі проектування оцінювання та забезпечення комплексної інформаційної безпеки пропонується виконувати з використанням математичного апарату теорії нечітких множин, а на етапі експлуатації з використанням статистичної теорії, яка є методологічною базою для методу «6-сигм». Систематизація послідовності дій метода «6-сигм», відома під абревіатурою DMAIC (define, measure, analyze, control) по суті, являє собою процес алгоритмізації оцінювання поточного і забезпечення необхідного рівня тих чи інших параметрів процесу [1]. Положення методу «6-сигм» пропонується застосовувати на етапі експлуатації, де може бути накопичено достатньо статистики і відповідно адекватно використано апарат математичної статистики.

Стосовно до вирішення завдання оцінювання та забезпечення гарантованого рівня комплексної інформаційної безпеки запропонований метод передбачає виконання послідовності операцій, які виконуються з урахуванням 2-х етапів – етапу проектування та

етапу експлуатації: визначення проблем і цілей, моніторинг, аналіз, підготовка та прийняття рішення, впровадження та супровід.

Визначення цілей проекту на створення КСЗІ, вимог замовника, узгодження всіх питань. **Моніторинг** передбачає своєчасне виявлення загроз, вразливостей, причин їх виникнення як для власних інформаційних ресурсів, так і виявлення можливостей і ознак проведення інформаційно-психологічних операцій з боку конкурентів. **Аналіз** передбачає виявлення причинно-наслідкового зв'язку виникнення та реалізації загрози через використання тієї або іншої уразливості і оцінки ймовірних ризиків, пов'язаних з даним сценарієм розвитку подій. Аналіз загроз обов'язково включає аналіз загроз проведення спеціальних інформаційно-психологічних операцій в різних середовищах. **Підготовка і прийняття рішень** передбачає формалізацію критерія прийняття рішення, формування множини можливих рішень і прийняття остаточного рішення. Ухвалення рішення реалізується у вигляді синтезу оптимальної КСЗІ і розробкою відповідної політики інформаційної безпеки. **Впровадження та супровід** характеризуються організацією контролю за виконанням ПІБ і супроводом роботи системи.

Запропонований метод управління комплексною інформаційною безпекою дозволить забезпечити достатній рівень захищеності як на етапах проектування, так і при експлуатації КСЗІ.

Список літератури:

1. Джордж М.Л. Бережливое производство + шесть сигм в сфере услуг / М.: Л. Джордж. – М.: Альпина Бизнес Букс, 2005. – 402с.

Хохлачова Юлія Євгеніївна, *асистент,*
Національний авіаційний університет

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ КРИТЕРІЇВ ОПТИМАЛЬНОСТІ ТА ОБМЕЖЕННЯ ЗАГРОЗ ІНФОРМАЦІЇ

Побудова математичних моделей критеріїв ефективності (оптимальності) та обмежень є ключовою проблемою в усіх задачах аналізу, синтезу та оптимізації ІС, що розробляються, тому побудова власне процедур формалізації критеріїв та обмежень є важливим та актуальним завданням. З огляду на це, у роботі розроблено відповідну систему правил, що базується на таких принципах: 1) критерії ефективності повинні дозволяти оптимальне керування, тобто готувати та приймати оптимальні рішення, у тому числі й при наявності обмежень; 2) з огляду на те, що у задачах оптимізації обмеження відіграють роль критеріїв, то математичні моделі обмежень конструюють також і моделі критеріїв; 3) будь-яка задача з обмеженнями може бути перетворена у послідовність задач без обмежень, тому для вибору канонічних форм можна використовувати допоміжну функцію Лагранжа як узагальнений критерій оптимальності, який враховує обмеження. Зазначена система правил математичного моделювання критеріїв оптимальності та обмежень будується на необхідних та достовірних умовах існування екстремумів функцій та функціоналів. Розглянемо їх більш детально:

Правило оптимальності. Будь-яка безперервна двічі диференційована функція $OC(cv_1,...,cv_\varepsilon)$ від ε аргументів може бути критерієм оптимальності ОС (optimality criterion) цільової функції, а самі аргументи є керованими змінними cv (controlled variables), якщо для області існування ОС дотримуються необхідні та достатні умови існування екстремумів.

Правило обмеження. Будь-яка безперервна двічі диференційована функція $L(cv_1,...,cv_\varepsilon)$ від ε незалежних аргументів може бути обмеженням (limitation), а самі аргументи є керованими змінними, якщо для області існування L дотримуються необхідні та достатні умови існування екстремумів та задані обмеження у вигляді:

$$L_1(cv_1,...,cv_\varepsilon) = L_1^*,...,L_\mu(cv_1,...,cv_\varepsilon) = L_\mu^*; \quad (1)$$

де μ – число обмежень.

Правило існування. Для того, щоб оптимальне рішення існувало та було єдиним, необхідно щоб число керованих змінних та число обмежень задовольняли умові:

$$\varepsilon > \mu. \tag{2}$$

Правило зведення. У випадках, коли обмеження (1) задані у вигляді нерівностей, оптимізація зводиться до відомих способів введення фіктивних допоміжних змінних. Якщо цільові функції та обмеження можуть мінятися місцями, то в задачах оптимізації повинна виконуватися необхідна умова (2).

Правило допоміжної функції. У задачах оптимізації з обмеженнями за критерій оптимізації використовується допоміжна функція Лагранжа виду:

$$\begin{aligned} AL(cv_1,...,cv_\varepsilon) = OC(cv_1,...,cv_\varepsilon) + (\lambda_1\left[L_1(cv_1,...,cv_\varepsilon) - L_1^* \right] + ... \\ +\lambda_\mu\left[L_\mu(cv_1,...,cv_\varepsilon) - L_\mu^* \right]), \end{aligned} \tag{3}$$

де λ_k – допоміжні невизначені множники Лагранжа, $k = \overline{1,\mu}$.

Правило канонічності. Система з $\varepsilon + \mu$ рівнянь оптимізації:

$$\begin{cases} \dfrac{\partial AL(cv_1,\lambda_1)}{\partial cv_1} = 0,..., \dfrac{\partial AL(cv_\varepsilon,\lambda_\varepsilon)}{\partial cv_\varepsilon} = 0 \\ \dfrac{\partial AL(cv_1,\lambda_1)}{\partial \lambda_1} = 0,..., \dfrac{\partial AL(cv_\mu,\lambda_\mu)}{\partial \lambda_\mu} = 0, \end{cases} \tag{4}$$

може бути подана у канонічній формі виду

$$\begin{cases} \dfrac{\partial AL_1(cv_1,\lambda_1)}{\partial cv_1} = \dfrac{\partial AL_2(cv_1,\lambda_1)}{\partial cv_1},..., \dfrac{\partial AL_1(cv_\varepsilon,\lambda_\varepsilon)}{\partial cv_\varepsilon} = \dfrac{\partial AL_2(cv_\varepsilon,\lambda_\varepsilon)}{\partial cv_\varepsilon} \\ L_1(cv_1,...,cv_\varepsilon) = L_1^*,..., L_\mu(cv_1,...,cv_\varepsilon) = L_\mu^*. \end{cases} \tag{5}$$

Таким чином систему (5) будемо називати першою канонічною формою представлення системи рівнянь оптимізації. Елементи обох частин рівнянь (5) будемо називати типовими елементами першої канонічної форми.

Правило критеріїв. Використання першої канонічної форми (5) системи рівнянь оптимізації дозволяє створювати критерії оптимізації у вигляді сепарабельних адитивних критеріїв:

$$OC(cv_1,...,cv_\varepsilon) = \sum_{i=1}^{\varepsilon}(\int \frac{\partial AL_1(cv_1,...,cv_\varepsilon;\lambda_1,...,\lambda_\mu)}{\partial cv_i} dcv_i - -\int \frac{\partial AL_2(cv_1,...,cv_\varepsilon;\lambda_1,...,\lambda_\mu)}{\partial cv_i} dcv_i), \tag{6}$$

Сепарабельність $OC(cv_1,...,cv_\varepsilon)$ означає, що всі недіагональні елементи матриці других часткових похідних цієї функції дорівнюють нулю.

Правило сепарабельного програмування. Сепарабельну форму та адитивність також зручно використовувати для обмежень виду (5):

$$OC_{1k}(cv_1) + ... + OC_{\varepsilon k}(cv_\varepsilon) = OC_k^*. \tag{7}$$

Задачу оптимізації, у якій критерій оптимізації представлений у вигляді (6), а обмеження у вигляді (7), будемо називати задачею сепарабельного програмування. Якщо $OC(cv_1,...,cv_\varepsilon)$ є випуклою функцією, а $L_k(cv_1,...,cv_\varepsilon)$ – угнутою, існує рішення прямих задач сепарабельного програмування. Для зворотних задач функції $OC(cv_1,...,cv_\varepsilon)$ та $L_k(cv_1,...,cv_\varepsilon)$ повинні володіти протилежними властивостями. Властивості сепарабельності та адитивності дозволяють створювати ефективні обчислювальні алгоритми пошуку оптимальних рішень. Представлення критерію оптимізації у вигляді (6) називається другою канонічною формою постановки задачі оптимізації. У задачах оптимізації при побудові допоміжних функцій Лагранжа (3) критерій та одне з обмежень міняються місцями. При цьому змінюється і характер екстремуму, і вимоги випуклості та вгнутості цільових функцій та обмежень. Доданки суми (6) будемо називати типовими елементами другої канонічної форми.

Запропонована система правил дозволяє створити загальну систему правил математичного моделювання сепарабельних критеріїв оптимізації та обмежень. Вона заснована на виборі типових елементів канонічних форм (5), (6) та методах сепарабельного програмування. Параметри канонічних форм грають роль параметрів сімейства оптимальних рішень, їх зручно використовувати як параметри середовища (зовнішнього оточення) або як параметри, які характеризують взаємодію системи, що розглядається з іншими системами. Для класифікації типових елементів першої канонічної форми (5) корисно використовувати методи аналітичної та диференційної геометрії, які володіють високою наочністю. У ролі типових елементів форм можуть бути обрані алгебраїчні функції (поліноми) q-го порядку, показові, експоненціальні, тригонометричні, трансцендентні та інші.

Система правил дозволяє ввести таку форму представлення системи рівнянь оптимізації, яка названа як "перша канонічна форма математичного моделювання критеріїв та обмежень", причому, за її допомогою інтегральне перетворення (друга канонічна форма математичного моделювання критеріїв та обмежень), дозволяє синтезувати морфологічним методом сепарабельних адитивних критеріїв та обмежень.

Такі математичні моделі критеріїв та обмежень мають ряд явних переваг:

- осмислений вибір керованих змінних та параметрів для пошуку оптимальних рішень, побудова таких критеріїв, які заздалегідь забезпечують виконання необхідних та достатніх умов оптимального управління;
- використання розвинутих методів сепарабельного програмування;
- застосування морфологічного метода синтезу можливих рішень;
- залучення такого мінімального числа вільних параметрів (некерованих змінних), які дозволяють адекватне відображення, в межах заданої точності моделювання, умов функціонування та взаємодії систем, що досліджуються.

Список літератури

1. Ленков С.В. Методы и средства защиты информации. В 2-х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко – К.: Арий, 2008.

2. Горелик В.А. Исследование операций / В.А. Горелик, И.А. Ушаков – М.: Машиностроение, 1986. – 288 с.

3. Вунш Г. Теория систем / Г. Вунш – М.: Сов. радио, 1978. – 288 с.

4. Тиснина Е.О. Абсолютная устойчивость положения равновесия системы поддержки принятия решений в системе защиты информации/ Е.О. Тиснина, В.А. Хорошко // Сучасний захист інформації, №4, 2010. – С. 74-79.

5. Мину М. Математическое программирование. Теория и алгоритмы / М. Мину – М.: Наука, 1990. – 488 с.

6. Хоменюк В.В. Элементы теории многоцелевой оптимизации / В.В. Хоменюк – М.: Наука, 1983. – 343 с.

7. Игнатов В.А. Аксиоматическая теория математического моделирования критериев оптимальности и ограничений / В.А. Игнатов, Ю.Н. Минаев, Н.Н. Гузий // Захист інформації, №4, 2005. – С. 46-56.

Мохор Володимир Володимирович, *д.т.н., професор,*
Максименко Євген Васильович,
Зінченко Ярослав Вікторович, *к.т.н.,*
Цуркан Василь Васильович, *к.т.н.,*
ІСЗЗІ НТУУ «КПІ»

УМОВИ ВИКОРИСТАННЯ СПЕКТРАЛЬНОГО ПІДХОДУ ДЛЯ ОЦІНЮВАННЯ РИЗИКУ БЕЗПЕКИ ІНФОРМАЦІЇ

Спектральний підхід рекомендується використовувати для оцінювання ризику за встановлений інтервал часу на етапі експлуатування системи менеджовування безпекою

інформації. На основі отриманих результатів можливе прийняття рішення про необхідність його обробляння та, як наслідок, вибір відповідних засобів і заходів [1 – 3].

Водночас використанню спектрального підходу передує виконання таких умов [4]:

1.Накопичення статистичних даних про збитки внаслідок реалізації загроз за встановлений інтервал часу для оцінювання як імовірнісних, так і часових та спектральних характеристик ризику.
2.Врахування динаміки зміни ризику шляхом його відображення за допомогою сигналу ризику, дослідження якого дозволить оцінити притаманні йому властивості та характеристики.
3.Встановлення еталонного прийнятного рівня ризику для порівняння визначених оцінок його величини. Цим забезпечується зіставність отриманих результатів при атестуванні ризику та, як наслідок, можливість обробляння неприйнятних оцінок.

Разом з тим, складно стверджувати необхідність чи достатність означеного переліку умов використання спектрального підходу. Це обумовлено, перш за все, нестаціонарністю сфери безпеки інформацій. Тому тільки за результатами дослідження сигналу ризику можна остаточно стверджувати або спростовувати адекватність такого відображення та можливість використання спектрального підходу.

Література:

1. Мохор В.В. Оцінювання ризику безпеки інформації на основі спектрального підходу/В.В.Мохор, Є.В.Максименко, Я.В.Зінченко, В.В. Цуркан // Безпека інформації у інформаційно-телекомунікаційних системах (26 – 28 травня 2015 р.): XVII міжн. наук.-практ. конф.: тези доп. (у друку).
2. Information technology. Security techniques. Information security management systems. Requirements: ISO/IEC 27001:2013. – Second edition 2013-10-01. – Geneva, 2013. – P. 23.
3. Information technology. Security techniques. Information security risk management: BS ISO/IEC 27005:2011. – Second edition 2011-06-10. – Geneva, 2011. – P. 68.
4. Матвеев Б.А. Теоретические основы исследования статистических рисков: монография / Б.А. Матвеев. – Челябинск: Изд-во ЮУрГУ, 2008. – 248 с.

Гнатюк Віктор Олександрович, *аспірант,*
Національний авіаційний університет,
Труфанов Андрій Іванович, *к.ф.-м.н., професор,*
Іркутський державний технічний університет (м. Іркутськ, РФ)

МЕРЕЖЕВО-ЦЕНТРИЧНИЙ ПІДХІД ДО ПРОЦЕСУ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Останнім часом термін «мережево-центричний» все частіше використовується в різних сферах діяльності, пов'язаних з використанням мережевих комп'ютерних технологій у сфері управління. Мережево-центрична концепція виникла у військовому середовищі не стільки в процесі теоретичних досліджень, скільки внаслідок систематичного аналізу результатів впровадження в збройні сили нових бойових засобів і підвищення рівня освіченості особового складу. Метою роботи є розгляд мережево-центричних комп’ютерних методів для управління протидією та ліквідації наслідків різних видів інцидентів інформаційної безпеки.

Протидія виникненню та ліквідації наслідків інцидентів інформаційної безпеки (ІБ) за допомогою засобів, об'єднаних інформаційними мережами в єдину систему, що здійснює проведення операцій, в яких наявні ресурси результативно використовуються в потрібному місці, в потрібний час, здійснюючи принцип масування результатів включає в себе:

1) Постійний комп'ютерний моніторинг потенційно небезпечних місць та об'єктів для визначення необхідних заходів щодо ліквідації наслідків кожного виду можливих інцидентів ІБ. Моніторинг – це систематичне накопичення та обробка даних про стан і динаміку зміни параметрів аналізованого об'єкта або процесу і представлення результатів у зручному для керівника або експерта вигляді. Завданням моніторингу при комплексному управлінні підготовкою до ліквідації наслідків різних видів інцидентів ІБ є своєчасна оцінка виникнення загроз кожного виду інциденту ІБ, аналіз динаміки їх розвитку та їх комплексна оцінка. У динаміці це збір та аналіз даних про втрати від інцидентів ІБ. Мережево-центрична система моніторингу об'єднує засоби моніторингу всіх рівнів і напрямків управління в єдине ціле. Вона повинна забезпечувати доведення всієї необхідної інформації до адресатів в реальному часі або близькому до нього в міру її отримання та, що дуже важливо, використовуючи інформацію, отриману на всіх рівнях і напрямах управління. Такий підхід дозволяє різко поліпшити розуміння сформованої ситуації керівниками усіх ступенів, підвищити рівень взаємодії і здійснювати синхронізацію зусиль по горизонталі і вертикалі управління.

2) Здійснення необхідних заходів з підготовки до боротьби з наслідками можливих груп інцидентів ІБ.

3) Формування цілей паралельної ліквідації можливих видів інцидентів ІБ, їх синхронізацію, узгодження і ранжування. Формування цілей та їх реалізація є однією з найважливіших процедур прийняття управлінських рішень. У більшості випадків доводиться формулювати цілі не однієї людини, наприклад, керівника, а групи експертів і керівників різних спеціальностей і часто різного рівня відповідальності, що, звичайно, збільшує ступінь невизначеності як у вихідних даних, так і в оцінках. Завдання ускладнюється суб'єктивністю оцінок і їх невизначеністю. Стосовно задачі паралельної ліквідації наслідків групи різних видів прогнозованих інцидентів ІБ з використанням мережево-центричних методів комп'ютерна технологія паралельної генерації цілей може бути виконана в три етапи: формування можливих цілей паралельної ліквідації наслідків групи інцидентів ІБ. Цілі формуються експертами на підставі аналізу аналогічних інцидентів ІБ, що сталися в інших місцях, особистого досвіду, інтуїції, логіки і комп'ютерних розрахунків. Експерти можуть працювати незалежно один від одного; комп'ютерне узгодження цілей всіма експертами з урахуванням несуперечності цілей, синергетичного ефекту аналізу наслідків аналогічних груп інцидентів ІБ, обмежень, що виникають у процесі розвитку інциденту ІБ; комп'ютерна оцінка, ранжування і вибір цілей.

4) Реалізація паралельних стратегій цілей, їх синхронізацію і взаємодію використовуваних ресурсів. Вибір стратегії для досягнення цілі не менш важливо, ніж її формулювання, оскільки фактичне виконання стратегії може спотворити ціль. Стратегії реалізації цілей належать до класу, так званих, неповних математичних моделей, тобто моделей, в яких включені лише істотні чинники. Вони можуть бути формалізовані з прийнятним ступенем точності. Основною областю застосування таких моделей є задачі, що зводяться до оцінок різних варіантів управлінських рішень досягнення поставлених цілей. Ці оцінки можуть і повинні бути зроблені, як з урахуванням наявних об'єктивних даних, так і використовуючи суб'єктивні уявлення керівників та експертів. У кожній прикладній області існують свої критерії та методи оцінок, але розроблені і загальні схеми, які можуть варіюватися залежно від конкретних умов. Мережево-центричний метод вимагає розгляду та оцінки всієї сукупності можливих стратегій реалізації згенерованих цілей.

5) Формування можливого набору паралельних оперативних впливів, їх диспетчеризацію, синхронізацію і маневрування ресурсами в динаміці управління.

Аналіз інцидентів ІБ які сталися останнім часом, показує, що в багатьох випадках вони відбуваються одночасно або протягом невеликого часового інтервалу. Незалежно від існуючих між ними причинних зв'язків сучасні засоби дозволяють об'єднувати переваги окремих технологій в єдину розподілену мережево-центричну систему, яка ефективно реалізовує ліквідацію наслідків групи інцидентів ІБ. Таке об'єднання дозволяє здійснити принцип масування результатів замість поширеного сьогодні принципу масування засобів.

Використання комп'ютерних засобів управління в мережево-центричних системах дозволяє керівникам різних рівнів здійснювати ефективну взаємодію окремих напрямків управління з використання засобів і тактики ліквідації наслідків інцидентів ІБ.

Кінзерявий Василь Миколайович, *к.т.н., доцент,*
Грабінський Дмитро Миколайович, *аспірант,*
Вороніна Анастасія Вячеславівна,
Національний авіаційний університет

ОЦІНКА СТІЙКОСТІ БЛОКОВИХ СИМЕТРИЧНИХ ШИФРІВ ДО ДЕЯКИХ ВИДІВ КРИПТОАНАЛІЗУ

Одними з найефективніших методів криптоаналізу блокових симетричних шифрів (БСШ) є диференціальний та лінійний криптоаналіз [1-3]. На сьогодні теорія аналізу та обґрунтування стійкості БСШ до зазначених методів криптоаналізу досить сильно розвинена [4-6]. У багатьох БСШ при шифруванні використовуються декілька різних таблиць підстановок, послідовність використання яких наперед фіксована (наприклад, ГОСТ 28147-89, Калина та інші). Так у роботах [4-6] отримані аналітичні верхні оцінки параметрів, що характеризують практичну стійкість зазначених БСШ відносно методів лінійного та диференціального криптоаналізу. Існують також БСШ, в яких операції підстановок визначаються раундовими ключами (наприклад, ADE). Логічно припустити, що використання рандомізованих вузлів заміни ускладнює криптоаналіз БСШ, проте кількісно це важко оцінити.

З огляду на це, *актуальною* задачею є виведення аналітичних виразів, що дозволяють довести практичну стійкість БСШ із рандомізованими вузлами заміни відносно методів лінійного і диференціального криптоаналізу та дозволить зробити кількісну оцінку ефективності таких БСШ.

Метою даної роботи є оцінка практичної стійкості певного класу БСШ із рандомізованими вузлами заміни відносно методів диференціального та лінійного криптоаналізу.

Розлянуто r-раундовий БСШ $\Im$ із рандомізованими вузлами заміни, множиною відкритих (шифрованих) повідомлень $V_n = \{0,1\}^n$, множиною раундових ключів $K = V_{n+q}$ та сімейством шифруючих перетворень

$$F_k = f_{r,k_r} \circ \ldots \circ f_{1,k_1},\ k = (k_1, \ldots, k_r) \in K^r, \qquad (1)$$

де $r = 2r' + 1,\ n = pt,\ q = pq',\ p = 4p',\ t,\ p',\ r',\ q'$ – натуральні числа. Параметр $b = 2^{q'}$ визначає кількість різних таблиць підстановок, що використовуються у БСШ.

Раундове перетворення $f_{i,k}(x)$ для будь-яких $x \in V_n$, $k \in K$, $i \in \overline{1, r}$ описується як

$$f_{i,k}(x) = \begin{cases} \varphi\left(x \oplus k^{(1)}, k^{(2)}\right), & \text{якщо } \mathrm{i} \equiv 1 \pmod 2,\ i < r \\ \varphi\left(x \overset{\circ}{+} k^{(1)}, k^{(2)}\right), & \text{якщо } \mathrm{i} \equiv 0 \pmod 2,\ i < r, \\ s\left(x \oplus k^{(1)}, k^{(2)}\right), & \text{якщо } \mathrm{i} = \mathrm{r} \end{cases} \qquad (2)$$

де $k^{(1)}$ та $k^{(2)}$ частини раундового ключа k ($k = \left(k^{(1)}, k^{(2)}\right),\ k^{(1)} \in V_n,\ k^{(2)} \in V_q$.

Підстановки φ і s визначаються за формулами:

$$\varphi(x, y) = s(x, y)M,\ x \in V_n,\ y \in V_q, \tag{3}$$

$$s(x, y) = \left(s_{y_{p-1}}(x_{p-1}), \ldots, s_{y_0}(x_0)\right),\ x = (x_{p-1}, \ldots, x_0), y = (y_{p-1}, \ldots, y_0), \tag{4}$$

де $x_j \in V_t,\ y_j \in V_{q'},\ s_{y_j}$ – підстановка на множині V_t (по індексу y_j обирається для використання одна таблиця підстановок із b можливих), $j \in \overline{0, p-1}$, M – оборотна $p \times p$ – матриця над полем $\mathrm{GF}(2^t)$, а множення $s(x, y)$ на M у виразі (3) виконується над цим полем при ототожненні двійкових векторів $s_{y_j}(x_j)$ із його елементами.

У формулі (2.2) символи $\oplus$ і $\overset{\circ}{+}$ відповідають відповідно операціям по координатного булевого додавання двійкових векторів довжини n та алгебраїчну операцію виду

$$x \overset{\circ}{+} k = \left(x^{(1)} + k^{(1)}, \ldots, x^{(4)} + k^{(4)}\right), \tag{5}$$

де $x = \left(x^{(1)}, \ldots, x^{(4)}\right)$, $k = \left(k^{(1)}, \ldots, k^{(4)}\right)$, $x^{(v)}, k^{(v)} \in V_{tp'}$, $v \in \overline{1,4}$, а $+$ це символ операції додавання за модулем $2^{tp'}$ на множині $V_{tp'}$.

Для розглянутого БСШ $\mathfrak{I}$ *отримано аналітичні верхні оцінки параметрів, що характеризують його практичну стійкість відносно методів лінійного та диференціального криптоаналізу*:

$$EDP(\Omega) \le \overset{\approx}{\Delta}^{r'B_M+1} \le \Delta^{r'B_M+1}, \tag{6}$$

$$ELP(\Omega) \le \overset{\approx}{\Lambda}^{r'B_M+1} \le \Lambda^{r'B_M+1}, \tag{7}$$

де $EDP(\Omega)$ – середня імовірність диференціальної характеристики Ω, $ELP(\Omega)$ – середня імовірність лінійної характеристики Ω, B_M – індекс галуження матриці M, а параметри Δ, Λ, $\overset{\approx}{\Delta}$, $\overset{\approx}{\Lambda}$ визначаються за формулами:

$$\Delta = \max\left\{d_{\oplus}^{(s_j)}(\alpha, \beta),\ d_{+}^{(s_j)}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\}, j \in \overline{0, b-1}\right\}, \tag{8}$$

$$\Lambda = \max\left\{l^{(s_j)}(\alpha, \beta),\ \Lambda^{(s_j)}(\alpha, \beta) : \alpha \in V_t, \beta \in V_t \setminus \{0\}, j \in \overline{0, b-1}\right\}, \tag{9}$$

$$\overset{\approx}{\Delta} = \max\left\{b^{-1}\sum_{j=0}^{b-1} d_{\oplus}^{(s_j)}(\alpha, \beta), b^{-1}\sum_{j=0}^{b-1} d_{+}^{(s_j)}(\alpha, \beta) : \alpha, \beta \in V_t \setminus \{0\}\right\}, \tag{10}$$

$$\overset{\approx}{\Lambda} = \max\left\{b^{-1}\sum_{j=0}^{b-1} l^{(s_j)}(\alpha, \beta),\ b^{-1}\sum_{j=0}^{b-1} \Lambda^{(s_j)}(\alpha, \beta) : \alpha \in V_t, \beta \in V_t \setminus \{0\}\right\}. \tag{11}$$

У формулах (8)–(11) $d_{\oplus}^{(s_j)}(\alpha, \beta)$ та $d_{+}^{(s_j)}(\alpha, \beta)$ – таблиці різниць підстановки s_j ($j \in \overline{0, b-1}$) відносно операцій додавання за модулем 2 та 2^t відповідно, а $l^{(s_j)}(\alpha, \beta)$, $\Lambda^{(s_j)}(\alpha, \beta)$ – таблиці лінійних апроксимацій підстановки s_j ($j \in \overline{0, b-1}$) відносно цих самих операцій:

$$d_{\oplus}^{(s_j)}(\alpha, \beta) = 2^{-t}\sum_{k \in V_t} \delta\left(s_j(k \oplus \alpha) \oplus s_j(k), \beta\right), \tag{12}$$

$$d_{+}^{(s_j)}(\alpha,\beta)=2^{-t}\sum_{k\in V_t}\delta\left(s_j(k+\alpha)\oplus s_j(k),\beta\right), \tag{13}$$

$$l^{(s_j)}(\alpha,\beta)=2^{-t}\sum_{k\in V_t}\left(2^{-t}\sum_{x\in V_t}(-1)^{\alpha x\oplus\beta s_j(x\oplus k)}\right)^2, \tag{14}$$

$$\Lambda^{(s_j)}(\alpha,\beta)=2^{-t}\sum_{k\in V_t}\left(2^{-t}\sum_{a\in\{0,1\}}\left|\sum_{x\in V_t:v(x,k)=a}(-1)^{\alpha x\oplus\beta s_j(x+k)}\right|\right)^2. \tag{15}$$

Проведено *порівння аналітичних верхніх меж стійкості БСШ із рандомізованими і фіксованими вузлами заміни* відносно методів лінійного та диференціального криптоаналізу.

Позначимо як $\Im'$ частковий випадок БСШ $\Im$, в якому $q'=0$, $q=0$. Тоді $\Im'$ буде БСШ із фіксованими вузлами заміни. У [4] доведено, що для БСШ $\Im'$ виконуються наступні нерівності:

$$EDP(\Omega)\le\Delta^{r'B_M+1}, \tag{16}$$

$$ELP(\Omega)\le\Lambda^{r'B_M+1}. \tag{17}$$

Із нерівностей (6)-(7), (16)-(17) та формул (8)-(15) слідує, що верхні аналітичні оцінки середніх ймовірностей диференціальних та лінійних характеристик БСШ $\Im$ будуть кращими у $\left(\tilde{\Delta}/\Delta\right)^{r'B_M+1}$ та $\left(\tilde{\Lambda}/\Lambda\right)^{r'B_M+1}$ разів за аналогічні оцінки БСШ $\Im'$. Тому, можна зробити висновок, що використання у БСШ рандомізованих вузлів заміни покращує оцінки стійкості до методів лінійного та диференціального криптоаналізу.

Покажемо ефективність використання рандомізованих вузлів заміни на прикладі БСШ Калина-128 [7], який являється конкретним прикладом БСШ $\Im'$ з параметрами $t=8$, $p'=4$, $r'=5$, $p=16$, $r=11$, $n=128$, $q'=0$, $q=0$, у кожному раунді використовуються 8 різних таблиць підстановок на множині V_8. Для БСШ Калина-128 $\Delta=0{,}031250$, $\Lambda=0{,}0625$, $r'=5$, $B_M=9$. Тоді, на основі нерівностей (16)-(17), аналітичні верхні межі стійкості відносно методів лінійного та диференціального криатоаналізу будуть наступними: $EDP(\Omega)\le 2^{-230}$, $ELP(\Omega)\le 2^{-184}$.

Припустимо, що у БСШ Калина-128 додатково ввели раундові ключі, що визначають, які таблиці підстановок використовуються у кожному раунді. У такому випадку отримаємо БСШ $\Im$ з параметрами $q'=3$, $q=48$, $b=8$. Для даного БСШ, на основі формул (8)-(15), визначено параметри $\tilde{\Delta}$, $\tilde{\Lambda}$: $\tilde{\Delta}=0{,}015625$, $\tilde{\Lambda}=0{,}0159302$. На основі нерівностей (6)-(7) визначено аналітичні верхні межі стійкості відносно методів лінійного та диференціального криатоаналізу: $EDP(\Omega)\le 2^{-276}$, $ELP(\Omega)\le 2^{-274}$. Як видно з розрахунків верхні аналітичні оцінки середніх ймовірностей диференціальних та лінійних характеристик удосконаленого БСШ Калина-128 відповідно покращилися у 2^{46} і 2^{90} разів у порівнянні із оригіналом.

Отже у роботі оцінено практичну стійкість БСШ $\Im$ (описуються формулами (1)−(5)) із рандомізованими вузлами заміни відносно методів диференціального та лінійного криптоаналізу. Показано, що використання рандомізованих вузлів заміни у БСШ дозволяє підвищити стійкість до вище зазначених методів криптоаналізу.

СПИСОК ВИКОРИСТАННЯ ДЖЕРЕЛ

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.Matsui M. Linear cryptanalysis methods for DES cipher // Advances in Cryptology – EUROCRYPT'93, Proceedings.– Springer Verlag, 1994. – P. 386 – 397.
4.Алексейчук А.Н. Оценки практической стойкости блочного шифра «Калина» относительно методов разностного, линейного криптоанализа и алгебраических атак, основанных на гомоморфизмах / А.Н. Алексейчук, Л.В. Ковальчук, Е.В. Скрынник, А.С. Шевцов // Прикладная радио-электроника. — 2008. — Т.7, № 3. — С. 203-209.
5.Алексейчук А.Н. Верхние оценки несбалансированности билинейных аппроксимаций раундовых функций блочных шифров ГОСТ и "Калина" / А.Н. Алексейчук, А.С. Шевцов // Сучасний захист інформації. – 2010. – № 2. – С. 23 – 30.
6.Алексейчук А.Н., Ковальчук Л.В. Верхние границы максимальных значений вероятностей дифференциальных и линейных характеристик шифра Фейстеля, содержащего сумматор по модулю 2m // Прикладная радиоэлектроника. – 2006. – Т. 5. – № 1. – С. 74 – 82.
7.Горбенко І.Д., Долгов В.І., Олійников Р.В., Руженцев В.І., Михайленко М.С., Горбенко Ю.І., Тоцький О.С., Казьміна С.В. Перспективний блоковий симетричний шифр "Калина" – основні положення та специфікації // Прикладная радиоэлектроника. – 2007. – Т. 6. – № 2. – С. 195 – 208.

Сніжко В'ячеслав Володимирович, *асистент,*
Національний авіаційний університет

ВИКОРИСТАННЯ КОГНІТИВНОГО МОДЕЛЮВАННЯ ПРИ ПОБУДОВІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Вирішення питань забезпечення інформаційної безпеки та управління захистом інформації сьогодні стає життєво необхідним для існування і розвитку будь–якої сучасної організації.

Безпека – поняття комплексне і не може розглядатися як проста сума її складових частин. Ці частини взаємопов'язані і взаємозалежні. Крім того, кожна частина критично значима. Отже, ніякі методи, які передбачають часткове ігнорування критеріїв безпеки (нехай і неявне) при комплексній оцінці безпеки неприйнятні. Тому розробка алгоритму, що дозволяє уніфікувати підходи до управління комплексною безпекою системи є актуальним завданням.

Під безпекою розуміється стан і тенденції розвитку захищеності життєво важливих елементів системи від зовнішніх і внутрішніх негативних факторів. При цьому необхідно врахувати, що безпека – динамічна категорія, що має множинну предметність. Діяльність щодо безпеки виникає в ході вирішення протиріччя між небезпекою і потребою управляти безпекою: передбачувати, запобігати, локалізовувати і усувати збитки від впливу загроз. Комплексна оцінка рівня безпеки (КОРБ) не може бути більшою мінімальної оцінки, отриманої для різних аспектів системи.

Безпека не існує сама по собі, поза людським впливом. Вона забезпечується для людини і нею ж оцінюється. Тому, поняття безпеки має не тільки об'єктивну, але й суб'єктивну сторону, оскільки оцінка її рівня проводиться в кінцевому підсумку людиною. Специфічними особливостями задачі створення систем захисту є:

- неповнота вихідної інформації про склад і характер загроз;
- багатокритеріальність задачі, пов'язана з необхідністю врахування великої кількості локальних показників;
- наявність як кількісних, так і якісних показників, які необхідно враховувати при вирішенні завдань розробки та впровадження систем захисту;
- неможливість застосування класичних методів оптимізації.

Когнітивний аналіз об'єкта дослідження дозволяє:

- прогнозувати напрямки розвитку системи (ситуації);
- виявити фактори, що впливають на розвиток ситуації;
- формалізувати процеси прийняття рішень;
- отримати як якісні, так і кількісні характеристики ситуації;

Оцінка інформаційних ризиків, котра базується на нечіткому когнітивному моделюванні дозволяє:

- виявити найбільш небезпечні загрози та вразливості, що впливають на інформаційну систему;
- оцінити можливий збиток від дії загроз на інформаційну систему;
- адаптуватися до нових зовнішніх і внутрішніх загроз та ітехнологій;
- дати ефективний і простий механізм прийняття рішень для служб, що займаються забезпеченням інформаційної безпеки.

Розробка алгоритму, який дозволить уніфікувати підходи до управління комплексною безпекою дозволить вирішити ряд питань пов'язаних з суб'єктивною стороною при аналізі та управлінні комплексною безпекою.

Сформулюємо математичну модель, що описує динаміку зміни рівня комплексної безпекою різних систем.

Назвемо рівнем комплексної безпеки системи (РКБС) оцінку, засновану на наборі показників і критеріїв, що характеризують стан системи в плані захищеності критичних для неї елементів.

Рівень комплексної безпеки системи можна охарактеризувати такою матрицею (матриця безпеки):

$$B = \begin{pmatrix} K_1 & F_1 & V_1 & T_1 & S_1 \\ K_2 & F_2 & V_2 & T_2 & S_2 \\ K_3 & F_3 & V_3 & T_3 & S_3 \\ -- & -- & -- & -- & -- \\ K_n & F_n & V_n & T_n & S_n \end{pmatrix}$$

де K_i – показник рівня безпеки по i –му критерію; F_i – тенденція змін i –го критерію (зростає, спадає, нейтральний); V_i – швидкість змін i –го критерію (наприклад: низька, нижче середнього, середня, вище середнього, висока); T_i – характерний для i –го критерію час, котрий дозволяє правильно інтерпретувати значення параметру V_i; S_i – степінь критичності негативних наслідків при реалізації ризиків, що погіршують значення i –го критерію.

Перший і четвертий стовпчик МБ характеризують поточний стан комплексної безпеки. Інші стовпці матриці відображають динаміку розвитку процесів і дозволяють будувати прогноз розвитку на майбутнє.

Необхідно проаналізувати основні загрози безпеці інформаційної системи, їх можна розділити на дві категорії: первинні і вторинні.

Ймовірності виникнення первинних загроз від нас не залежать. Однак сукупність превентивних заходів захисту дозволяє послабити вплив первинних загроз на рівень безпеки системи. Цей факт може бути описаний за допомогою матриці превентивних заходів (МПЗ):

$$Z_j = \begin{pmatrix} z_{11} & z_{12} & z_{13} & z_{14} & z_{15} \\ z_{21} & z_{22} & z_{23} & z_{24} & z_{25} \\ -- & -- & -- & -- & -- \\ z_{n1} & z_{n2} & z_{n3} & z_{n4} & z_{n5} \end{pmatrix}$$

де $j = 1...M$, де M – загальна кількість превентивних заходів.

Якщо все ж, незважаючи на превентивні заходи захисту, реалізація певної множини первинних загроз призвела до виникнення наслідків, то необхідно вжити заходів для їх локалізації та усунення.

Реалізація цих заходів може бути формалізована за допомогою матриці ліквідації наслідків (МЛН): З первинними загрозами ми починаємо боротися ще до їх настання. У випадку з вторинними загрозами ми повинні не допустити їх, тобто і боротися з причинами, котрі їх викликають. Це принципова відмінність в блоках заходів, вплив яких формалізовано множиною матриць Z_j і матрицею L.

$$L = \begin{pmatrix} l_{11} & l_{12} & l_{13} & l_{14} & l_{15} \\ l_{21} & l_{22} & l_{23} & l_{24} & l_{25} \\ -- & -- & -- & -- & -- \\ l_{n1} & l_{n2} & l_{n3} & l_{n4} & l_{n5} \end{pmatrix}$$

При побудові нечіткої когнітивної моделі (НКМ) об'єкт дослідження представляють у вигляді знакового орієнтованого графа. В якості такої моделі при оцінці комплексної безпеки системи (КБС) може бути прийнятий:

$$KBS = < G, QL, E >.$$

Тут G – орієнтований граф, що має одну кореневу вершину і не містить петель і горизонтальних ребер в межах одного рівня ієрархії:

$$G = < \{GF_i\}; \{GD_{ij}\} >$$

де $\{GF_i\}$ – множина вершин графа (факторів або концептів в термінології НКМ);

$\{GD_{ij}\}$ – множина дуг, що з'єднують i–у і j–у вершини (множина причинно-наслідкових зв'язків між концептами; при цьому дуги розташовані так, що початку дуги відповідає вершина нижнього рівня ієрархії (рангу), а закінченню дуги – вершина рангу, на одиницю меншого); $GF_0 = K$ – коренева вершина, що відповідає рівню комплексної безпеки в цілому (інтегральному критерію безпеки – цільовому концепту); QL – набір якісних оцінок рівнів кожного фактору в ієрархії; E – система відношень переваги одних факторів над іншими за ступенем їх впливу на заданий елемент.

Загальну модель аналізу та управління комплексною безпекою на основі нечіткого когнітивного моделювання можна представити в наступному вигляді:

1. Збір інформації про об'єкт захисту: ідентифікація активів і встановлення початкового рівня безпеки. У процесі ідентифікації слід розглянути основні характеристики активів: інформаційну цінність, чутливість активів до загроз, наявність захисних заходів. При цьому необхідно врахувати, що в числі факторів, що впливають на безпеку, особливе місце займають суб'єктивні фактори, які є найменш прогнозованими.
2. Вибір критеріїв, що характеризують стан різних сторін забезпечення безпеки, визначення їх прийнятного рівня.
3. Побудова когнітивної моделі у вигляді знакового-орієнтованого графа.
4. Розрахунок і аналіз рівня комплексної безпеки системи (РКБС).

5. Якщо РКБС не знаходиться в прийнятному діапазоні значень, то виробляються зміни у складі концептів, що беруть участь у побудові когнітивної моделі, у складі зв'язків між концептами, змінюються їх значення за допомогою введення захисних заходів.

Таким чином, процес забезпечення безпеки системи передбачає вирішення двох взаємопов'язаних завдань: пряма задача (аналіз стану системи) і оберненої задачі управління (вплив на систему).

При вирішенні першого завдання потрібно визначити значення критеріїв безпеки K_i та інтегрального критерію K при заданих значеннях всіх концептів, котрі впливають на них.

Якщо отримані значення знаходяться поза діапазоном прийнятності, то при вирішенні оберненої задачі необхідно підібрати такі керуючі впливи Z_j та L, які забезпечать повернення цільових критеріїв у безпечний діапазон.

Якщо існує не єдиний набір необхідних управляючих впливів, то на цьому етапі може виникнути задача оптимізації, що складається в знаходженні такої комбінації Z_j і L, яка забезпечує максимальний вплив на негативні фактори при заданих або мінімальних витратах на реалізацію способів і засобів захисту.

Управління інформаційною безпекою значно спрощується і формалізується при використанні нечіткого когнітивного моделювання. Використання даного підходу сприяє вирішенню проблем пов'язаних з суб'єктивною стороною в процесах аналізу інформаційних ризиків і загроз безпеці. Це дозволяє уніфікувати підходи до управління комплексною безпекою і приступити до розробки відповідних обчислювальних процедур і модулів, які можуть бути в подальшому використані при побудові систем захисту інформації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Гайдамакін Н. А. Розмежування доступу до інформації в комп’ютерних системах [Текст] / Н. А. Гайдамакін. – Е.: Урал, 2003. – 328 с.

2. Борисов В. В. Нечіткі моделі і мережі [Текст] / В. В. Борисов, В. В. Круглов, А. С. Федулов. – М.: Телеком, 2007. – 284 с.

3. Райков А. Н. Інтелектуальні інформаційні технології [Текст]: навч. посібник / А. Н. Райков. – М.: МГИРЕА(ТУ), 2000. – 96 с.

4. Васильєв В. І. Аналіз і управління інформаційною безпекою внз на основі когнітивного моделювання [Текст] / В. І. Васильєв, Р. Т. Кудрявцева // Системи управління та інформаційні технології. – 2007. – Т. 27, №1. – С. 74–81.

5. Ажмухамедов І. М. Управління інформаційною безпекою регіону на основі когнітивного моделювання [Текст] / І. М. Ажмухамедов // Вістник АГТУ. – 2010. – №1. – С. 96–102.

Фесенко Андрей Алексеевич, *аспирант,*
Швец Валериан Анатольевич, *к.т.н., доцент,*
Национальный авиационный университет

МЕТОД ИНДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ НА БАЗЕ РАДУЖНОЙ ОБОЛОЧКИ ГЛАЗА

В последнее время значительно повысился интерес к тематике цифровой идентификации личности, что принято связывать с ростом угроз международного терроризма, проблемами процессов демократизации при переходе к информационному обществу. Интерес к цифровой идентификации личности возрастает также в связи с увеличением объемов торговых операций, осуществляемых через глобальные компьютерные сети, в частности через Интернет. Цифровая идентификация личности неразрывно связана с такими понятиями, как идентификация личности, биометрия, электронная цифровая подпись, электронные регистры, паспорта.

Сравнение различных биометрических методов идентификации (табл. 1.) показало, что по совокупности качеств широкое использование идентификации по радужной оболочке глаза имеет заметные преимущества перед большинством других биометрических характеристик.

Таблица 1. Сравнение различных биометрических методов идентификации

Экспертная оценка БХЧ: (+ + + – высокая оценка, + + – средняя, + – низкая)

Характеристика	*Универсальность*	*Уникальность*	*Постоянство*	*Измеримость*
Видеообразы лица	+++	+	++	+++
Термограмма лица	+++	+++	+	+++
Отпечаток пальца	++	+++	+++	++
Геометрия руки	++	++	++	+++
Радужная оболочка глаза	+++	+++	+++	++
Сетчатка	+++	+++	++	+
Подпись	+	+	+	+++
Голос	++	+	+	++
Отпечаток губ	+++	+++	++	+
Особенности уха	++	++	++	++
Динамика подписи	+++	+++	+	+++
Походка	+++	++	+	+

В качестве базового метода выделения радужной оболочки используется метод локализации радужки глаза, который включает в себя простую фильтрацию, выделение перепадов яркости и преобразование Хоха. Преобразование Хоха позволяет перейти от радиальной системы координат, на которой базируется объекты изображения радужки, так как она аппроксимируется кругом, в декартову систему координат.

Другой метод определения границ радужки заключается в выделении границ путем максимизации суммы градиентов яркости в направлении перпендикулярном к границе радужки:

$$max_{(r,x_0,y_0)}\left|G_\sigma(r) * \frac{\partial}{\partial r}\oint_{x_0,y_0}\frac{I(x,y)}{2\pi r}ds\right|$$

Предложенный алгоритм позволяет определить координаты центров и радиусы радужки и зрачка с точностью до одного пикселя при невысоких вычислительных затратах даже для изображений с большим разрешением. Уменьшить вычислительные затраты можно методом, алгоритм которого представлен на рис. 1.

После нахождения радужной оболочки необходимо выделить текстурные признаки на радужке. Существует много методов выделения текстурных признаков, к которым предъявляться следующие требования:

– нечувствительность к изменению яркости и контраста;

– нечувствительность к сдвигу изображения (к повороту в декартовой системе координат);

– хорошая разделяющая способность.

Выделение текстурных признаков в основе реализуется с применением фильтров Габора. Однако фильтры Габора имею недостаток, заключающийся в недостаточной вычислительной эффективности. Один из самих вычислительно эффективных полосовых фильтров – DoG-фильтр (DifferenceofGaussian), для которого в отличие от фильтра Габора существует эффективный рекурсивный алгоритм.

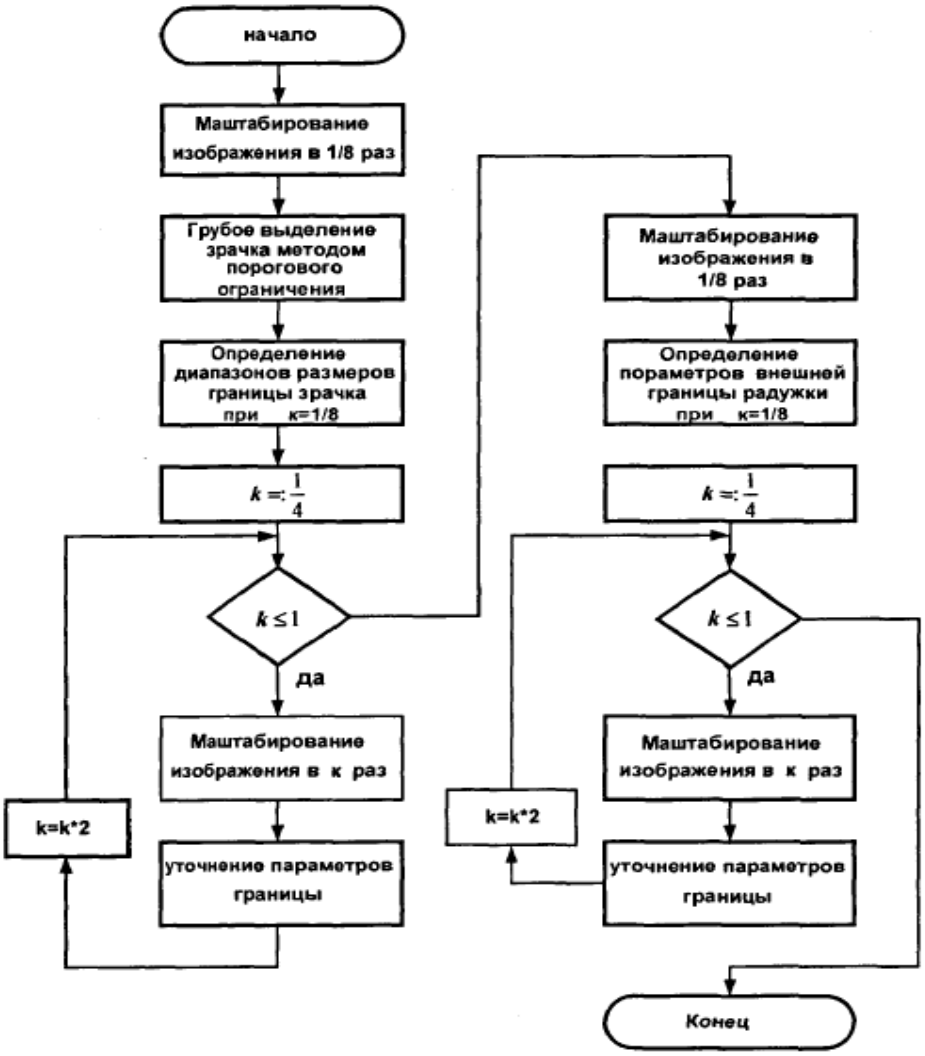


Рис. 1. Схема интегрально-дифференциального алгоритма локализации радужной оболочки с последовательным уточнением

Предложена и исследована система признаков на основе DoG-фильтра. DoG-фильтр описывается следующим выражением:

$$DoG(x,y) = g(x,y,\sigma) - g(x,y,1.6\sigma), \quad (1)$$

где $$g(x,y) = \frac{1}{2\pi\sigma^2} exp\left(\frac{-(x^2+y^2)}{2\sigma^2}\right) \quad (2)$$

Одной из особенностей DoG-фильтра является то, что его отклик меняет знак в тех областях изображения, где присутствует перепад яркости. На этом свойстве основано действие контурного детектора. В однородных областях изображения отклик фильтра равен нулю, однако таких областей на изображении радужной оболочки практически не встречается.Структура радужки может быть закодирована знаками отклика DoG-фильтра в узлах ортогональной сетки:

$$h(i,j) = \begin{cases} 1, & D(i,j) \geq 0 \\ 0, & D(i,j) < 0 \end{cases} \quad (3)$$

где $$D(x,y) = I(x,y) * DoG(x,y,\sigma), \quad (4)$$

(i, j) – позиция на изображении, в которой определяется бит кода радужки.

С изложенной выше информации можем сделать следующие выводы, что предварительная обработки изображения радужной оболочки глаза состоит из четырех этапов: локализация радужки, геометрическая нормализация изображения радужной

оболочки, яркостная нормализация и подавление шумов. Предлагается новый интегрально-дифференциальный алгоритм определения границ радужной оболочки с последовательным уточнением и определением области поиска центра зрачка путем порогового ограничения. Разработанный алгоритм требует меньших вычислительных затрат при сохранении высокой точности. К методу выделения текстурных признаков изображения радужки предъявляться следующие требования:

1) нечувствительность к изменению яркости и контраста;

2) нечувствительность к сдвигу изображения (к повороту в полярной системе координат);

3) хорошая разделяющая способность.

Фазовое представление изображение позволяет избавиться от влияния неравномерного освещения при идентификации личности по радужке глаза. Локальные фазы вейвлетов Габора несут много информации о структуре изображения. Поэтому использование локальных фаз вейвлетов Габора в качестве признаков для распознавания является более предпочтительным. Фильтр Габора уступает в вычислительной эффективности DoG-фильтру. Поэтому система признаков на основе DoG-фильтра может оказаться более эффективной. Более того знаки отклика DoG-фильтра несут информацию о локальной структуре изображения и не чувствительный к изменениям яркости и контраста. Перечисленные свойства позволяют заключить, что использование знаков отклика DoG-фильтра в качестве признаков текстуры радужки является перспективным.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Евангели А. Технологии биоидентификации и биометрический рынок. // PC Week /RE. – 2003 - № 7 – с. 24-25.

2. Матвеев И.А., Ганькин К.А. Распознавание человека по радужке. // Системы безопасности. – 2004 - № 5 – с. 72-76

3. Хебайши М.А., Жирков В.Ф., Идентификация Личности По Радужке Глаза , 5 Международная Научно-Техническая Конференция, ФРЭМЭ'2002, 2528 Июня, Вл.Г.У., С.133 - 134.

Гізун Андрій Іванович, *асистент,*
Національний авіаційний університет

СИСТЕМА ВИЯВЛЕННЯ ІНЦИДЕНТІВ – ПОТЕНЦІЙНИХ КРИЗОВИХ СИТУАЦІЙ

Оскільки лише виявлення інциденту, враховуючи важливість захисту інформаційно-комунікаційних систем та мереж (ІКСМ) в поєднані з стрімким розвитком сучасних засобів та способів порушення інформаційної безпеки, на сьогодні є не достатнім. Виникає необхідність в їх ідентифікації, так як вибір контрзаходів є більш ефективним для конкретного і заздалегідь відомого інциденту. Тому основне призначення запропонованої в роботі системи – прогнозування або виявлення та ідентифікація інцидентів-потенційних кризових ситуацій (ІПКС).

Метою роботи є розширення функціональних можливостей сучасних систем управління кризовими ситуаціями (КС) в аспекті їх виявлення та ідентифікації та автоматизації процесів прийняття рішень в умовах нечітко формалізованого середовища та впливу КС шляхом розробки архітектури системи виявлення ІПКС (СВІПКС).

На сьогодні аналогічних систем практично немає. Подібні системи для виявлення вторгнень, комп’ютерних атак, системи промислової і виробничої безпеки засновані на теорії ймовірності і ґрунтуються на сигнатурному або компараторному принципах [1]. Такий підхід не дозволяє виявляти невідомі атаки чи інциденти, контролювати слабоформалізований простір. Крім того для таких систем необхідний довготривалий підготовчий етап перед введенням їх в експлуатацію. В рамках такої підготовки зазвичай проходить вибірка

статистичних даних, навчання системи тощо. Тому при розробці даної системи будемо використовувати підходи засновані на нечіткій логіці та експертні методи, що позбавлені таких недоліків. Слід також згадати подібні системи на базі нечіткої логіки для виявлення аномального стану [2], порушника ІБ [3]. Прототип цієї системи описаний в [4]

Метою роботи СВІПКС є виявлення та ідентифікація ІПКС. Вхідними даними системи є ідентифікатори ІПКС, контрольовані (ідентифікуючі) параметри та їх значення. На виході системи – інформація щодо ІПКС, ймовірності його реалізації тощо.

Робота запропонованої системи ґрунтується на застосування таких методів нечіткої логіки [5] як метод лінгвістичних термів з використанням статистичних даних (МЛТС) – для побудови еталонних значень параметрів, лінійної апроксимації по локальним максимумам (ЛАЛМ), узагальненої відстань Хемінга (УВХ) – для обробки нечітких даних та проведення операцій нечіткої логіки. Крім того, використовується також експертні методи оцінювання та ранжування, а саме метод середніх рангів в процесі побудови наборів евристичних правил (ЕП).

СОКС включає такі структурні елементи як: система датчиків (СД); модуль первинної обробки вхідних параметрів, що вміщує регістри ідентифікуючих параметрів (РІП), регістри ІПКС (РІПКС), блок формування зв’язки інцидент-параметр (БФЗІП); модуль вторинної обробки ідентифікуючих параметрів, що складається з блоку фазифікації ідентифікуючих параметрів (БФІП) та блоку формування кортежів фазифікованих параметрів (БФКФП); модуль виконання нечітких арифметичних операцій, до якого відносяться блок формування ідентифікатора поточного стану і блок прийняття рішення; модуль формування еталонів та евристичних правил, до складу якого входять однойменні відповідні блоки; модуль представлення результату, що містить блок логічного висновку та блок візуалізації; а також модуль управління режимами (МУР), що переводить систему в режим корекції еталонів (РКЕ) або режим корекції евристичних правил (РКЕП).

СД розміщена в контрольованому середовищі (ІКСМ, внутрішнє середовище будівель та приміщень, зовнішнє середовище певних територій, населених пунктів, держави тощо), що є нечітким та слабоформалізованим. В залежності від типу середовища датчики можуть бути різного роду – технічні, екологічні, фізичні і т.п. Так в ІКСМ в якості датчиків використовуються програмні та апаратні засоби для фіксації мережевих та хостових параметрів, наприклад tcpdump для контролю трафіку, програмний засіб Everest для визначення завантаженості CPU, оперативної памяті тощо чи їх аналоги. В серверній використовуються датчики температури, гігрометри для визначеня рівня вологи, датчики наявності пилу, диму і т.д. Склад СД залежить від поставлених цілей і області застосування.

В модулі первинної обробки вхідних параметрів задаються ІПКС, які система прогнозує виявляє та ідентифікує, а також відповідні їм ідентифікуючі параметри. В РІПКС заносяться ідентифікатори основних класів інцидентів $IKS_i, i=\overline{1,n}$. В РІП аналогічно заносяться з певною періодичністю поточні значення ідентифікуючтх параметрів $P_j, j=\overline{1,m}$ [6]. В БФЗІП формуються зв'язки $IKS_i \to P'_i$ конкретного типу ІПКС з параметрами $P'_i = \left\{ \bigcup_{i=1}^{n} \bigcup_{j=1}^{k_i} P_j \mid P_j \in P \right\}$, $(i=\overline{1,n}, j=\overline{1,k_i})$, що необхідні для його виявлення, де k_i – кількість параметрів необхідних для виявлення *i*-ого ІПКС.

Модуль вторинної обробки ідентифікуючих параметрів призначений для фазифікації ідентифікуючих параметрів та подальшого їх групування відповідно до ІПКС, які вони визначають. В БФІП проводиться процедура фазифікації, яка полягає в перетворені виміряних поточних параметрів за певний період в нечіткі числа (НЧ), в результаті формуються $\underset{\sim}{P}_j$ $(i=\overline{1,m})$. В БФКФП уже фазифіковані ідентифікуючі параметри групуються

в кортежі у відповідністю з сформованими в БФЗІП зв'язками. Так для окремих ІПКС створюються кортежі $< \underset{\sim}{P}_i^{'} >= \bigcup_{i=1}^{n} < \bigcup_{j=1}^{k_i} \underset{\sim}{P}_j \mid \underset{\sim}{P}_j \subseteq \underset{\sim}{P} >$ з елементів підмножини $\underset{\sim}{P}_i^{'}$.

В модулі формування еталонів та ЕП формуються еталонні величини, необхідні для виміру поточних значень контрольованих параметрів та евристичні правила для прийняття рішення. БФНЕ призначений для створення експертами множини еталонів ідентифікуючих параметрів $T^e = \bigcup_{j=1}^{m} \bigcup_{s=1}^{r} T_{js}^e = \{T_{1s}^e, T_{2s}^e, ..., T_{ms}^e\}$, де $(s = \overline{1,r})$ – кількість терміву лінгвістичній зміні (ЛЗ), що характеризує параметр. В БФЕП у процесі зіставлення ідентифікаторів поточного стану LC, що визначається комбінацією значень поточних параметрів, та лінгвістичних ідентифікаторів ймовірності реалізації ІПКС формується набір правил $\mathrm{ER} = \left\{ \bigcup_{i=1}^{n} ER_i \right\} = \{ER_1, ER_2, ..., ER_n\}$ для всіх заданих інцидентів. Тобто $ER = \bigcup_{i=1}^{n} \left\{ \bigcup_{p=1}^{P_i} ER_{ip} = (LC_{ip} \to LI_{ip}) \right\}$. де ER_{ip} є p-е правило виявлення аномалії породженої і-им інцидентом, P_i (i=1,n) - загальна кількість можливих правил, спрямованих на виявлення і-ого ІПКС, а LI_{ip} - один з елементів множини лінгвістичних ідентифікаторів ймовірності реалізації ІПКС, необхідних для відображення судження експерта в лінгвістичній формі. За умов дослідження, наприклад, 1-е правило для виявлення $IKS_4 = VA$ (вірусна атака) матиме вигляд: $ER_{41} = \{(\underset{\sim}{P}_{CPU}^{'} \cong H,\ \underset{\sim}{P}_{CNCh}^{'} \cong H,\ \underset{\sim}{P}_{STF}^{'} \cong M,\ \underset{\sim}{P}_{MU}^{'} \cong H,\ \underset{\sim}{P}_{NEr}^{'} \cong M) \to H\}$, що словесно можна інтерпретувати таким чином: "Якщо поточні значення $\underset{\sim}{P}_{CPU}^{'}$, $\underset{\sim}{P}_{CNCh}^{'}$, $\underset{\sim}{P}_{STF}^{'}$, $\underset{\sim}{P}_{MU}^{'}$, $\underset{\sim}{P}_{NEr}^{'}$ найбільш близько розташовані до значень H, H, M, H, M відповідно, що входять до $\mathrm{T}^{\mathrm{e}}_{CPU}, \mathrm{T}^{\mathrm{e}}_{CNCh}, \mathrm{T}^{\mathrm{e}}_{STF}, \mathrm{T}^{\mathrm{e}}_{MU}, \mathrm{T}^{\mathrm{e}}_{NEr}$, то рівень можливості виникнення ІПКС в даний момент буде НИЗЬКИЙ".

Утворені еталони та евристичні правила є основними експертними даними, що забезпечують роботу СВІПКС. Вони задаються перед початком роботи системи з виявлення ІПКС. Існує можливість їх корекції. Для цього МУР переводить в систему в РКЕ або РКЕП, під час яких еталони та ЕП можуть бути змінені експертом чи оператором системи.

Призначення модуля виконання нечітких арифметичних операцій полягає в порівнянні поточних значень параметрів з еталонними і визначені ЕП, що узгоджує поточну ситуацію, тобто прийняті рішення щодо факту існування чи можливості появи ІПКС. В БФІПС виміряні і фазиковані ідентифікуючі параметри, оформлені в вигляді кортежів, з використанням методу УВХ порівнюються з еталонами, визначаючи відповідні (найбільш близькі) поточній ситуації терми, і на основі цього формується ідентифікатор поточного стану $LC = \underset{j=1}{\overset{k_i}{\wedge}} t_j = \underset{j=1}{\overset{k_i}{\wedge}} (\underset{\sim}{P}_j^{'} \cong \underset{s=1}{\overset{r}{\vee}} T_{js}^e)$. В БПР LC порівнюється з наборами ЕП, в процесі чого шукається правило, що погоджує поточний ідентифікатор. Ймовірність появи ІПКС прирівнюється значенню лінгвістичного ідентифікатора ймовірності реалізації ІПКС LI_{ip} правила, що спрацювало.

Призначення модуля представлення результату полягає в відображені отриманих результатів в зрозумілій для оператори системи вигляді. Отриманий результат може бути відображений в лінгвістичній формі. В БЛВ конкретній поточній ситуації присвоюється відповідний їй ідентифікатор ІПКС і ймовірність його реалізації, що відповідає лінгвістичному ідентифікатору правила, що його ідентифікував, тобто $IKS_i \to LI_i$. Крім того здійснюється привязка до правила, за яким ІПКС був ідентифікований. В БВ формується остаточний результат і виводиться на екран оператора системи. На екрані відображені

наступні дані: конкретний тип ІПКС, лінгвістичний ідентифікатор імовірності його реалізації та використовуване правило: $< IKS_i \rightarrow LI_i, ER_{ip} >$.

В роботі запропоноване нове структурне рішення, на основі якого можна розробляти алгоритмічне, програмне і програмно-апаратне забезпечення, що застосовується для виявлення та ідентифікації ІПКС в різних середовищах, зокрема в ІКСМ. Робота описаної СВІПКС заснована на методі виявлення ІПКС. Система працює з заданими нечіткими параметрами, за якими здійснюється ідентифікація ІПКС. За рахунок використання методів нечіткої логіки та експертних підходів система може бути використана в нечіткому слабоформалізованому просторі, а також не потребує великих затрат часових і виробничих ресурсів для збирання та опрацювання статистичних даних, обробки складних математичних моделей теорії імовірності. Запропонована СВІПКС може використовуватись автономно або як складова комплексної системи захисту інформації.

СПИСОК ИСПОЛЬЗОВАНЫХ ИСТОЧНИКОВ

1.Гізун А. І. Аналіз сучасних систем управління кризовими ситуаціями / А.І. Гізун, А.О. Корченко, С.О. Скворцов // Безпека інформації. – 2015. – Т.21. – №1.
2.Корченко А.А. Система выявления аномального состояния в компьютерных сетях / А.А. Корченко // Безпека інформації. – №2 (18). – 2012. – С. 80-84.
3.Корченко А. О. Система виявлення та ідентифікації порушника в інформаційно-комунікаційних мережах // А.О. Корченко, В.В. Волянська, А.І. Гізун / Безпека інформації. – 2013. – Т.19. – №3. – С. 158-162.
4.Іванченко Є. В. Базова архітектура експертної системи прогнозування та попередження кризових ситуацій / Є.В. Іванченко, О.В. Гавриленко, А.І. Гізун // Захист інформації. - 2012. - № 3. - С. 94-104.
5.Корченко А.Г. Построение систем защиты информации на нечетких множествах : Теория и практические решения / А.Г.Корченко. — К. : МК-Пресс, 2006. — 320 с.
6.Гізун А. І. Основні параметри для ідентифікації порушника інформаційної безпеки / А.І. Гізун, В.В. Волянська, В.О. Риндюк, С.О. Гнатюк // Захист інформації. – 2013. – Т.15. – №1. – С. 66-75.
7.Азарсков В. Параметры прогнозирования и идентификации атак в информационно-коммуникационных системах / В. Азарсков, А. Гизун, А. Грехов, С. Скворцов // Захист інформації. - 2014. - 16, № 1. - С. 89-95.

Васєв Володимир Олександрович, *нач. відділу,*
Управління Державної служби спеціального зв'язку
та захисту інформації в Миколаївській області

ПРИНЦИПИ ПОБУДОВИ ЗАХИЩЕНИХ СИСТЕМ ПАКЕТНОЇ ПЕРЕДАЧІ ДАНИХ НА ОСНОВІ IP-ПРОТОКОЛУ

Системи пакетної передачі даних на основі IP-протоколу забезпечують інформаційний обмін усіма видами інформації в телекомунікаційних мережах і мають високі показники гнучкості, масштабованості та легкості взаємодії з іншими вузлами та системами зв'язку. Найбільш поширеною сферою використання таких систем є організація глобальної мережі Інтернет та інших комп'ютерних мереж, передача електронної пошти, інших видів інформації (даних, аудіо, відео), організація телефонного зв'язку (IP-телефонія), відеоконференцзв'язку, побудова складних систем сигналізації, відеоспостереження, контролю доступу тощо. Для встановлення зв'язку між територіально рознесеними терміналами можуть використовуватися будь-які комп'ютерні мережі, глобальна мережа Інтернет, а також цифрові транспортні мережі загального користування по каналах оптичного, дротового, супутникового, радіорелейного та стільникового (GPRS, 3G, 4G) зв'язку. Проте, актуальною проблемою залишається необхідність забезпечення

конфіденційності та цілісності даних, авторизації джерела даних, унеможливлення аналізу трафіку та топології мережі. Для вирішення цих питань створюються захищені мережі передачі даних на базі сучасного цифрового обладнання.

Побудова захищеної мережі передачі даних здійснюється за допомогою засобів шифрування трафіку IP-мереж відповідного рівня таємності, центру сертифікації ключів (ЦСК), пристроїв генерації ключових даних, централізованої система керування (або робоча станція адміністратора) та кінцевого обладнання обробки інформації (захищені локальні обчислювальні мережі). IP-шифратори забезпечують шифрування та контроль цілісності потоків мережних IP-пакетів, що передаються через них між розподіленими ЛОМ або між клієнтами та ЛОМ.

Пристрої генерації ключових даних призначені для генерації, зберігання та розподілу особистих ключів. ЦСК забезпечує сертифікацію відкритих ключів IP-шифраторів, адміністратора та клієнтів з метою розподілу повноважень та надання доступу до інформаційних ресурсів. Розподілення ключів здійснюється двома методами: передачею мережею шифрованого зв'язку та/або на носіях ключових даних. Централізована система керування (РС адміністратора) призначена для управління мережею, налагодження параметрів конфігурації, моніторингу та протоколювання подій, перегляду статистичної інформації.

Приклад побудови захищеної IP-мережі наведено на рис.1.

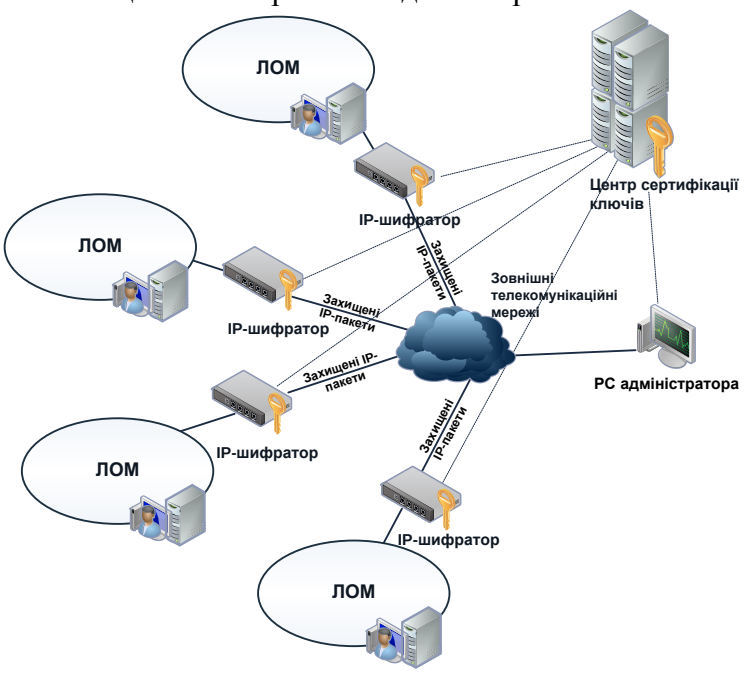


Рис.1. Структурна схема організації захищеної IP-мережі.

Засоби захисту трафіку IP-мереж (IP-шифратори) призначені для криптографічної обробки IP-пакетів, що передаються між локальними обчислювальними мережами (ЛОМ), окремими персональними комп'ютерами та IP-терміналами скрізь мережу загального користування [3]. IP-пакети, отримані через внутрішні мережні інтерфейси із ЛОМ, зашифровуються та захищаються контрольною сумою і маршрутизуються на зовнішній інтерфейс для передачі через зовнішні мережі. При цьому отримані IP-пакети після зашифрування інкапсулюються у нові IP-пакети, у поле даних якого інкапсулюється зашифрований оригінальний IP-пакет або команди керування, а заголовки містять IP-адресу відправника й одержувача, задані в конфігурації засобу захисту. IP-пакети, отримані через зовнішні інтерфейси із зовнішньої мережі, розшифровуються та перевіряються на цілісність і маршрутизуються на внутрішній інтерфейс для передачі у ЛОМ. При цьому заголовок IP-пакету відновлюється у початкове (оригінальне) значення. Таким чином передача сформованих нових IP-пакетів між взаємодіючими засобами утворює захищене віртуальне

з’єднання (VPN-тунель) у відкритій IP-мережі.

Сьогодні в Україні серійно виробляється низка засобів криптографічного захисту інформації (КЗІ) в IP-мережах, що мають позитивні експертні висновки, зареєстровані в Адміністрації Держспецв’язку та допущені для захисту інформації з обмеженим доступом [2]. До таких засобів належать О-271Е, О-371Е, Скат-Е, Гном-Е, Пелена-Е (ТОВ «Трител»), Онікс-100, Онікс-200 (НВФ «Криптон»), CryptoIP-448, CryptoIP-459D/DO (ТОВ «АВТОР»), Канал-201, Канал-201 (ТОВ «ІІТ») та інші. Один з видів продукція виробництва ТОВ «Трител» наведено на рис.2.

Рис 2. Продукція виробництва ТОВ «Трител»

Приклад побудови захищеної IP-мережі спеціального призначення з використанням продукції виробництва ТОВ «Трител» наведено на рис.3.

Рис.3. Схема організації захищеної IP-мережі спеціального призначення.

До телекомунікаційних мереж спеціального призначення, призначених для обробки державних інформаційних ресурсів, висуваються підвищені вимоги щодо їх надійності та забезпечення конфіденційності інформації. Захист інформації в таких системах здійснюється засобами технічного та криптографічного захисту, що запобігає несанкціонованому доступу

до інформації, порушенню її цілісності, достовірності, перехопленню у відкритих каналах зв'язку, а також витоку технічними каналами [4].

Відповідно до законодавства України, для криптографічного захисту інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або яка є власністю держави, використовуються криптосистеми і засоби КЗІ, допущені до експлуатації встановленим порядком [1]. Такі засоби повинні мати позитивний експертний висновок або сертифікат відповідності в сфері КЗІ. Крім того, все кінцеве обладнання обробки та комутації інформації (маршрутизатори, комп'ютери, IP-телефони, термінали відеоконференцзв'язку тощо) повинне мати комплексну систему захисту інформації (КСЗІ), що забезпечує захист від витоку інформації технічними каналами (ПЕМВН) та несанкціонованого доступу (НСД). Підтвердження відповідності КСЗІ здійснюється за результатами державної експертизи [4]. Засоби КЗІ та кінцеве обладнання можуть застосовуватися на стаціонарних та рухомих об'єктах (комплексних апаратних зв'язку). Вони повинні мати резервні джерела живлення та надійні (дублюючі) канали зв'язку.

Висновок.

Враховуючи актуальність проблеми захисту інформації, побудова захищених телекомунікаційних мереж є пріоритетною задачею державної політики у сфері інформатизації. Система захисту інформації має бути інтегрована в процес створення та розвитку інформаційних систем як обов'язковий елемент.

Джерела:

1. Указ Президента України від 22.05.98 №505/98 «Про затвердження Положення про порядок здійснення криптографічного захисту інформації в Україні».

2. Офіційний веб-сайт Держспецв'язку: www.dsszzi.gov.ua.

3. Веб-сайт ТОВ «ІІТ»: www.iit.com.ua.

4. Веб-сайт ТОВ «Трител»: www.tritel.ua.

Гур'єв Володимир Іванович, *к. т. н.,*
Чернігівський національний технологічний університет

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ХМАРНИХ ОБЧИСЛЕНЬ У ВНЗ

Хмарні обчислення є динамічним і масштабованим способом доступу до зовнішніх обчислювальних ресурсів у якості сервісу, що надається через Інтернет, при цьому користувачу не потрібно ніяких спеціальних знань про інфраструктуру "хмари" або навичок управління цією «хмарною» технологією.

Під "хмарою", звичайно треба розуміти не сам Інтернет, а весь той набір апаратного та програмного забезпечення, який забезпечує обробку та виконання замовлень клієнта «з іншого боку». Якщо не мудрувати з означеннями і побачити сутність, навіть сама проста дія через Інтернет - запит сторінки сайту, до певної міри, є прикладом хмарних обчислень. Інтернет, власне, виник саме для того, щоб забезпечити віддалений доступ до обчислювальних ресурсів.

Термін "хмарні обчислення" (англ.- cloud computing) застосовується до всіх послуг, які надаються через Інтернет. Поява англійського терміну почало активно обговорюватися у 2008 році на одній з тематичних інтернет конференцій. В результаті обговорень були різні версії, за однією з яких термін **cloud** був вперше використаний головою компанії **Google** Шмідтом і отримав поширення в засобах масової інформації. Інша популярна версія припускає, термін **cloud computing**, став широко використовуватися у Сполучених Штатах з 2005 року, після запуску компанією Amazon проекту **Elastic Compute Cloud** (Amazon EC2) і був широко поширений в науковому середовищі, бізнесі, серед постачальників інформаційних технологій.

Термін «хмара» використовується як метафора, що базується на зображенні Інтернету на діаграмі комп'ютерної мережі, або як образ комплексної інфраструктури, яка приховує всі технічні подробиці.

Зараз важко знайти того, хто першим придумав малювати на схемах хмари, але ідея прижилася, міцно увійшла до практики і врешті-решт з легкої руки професора Рамната К. Челлапа (Ramnath K. Chellappa) з школи бізнесу університету Еморі (Атланта, Джорджія), який запропонував рахувати обчислення економічними , а не технічним явищем, яке і дало підставу новому типу обчислень - Cloud Computing, яке і перекладають на інші мови як – «хмарні обчислення»

Суть хмарних обчислень — надання користувачам віддаленого доступу до послуг, обчислювальним ресурсам та додаткам (включаючи операційні системи та інфраструктуру) через мережу Інтернет. Розвиток цієї сфери хостингу було обумовлено необхідністю програмного забезпечення та цифрових послуг, якими можна управляти зсередини, але які були б більш рентабельними і ефективними.

Ці Інтернет-послуги, які також називають «хмарними сервісами» можна поділити на три основні категорії:

- інфраструктура як сервіс;
- платформа як сервіс;
- програмне забезпечення як сервіс.

У порівнянні з традиційним підходом, хмарні сервіси дають змогу керувати більш значними інфраструктурами, обслуговувати різні групи користувачів в межах однієї хмари, а також означають повну залежність від провайдера хмарних послуг.

При наданні хмарного сервісу використовується тип оплати "плата за використання". Зазвичай за одиницю виміру часу роботи приймається хвилина або година користування ресурсами. При оцінюванні обсягу даних за одиницю виміру приймається Мегабайт інформації, що зберігається. При цьому користувач оплачує тільки той об’єм ресурсів, що в дійсності був використаний протягом деякого часу. Крім того, хмарна інфраструктура дозволяє користувачеві, за бажанням, "підняти" і "опустити" максимальні обмеження ресурсів, скориставшись гнучкість сервісу, що надається. Споживачеві хмарних послуг, не потрібно турбуватися про інфраструктуру, яка забезпечує функціональність послуги. Усі завдання для налаштування, усунення несправностей, розширення інфраструктури та ін. бере на себе сервис-провайдер.

Існують різні базові варіанти розгортання «хмарних середовищ»:

- приватна (закрита) хмара, що використовується для послуг в рамках компанії і замовника та постачальника послуг (компанія створює "хмару" для себе, в рамках цієї організації;
- громадська (відкрита) хмара, що використовується «хмарним» провайдером для надання зовнішнім клієнтам сервісів хмарної структури;
- змішана (або гібридна) хмара, використовується в поєднанні з двома вище вказаними варіантами розгортання.

Переваги хмарних обчислень

- Користувач оплачує за послуги тільки коли це необхідно, і саме головне він платить тільки за те, що використовує.

- Хмарні технології дозволяють економити на придбанні, підтримці модернізації програмного забезпечення та устаткування.

- Масштабованість, відмовостійкість та безпека - автоматичне виділення і звільнення необхідних ресурсів в залежності від потреб застосування. Технічне обслуговування, оновлення ПЗ проводить провайдер послуг.

- Віддалений доступ до даних у хмарі - можна працювати з будь-якої точки на планеті, де є доступ в Інтернет.

Недоліки хмарних обчислень

- Користувач не має доступу до внутрішньої хмарної інфраструктури. Збереження даних користувачів залежить від компанії інтернет-провайдера.

- Не всі дані можна довіряти провайдеру в Інтернеті, не тільки для зберігання, але навіть для обробки.

- Не кожен додаток дозволяє зберегти, наприклад, на флешку проміжні етапи обробки інформації, а також кінцевий результат роботи, але ж результати онлайн зручні не завжди.

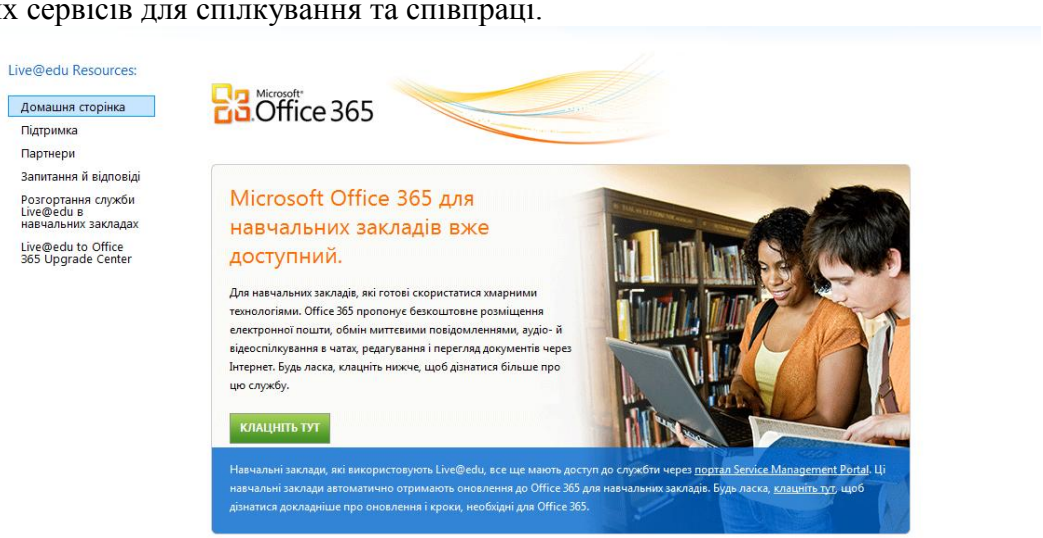
- Існує ризик, що провайдер онлайнових послуг одного разу не зробить резервного копіювання даних, і вони будуть втрачені в результаті аварії на сервері.

- Довіряючи свої дані інтернет-сервісу, ви втрачаєте контроль над ними і обмежуєте свою свободу.

Компанія Microsoft, є одним з лідерів у забезпеченні послуг хмарних обчислень і в самому найближчому майбутньому планує надавати можливість створювати, публікації та редагування документів Word, Excel, PowerPoint і OneNote в онлайні через Microsoft Office Web Apps і браузер Microsoft Internet Explorer, Mozilla Firefox і Apple Safari.

Компанія TechExpert вперше в Україні пропонує своїм клієнтам інноваційне рішення - впровадження хмарних технологій Microsoft Live@edu, IT-інфраструктур навчального закладу.

Новітній сервіс Microsoft Live@edu – це безкоштовне рішення для організації електронної пошти для студентів, випускників, співробітників і викладачів, а також набір користувацьких сервісів для спілкування та співпраці.



Актуальність даної послуги зумовлена тим, що більшість українських ВНЗ стикається з проблемою легалізації, придбання й оновлення ПЗ, а сервіс Live@edu дозволяє мінімізувати витрати на ці завдання, при цьому забезпечує широку функціональність.

Це рішення дозволяє організувати централізоване управління корпоративною електронною поштою, без необхідності закупівлі сервера та коштовного програмного забезпечення. А також, організувати онлайн розклад пар доступного безпосередньо з пошти, особисті і загальні файлові сховища, створити простір для спільної роботи.

Сучасні комп’ютерні технології дозволяють студентам та викладачам використовувати для спілкування та роботи декілька пристроїв: ноутбуки, комп’ютери, смартфони, мобільні

телефони тощо. Інструменти Google, Apps підтримуються самими різними пристроями, тому є загальнодоступною і універсальною ІТ-технологією для роботи у освітньому середовищі.

Для дистанційного навчання можна використовувати безкоштовну програму Skype – на сьогодні найбільш доступна технологія для онлайн спілкування викладача та студента.

Існує багато хмарних сервісів, які можна використовувати у освітньому процесі. Одним з найбільш ефективних та актуальних сервісів є застосування порталу Uztest/ru – це сайт, що має вигляд віртуального кабінета вчителя, у якому розміщено інформаційні ресурси та інтерактивні сервіси для підготовки і проведення занять з математики.

Таким чином "хмарні обчислення"- область автоматизації, віртуалізації ІТ-процесів, що інтенсивно розвивається і більш модна в останні часи. Динаміка зростання таких розрахунків вражає. Так, Microsoft рішень, що використовують хмарні обчислення, не менше 70%. Amazon, Google, і т. д теж не пасуть задніх. Microsoft прогнозує на подальше 100% "хмарність" ІТ-рішень. На сьогодні "китами" індустрії хмарних обчислень вважаються Google, Amazon, Microsoft, IBM, Sun, Ubuntu і інші. Відповідно дослідженням, попит на «готових до роботи у хмарі" ІТ- професіоналів буде рости на 26% на рік до 2016 року, світ відкриває до 7 мільйонів робочих вакансій, пов'язаних з хмарою.

Список використаних джерел

1. Полумієнко С.К., Рибаков Л.О., Грінченко Т.О. ІТ проекція технологічного розвитку України. - К.: Азимут-Украина, 2011.-184 с.

2. Поленок С.П. Информационное общество как третий путь развития. Тези доповідей. Міжн. наук. конгрес ”Інформаційне суспільство в Україні ” 25-26 жовтня 2012р. - 205 с.

3. Иванников В. П. Облачные вычисления в образовании, науке и госсекторе. [Электронный ресурс]. – Режим доступа: http://paco.ipu.ru/pdf/P301.pdf

4. Гриб’юк О. О. Перспективи впровадження хмарних технологій в освіті. Київ, Інститут інформаційних технологій і засобів навчання АПН України [Электронный ресурс]. – Режим доступа: http://lib.iitta.gov.ua/1111/1/grybyuk-stattya1-hmary+_Copy.pdf

Гнатюк Сергій Олександрович, *к.т.н., доцент,*
Жмурко Тетяна Олександрівна, *аспірант,*
Національний авіаційний університет (м. Київ, Україна),
Сєйлова Нургуль Абадуллаївна, *к.т.н., доцент,*
Казахський НТУ ім. К.І. Сатпаєва (м. Алмати, Республіка Казахстан)
Стояновіч Александар, *аспірант,*
Федеральний університет Сеара (м. Форталеза, Бразилія)

МЕТОД ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА БАЗІ КВАНТОВИХ ТЕХНОЛОГІЙ

Сьогодні потужні інформаційно-комунікаційні системи (ІКС) обслуговують банки, контролюють ядерні реактори, використовуються в авіації, контролюють супутники і космічні кораблі тощо. У той же час збільшується не тільки кількість цінної (критичної) інформації, що циркулює в ІКС, але також збільшується кількість потенційних кіберзагроз. З огляду на це, існує гостра потреба у розробці та реалізації сучасних і ефективних систем інформаційної безпеки, які можуть надійно гарантувати безпеку даних, враховуючи, що більшість важливих рішень, прийнятих на різних рівнях (від президента до пересічного громадянина), залежить від основних характеристик безпеки (цілісність, доступність, конфіденційність) відповідної цінної інформації. Такі системи використовуються в Україні, особливо в банківському секторі, у сфері державного управління, на стратегічно важливих економічних об'єктах, у національній та військовій безпеці, та у більшості об’єктів національної критичної інфраструктури.

Для захисту даних найчастіше використовують різноманітні традиційні криптографічні методи захисту інформації (ЗІ). Однак, у зв'язку з швидким розвитком обчислювальних засобів (поява суперкомп'ютерів, квантових комп'ютерів, розвиток GRID-технологій тощо) міжнародне наукове товариство ставить під питання надійність сучасних методів ЗІ в ІКС. Ймовірною альтернативою можуть бути методи квантової криптографії (КК), що є найбільш розвинутим напрямком квантової теорії інформації. Основна задача КК полягає у створенні каналу передачі інформації, абсолютна захищеність якого буде гарантуватись фундаментальними законами квантової механіки, що дозволяють зафіксувати будь-яку спробу проникнення ззовні [1-3]. Однак, робота систем ЗІ на базі квантових протоколів потребує не лише використання самих протоколів, а й паралельного використання засобів класичної криптографії та завадостійкого кодування, оскільки, не менш важливими є виправлення помилок та підвищення рівня захищеності [3].

Одним із ефективних методів захисту на базі квантових технологій є пінг-понг протокол [1, 2], який не потребує великого об'єму квантової пам'яті та може використовуватися в існуючих системах (ЗІ). З огляду на це, а також з урахуванням недоліків пінг-понг протоколу [1], підвищення його ефективності (захищеності) є актуальною науковою задачею. Метою роботи є підвищення захищеності систем ЗІ на базі квантових технологій за рахунок розробки нового методу підсилення секретності.

У роботі [4] запропоновано неквантовий метод підсилення асимптотичної стійкості пінг-понг протоколу з парами повністю переплутаних кутритів. Недоліком описаного методу є те, що для передачі всього повідомлення генерується та використовується дуже велика кількість випадкових, оборотних над полем Галуа, тритових матриць, що потребує великих часових та ресурсних затрат. Для наглядного розуміння в табл. 1 наведено розмір тритових матриць у залежності від загального розміру повідомлення m та параметру r. З таблиці видно, що для передачі повідомлення розміром m квантовим каналом потрібно використовувати матриці загальним розміром $r \cdot m$ тритів. Крім того, у роботі [4] не описано як саме генеруються тритові матриці, тому не можливо оцінити їх псевдовипадковість.

Для розуміння загальних розмірів даних в бітах переведемо загальний розмір з трійкової системи числення в двійкову: 100 000 000 тритів приблизно дорівнюють 20 МБ (якщо переводити кожні 20 тритів у 32 біти). Тому, загальний розмір матриць M_i при $r = 28$ становитиме 560 МБ, які спочатку потрібно згенерувати, виконати множення M_i на a_i, потім передати класичним (неквантовим) каналом, а наприкінці обернути та виділити з $b_i - a_i$, що займе занадто багато часу. Пропонується використовувати замість матриць M_i розміром $r \times r$ ключову трійкову послідовність k_i розміром r. Повідомлення b_i буде вираховуватись за формулою $b_i = k_i + a_i$, а a_i – за формулою $a_i = b_i - k_i$, де операції "+" та "–" – означають відповідно операції потритового додавання та віднімання за модулем 3.

Таблиця 1. *Загальний розмір матриць* M_i

	Загальний розмір повідомлення *m* в тритах						
	100	1000	10000	100000	1000000	10000000	100000000
r=4	400	4000	40000	400000	4000000	40000000	400000000
r=8	832	8000	80000	800000	8000000	80000000	800000000
r=12	1296	12096	120096	1200096	12000096	120000096	1200000096
r=16	1792	16128	160000	1600000	16000000	160000000	1600000000
r=20	2000	20000	200000	2000000	20000000	200000000	2000000000
r=24	2880	24192	240192	2400192	24000192	240000192	2400000192
r=28	3136	28224	280672	2800448	28000560	280000112	2800000336

Ключова трійкова послідовність k_i буде формуватись за допомогою генератора псевдовипадкових трійкових послідовностей, та 96-тритового ключа K. Після завершення квантової передачі, у випадку відсутності атаки, замість передачі матриць M_i буде передаватись ключ K звичайним каналом зв'язку. Проаналізуємо швидкість роботи існуючого [4] та запропонованого методу підсилення секретності пінг-понг протоколу. Нехай необхідно передати за допомогою пінг-понг протоколу повідомлення довжиною $m = r \cdot l$ − трит, де r − розмір блоку даних, а l − кількість таких блоків. Позначимо як t_1 − час генерування ключових даних.

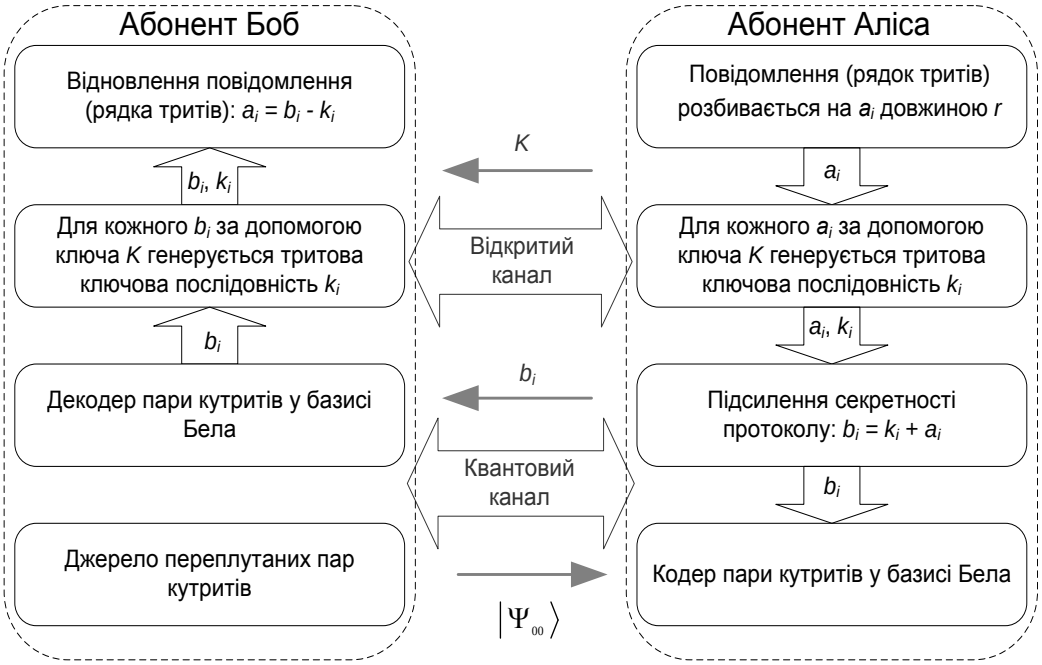


Рис.1. Загальна схема запропонованого методу підвищення захищеності

Для відомого методу підсилення секретності − час генерування оборотних матриць M_i ($i = \overline{1,l}$) розміром $r \times r$, а для запропонованого − час генерування ключової послідовності k_i розміром r. Тоді t_2 − час утворення повідомлення b_i, а t_3 − час передачі повідомлень b_i квантовим каналом за пінг-понг протоколом. Позначимо як t_4 − час передачі оборотних матриць M_i по класичному каналі для існуючого методу підсилення секретності, а для запропонованого – час передачі 96 тритового ключа K. Час формування оборотних матриць M_i^{-1} для існуючого методу підсилення або час генерування ключової послідовності k_i розміром r для запропоновано методу підсилення секретності позначимо як t_5. Тоді t_6 − час відновлення повідомлення a_i. Швидкість роботи кожного з методів буде визначатися за такою формулою: $V = \dfrac{r \cdot l}{t_1 + t_2 + t_3 + t_4 + t_5 + t_6}$ трит / сек.

Оскільки швидкість роботи протоколу залежить від V_{gen}, V_{kv}, V_{kl}, V_x, r та l, то для більш конкретної оцінки швидкостей обох методів підсилення було вирішено провести моделювання роботи протоколу з різними показниками V_{gen}, V_{kv}, V_{kl}, V_x, r та l. Для цього була запропонована модель, яка складається таких етапів:

1. На початку фіксуються базові параметри протоколу: V_{kv}, V_{kv}, V_x, V_{gen}.
2. Обирається метод підсилення безпеки пінг-понг протоколу.
3. Обирається довжина повідомлення m (10^4, 10^5, 10^6) у тритах.

4. Обирається параметр r (4, 12, 20) та розраховується параметр l.

5. Після чого для обраних параметрів V_{gen}, V_{kv}, V_{kl}, V_x, r та l розраховується загальна швидкість роботи пінг-понг протоколу, яку заносять у таблицю для подальшої обробки.

Результати моделювання наведені в табл. 2, причому для моделювання роботи протоколу обрано 5 різних комбінацій параметрів V_{gen}, V_{kv}, V_{kl}, V_x: $V_{gen} = 10^8$ трит / сек, $V_{kl} = V_x = V_{kv} = 10^6$ трит / сек. $V_x = 10^8$ трит / сек, $V_{kl} = V_{gen} = V_{kv} = 10^6$ трит / сек. $V_{kv} = 10^8$ трит / сек, $V_{kl} = V_x = V_{gen} = 10^6$ трит / сек. $V_{kl} = 10^8$ трит / сек, $V_{gen} = V_x = V_{kv} = 10^6$ трит / сек. $V_{gen} = V_{kl} = V_x = V_{kv} = 10^6$ трит / сек.

Таблиця 2. *Швидкість роботи методів підсилення секретності в трит / сек*

Комб. парам.	Методи підсилення	$m = 10000$ трит			$m = 100000$ трит			$m = 1000000$ трит		
		$r = 4$, $l = 2500$	$r = 12$, $l = 834$	$r = 20$, $l = 500$	$r = 4$, $l = 25000$	$r = 12$, $l = 8334$	$r = 20$, $l = 5000$	$r = 4$, $l = 250000$	$r = 12$, $l = 83334$	$r = 20$, $l = 50000$
1	Відомий	14916	1703	617	14916	1703	617	14916	1703	617
	Новий	330076	33076	33076	331020	331020	331020	331115	331115	331115
2	Відомий	103950	32530	17550	103950	32530	17550	103950	32530	17550
	Новий	330076	330076	330076	331020	331020	331020	331115	331115	331115
3	Відомий	14263	1672	610	14263	1672	610	14263	1672	610
	Новий	248780	248781	248781	249316	249316	249316	249370	249370	249370
4	Відомий	14916	1703	617	14916	1703	617	14916	1703	617
	Новий	199996	199996	199996	199999	199999	199999	199999	199999	199999
5	Відомий	14084	1669	610	14084	1669	610	14084	1669	610
	Новий	199616	199617	199616	199961	199961	199961	199996	199996	199996

Як видно з табл. 2 при збільшені параметра r швидкість запропонованого методу не змінюється, а швидкість методу [4] зменшується у 6-24 рази (в залежності від параметрів V_{gen}, V_{kv}, V_{kl}, V_x). При збільшені параметру l швидкості методів практично не змінюються. Швидкість роботи запропонованого методу у порівняні з відомим збільшується у мінімум у 3 рази і залежить від параметрів V_{gen}, V_{kv}, V_{kl}, V_x, r та l. Таким чином, використання запропонованого методу підвищення захищеності дозволить також підвищити швидкість роботи пінг-понг протоколу.

Список використаної літератури

1.Quantum Secure Telecommunication Systems / [Oleksandr Korchenko, Petro Vorobiyenko, Maksym Lutskiy, Yevhen Vasiliu, Sergiy Gnatyuk] // Telecommunications Networks: Current Status and Future Trends / edited by Jesus Hamilton Ortiz. — Rijeka, Croatia : InTech, 2012. — P. 211-236.

2.Korchenko O. Modern quantum technologies of information security against cyber-terrorist attacks / O. Korchenko, Ye. Vasiliu, S. Gnatyuk // Aviation. Vilnius: Technika, 2010, V. 14, № 2, pp. 58-69.

3.Корченко О.Г. Імітаційне моделювання роботи системи квантового прямого безпечного зв'язку із застосуванням завадостійких кодів для кутритів / О.Г. Корченко, Є.В. Василіу, С.О. Гнатюк, В.М. Кінзерявий // Захист інформації. — 2011. — №2 (51). — С. 61-69.

4.Василиу Е.В. Синтез основанной на пинг-понг протоколе квантовой связи безопасной системы прямой передачи сообщений / Е.В. Василиу, С.В. Николаенко // Наукові праці ОНАЗ ім. О.С. Попова. — 2009, № 1. — С. 83-91.

Струбицький Павло Романович, *к.т.н., доцент,*
Тернопільський національний економічний університет

ПРОБЛЕМИ І АСПЕКТИ ЗБОРУ СОЦІАЛЬНИХ ДАНИХ В ІНТЕРНЕТ – МЕРЕЖАХ

Аналіз соціальних даних стрімко набирає популярність у всьому світі [1, 2] завдяки появі у 1990-х роках онлайнових сервісів соціальних мереж (SixDegrees, LiveJournal, Facebook, Twitter, YouTube та ін.). З цим пов'язаний феномен соціалізації персональних даних: стали публічно доступними факти біографії, листування, щоденники, фото-, відео-, аудіоматеріали, замітки про подорожі і т.д. Таким чином, соціальні мережі є унікальним джерелом даних про особисте життя і інтереси реальних людей. Це відкриває безпрецедентні можливості для вирішення дослідницьких і бізнес-задач (багато з яких до цього неможливо було вирішувати ефективно через нестачу даних), а також створення допоміжних сервісів і додатків для користувачів соціальних мереж. Крім того, цим обумовлюється підвищений інтерес до збору й аналізу соціальних даних з боку компаній і дослідницьких центрів.

Аналітичне агентство Gartner опублікувало звіт під назвою "Цикл ажіотажу для технологій, що розвиваються» [6]. Згідно зі звітом, технології "Соціальна аналітика" і "Великі дані" в даний час знаходяться на так званому "Піку завищених очікувань". Зокрема, дослідженнями соціальних даних активно займаються університети Карнегі-Меллон, Стенфорд, Оксфорд, INRIA, а також компанії Facebook, Google, Yahoo!, LinkedIn і багато інших. Компанії-власники сервісів онлайнових соціальних мереж (Facebook, Twitter) активно інвестують в розробку вдосконалених інфраструктурних (Cassandra, Presto, FlockDB, Thrift) і алгоритмічних (нові алгоритми пошуку та рекомендації користувачів, товарів і послуг) рішень для обробки великих масивів даних користувача. Виникають і успішно розвиваються комерційні компанії, що надають послуги з доступу до сховищ соціальних даних (GNIP), збору соціальних даних за заданими сценаріями, соціальної аналітики, а також розширенню існуючих платформ за допомогою соціальних даних.

Таким чином, фахівці з дослідницьких центрів і компаній всього світу використовують дані соціальних мереж для моделювання соціальних, економічних, політичних та інших процесів від персонального до державного рівня з метою розробки механізмів впливу на ці процеси, а також створення інноваційних аналітичних і бізнес-додатків і сервісів.

Разом з тим, при роботі з соціальними даними потрібно брати до уваги такі фактори, як нестабільність якості користувацького контенту (спам і неправдиві акаунти), проблеми із забезпеченням приватності особистих даних користувачів при зберіганні та обробці, а також часті оновлення моделі користувачів і функціоналу. Все це вимагає постійного вдосконалення алгоритмів вирішення різних аналітичних та бізнес-завдань.

Обробка соціальних даних вимагає також розробки відповідних алгоритмічних та інфраструктурних рішень, що дозволяють враховувати їх розмірність. Наприклад, база даних соціальної мережі Facebook на сьогоднішній день містить більше 1 мільярди акаунтів користувачів і більше 100 мільярдів зв'язків між ними. Кожен день користувачі додають більше 200 мільйонів фотографій і залишають більше 2 мільярдів коментарів до різних об'єктів мережі. На сьогоднішній день більшість існуючих алгоритмів, що дозволяють ефективно вирішувати актуальні завдання, не здатні обробляти дані подібної розмірності за прийнятний час. У зв'язку з цим, виникає потреба в нових рішеннях, що дозволяють здійснювати розподілену обробку та зберігання даних без істотної втрати якості результатів.

Веб-інтерфейси соціальних мереж є джерелами даних реального часу і призначені для перегляду та взаємодії зі сторінками соціальної мережі у веб-браузері або для використання даних користувачів спеціалізованими додатками. Оскільки сценарії використання інтерфейсів соціальних мереж не передбачають автоматичного збору даних множини користувачів з метою побудови соціального графа, то виникає ряд проблем:

1. Приватність даних - часто доступ до даних користувачів дозволений тільки для зареєстрованих і авторизованих учасників мережі, що вимагає підтримки емуляції користувача сесії за допомогою спеціальних облікових записів (аккаунтів).

2. Слабка структурованість даних - у багатьох випадках програмні інтерфейси (API) соціальних мереж мають обмежений функціонал, що вимагає підтримки отримання за допомогою користувацького веб-інтерфейсу статичних копій HTML-сторінок, коректної обробки їх динамічної частини (включаючи виконання асинхронних запитів до сервера соціальної мережі), вилучення потрібних даних за допомогою алгоритму та/або шаблону і побудови їх структурованого уявлення, зручного для подальшої автоматичної обробки.

3. Обмеження доступу та блокування - з метою запобігання несанкціонованого автоматичного збору даних і обмеження навантаження на інфраструктуру сервісу соціальної мережі власники сервісів часто вводять явні чи приховані обмеження на допустиму кількість запитів від одного акаунта користувача і/або IP-адреси в одиницю часу, що вимагає обліку кількості посилаються запитів, а також підтримки динамічної ротації використовуваних для збору даних акаунтів користувача і IP-адрес.

4. Розмірність даних обумовлює необхідність в паралельному методі збору даних, а також в методах отримання репрезентативної вибірки користувачів соціальної мережі.

У зв'язку з постійною необхідністю отримання великих наборів даних із соціальних мереж, потрібно розробити відповідний інструмент, можливо у вигляді фреймворку, для збору даних з різних інтернет-сервісів.

Інструмент повинен підтримувати скачування даних із соціальних мереж Facebook, Twitter. Також, бажано, щоб було реалізовано декілька способів отримання репрезентативних вибірок користувачів соціальних мереж. Реалізація механізмів автоматичного вибору облікового запису соціальної мережі для кожного запиту, а також підтримка проксі-з'єднань. Це забезпечує стійкість до блокувань за IP-адресами і облікових записів. Крім того, фреймворк мав би підтримувати багатопотокове скачування.

Незважаючи на наявність засобів для збору даних із соціальних мереж і великої кількості доступних наборів даних, актуальною є задача створення моделей випадкових соціальних графів та інструментів для генерації випадкових графів із заданим набором властивостей. Для достовірного тестування методів аналізу соціальних даних вони повинні бути застосовані до множини наборів даних з різними властивостями. Наприклад, методи пошуку співтовариств користувачів в соціальному графі можуть показувати істотно різні результати залежно від розміру вихідного графа, середнього ступеня вершини, коефіцієнта кластеризації та інших структурних властивостей. Збір необхідних для достовірного тестування реальних даних утруднений не тільки внаслідок часових витрат на скачування і обробку великих масивів слабоструктурованої інформації, але і в силу складності управління процесом збору з метою отримання набору даних з конкретним набором властивостей.

Тому, доцільно розробити модель і метод для генерації випадкових графів, що володіють основними властивостями соціальних мереж (розподіл ступенів, діаметр, коефіцієнт кластеризації і т.д.) і заданою структурою співтовариств користувачів. Для кожного користувача здійснюється генерація атрибутів профілю, соціальних зв'язків, спільнот і текстових повідомлень.

При заповненні свого профілю в соціальній мережі користувачі часто помилково або навмисно не заповнюють деякі поля або дають неправдиву інформацію про факти своєї біографії, інтереси та вподобання. Крім того, в контентних мережах (Twitter, YouTube) користувацький профіль часто обмежений набором базових атрибутів, недостатнім для вирішення багатьох завдань, що припускають персоналізацію результатів.

Таким чином, актуальні методи часткової ідентифікації авторів повідомлень за значеннями їх демографічних атрибутів. Зокрема, в системах інтернет-маркетингу та рекомендацій особливу важливість представляє визначення демографічних атрибутів користувача для цільового просування товарів і послуг в групах користувачів з однаковими

значеннями атрибутів. Крім інтернет-сервісів, такі демографічні характеристики знаходять застосування в різних дисциплінах: соціологія, психологія, кримінологія, економіка, управління персоналом та ін.

Демографічні атрибути можна умовно розділити на категоріальні (стать, національність, раса, сімейний стан, рівень освіти, професія, працевлаштованість, релігійні та політичні погляди) і чисельні (вік, рівень доходів). Умовність розподілу пов'язана з тим, що значення чисельного атрибуту можна відобразити в набір категорій і надалі розглядати цей атрибут як категоріальний. Зокрема, значення віку можна розділити на кілька вікових категорій, що часто застосовується на практиці.

1. Najork M., Wiener J. L. Breadth-first crawling yields high-quality pages // Proceedings of the 10th international conference on World Wide Web. – ACM, 2001. – С. 114-118.

2. Leskovec J., Faloutsos C. Sampling from large graphs //Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining. – ACM, 2006. – С. 631-636.

3. Gjoka M. et al. Practical recommendations on crawling online social networks //Selected Areas in Communications, IEEE Journal on. – 2011. – Т. 29. – No. 9. – С. 1872-1892.

4. Boyd, D. M. and Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. Journal of Computer-Mediated Communication, 13(1), article 11

5. George Pallis, Demetrios Zeinalipour-Yazti, Marios D. Dikaiakos. Online Social Networks: Status and Trends. New Directions in Web Data Management 1, Studies in Computational Intelligence Volume 331, 2011, pp 213-234

6. Francois Fleuret. Fast Binary Feature Selection with Conditional Mutual Information // JMLR, 5:1531–1555, 2004

7. Koby Crammer, Ofer Dekel, Joseph Keshet, Shai Shalev-Shwartz, Yoram Singer. Online Passive-Aggressive Algorithms // JMLR, 7(Mar):551–585, 2006

Струбицький Ростислав Павлович, *аспірант,*
Національний університет «Львівська політехніка»

ПІДХОДИ ДО МУЛЬТИПЛЕКСУВАННЯ ПЕРЕДАЧІ ДОКУМЕНТІВ У РОЗПОДІЛЕНИХ МЕРЕЖАХ

Обсяги інформації та бази даних, з якими працюють сьогоднішні підприємства і компанії з кожним роком зростають у геометричній прогресії. Зростають запити керівників підприємств не тільки до швидкості роботи машин з величезними обсягами інформації, але й до якості, надійності зберігання даних, накопичувачів інформації. Саме тому правильно обрана система зберігання даних — дуже важлива складова успіху в бізнесі. Використання хмаркового сховища даних, дозволяє не тільки забезпечити резервування даних, але й розміщення їх поблизу споживача даних.

При виборі високошвидкісних протоколів передачі даних, слід звернути увагу на можливість мультиплексування документів, та отримання одного документа з різних джерел.

Мультиплексування документів необхідне для одночасного отримання декількох документів з одного джерела. При використанні почергового отримання документів, користувач може стикнутися із проблемою, коли отримання досить малих робочих документів, може відкластися на великий проміжок часу через попадання в чергу великих документів [1].

Існують декілька видів забезпечення мультиплексування:

Канальне мультиплексування — документи діляться на пакети, кожний пакет отримує ідентифікатор документу (каналу передачі даних), який однозначно з'язує декілька пакетів, що стосуються одного документу.

Мультиплексування з розподілом у часі — мультиплексор в кожний момент часу видає в загальний канал дані одного документу, віддаючи йому всю смугу пропускання, але по чергово для документів через рівні проміжки часу.

Мультиплексування з розподілом за з'єднаннями — між двома точками передачі даних створюється стільки з'єднань, скільки потрібно одночасно передавати документів.

Оскільки використання хмаркових сховищ даних повинно забезпечувати швидкий доступ до клієнтських документів з різних куточків світу, а вузли хмаркового сховища можуть знаходитися достатньо "далеко" (поганий/повільний канал з'язку) доцільним є використання методів отримання документу з різних джерел та зіставлення його на клієнтській частині.

Існує два підходи до забезпечення даного режиму роботи:

Отримання одного файлу з одного вузла — клієнтське програмне забезпечення робить запити до вузла для отримання цілого документу. Таким чином документи приходять цілісно. Даний метод ефективніший коли на сховищі розміщено багато файлів невеликого розміру.

Отримання одного документу з різних вузлів — у даному випадку клієнтське програмне забезпечення само вирішує яку частину документу з якого вузла отримати. Таким чином з "ближчих" (з якими є кращий/швидший зв'язок) вузлів можна отримати більші частини документу. Даний метод ефективніший у випадку коли необхідно отримати один достатньо великий файл, а пропускна здатність вхідного каналу передачі даних значно перевищує передачу даних з одним вузлом (Рис. 1).

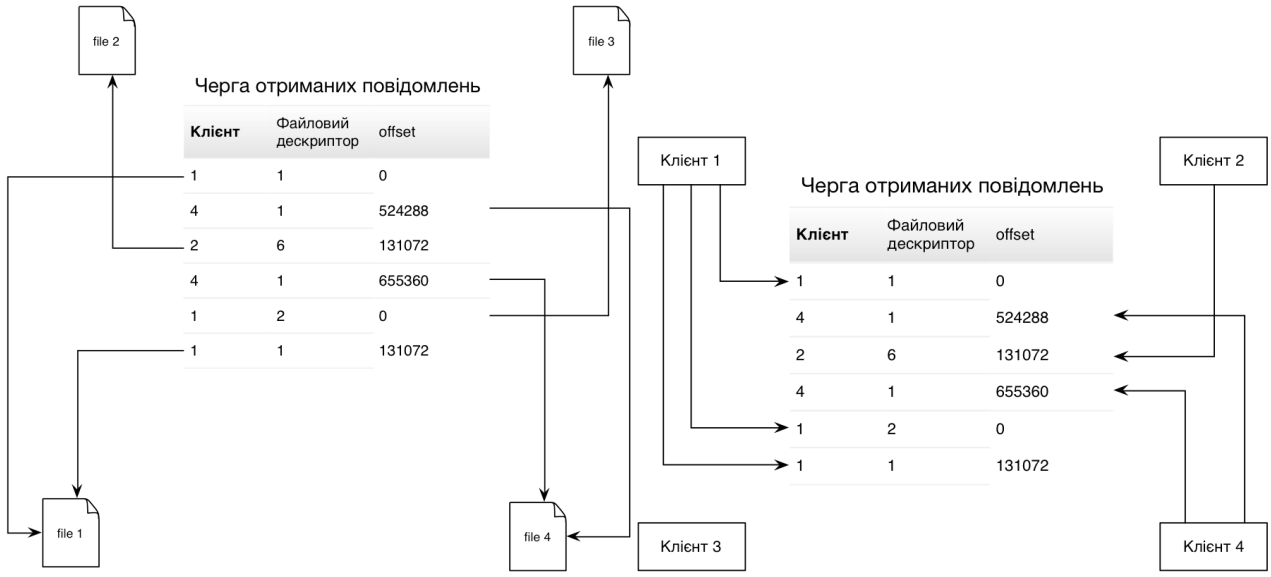


Рис. 1. Модель мультиплексування документів.

Сучасні хмаркові сховища даних, щоб залишатися конкурентними, надійними та швидкими повинні постійно удосконалювати методи та засоби надання послуг клієнтам. Так мультиплексування та зіставлення даних на даний час є однією з критичних вимог до даного сервісу.

1.Кучук, Г.А., Можаєв О.О., Воробйов О.В. Аналіз та моделі самоподібного трафіка. - Авиационно-космическая техника и технология, № 9 (2006). - С.173-180.

Нємкова Олена Анатоліївна, *к.ф.-м.н., доцент,*
Львівський інститут банківської справи УБС НБУ (м.Київ)

ШВИДКА ІДЕНТИФІКАЦІЯ ОБ'ЄКТІВ У КІБЕРПРОСТОРІ ЗА ДОПОМОГОЮ БІОМЕТРИЧНИХ ШАБЛОНІВ

Актуальність тематики обумовлена тим фактом, щоу кіберпросторі велика частина інформації представлена у вигляді зображень. Щоб знайти потрібне зображення об'єкта (ідентифікувати його) в базах даних,необхідно виконати його порівняння з великою кількістю зображень. Хешування зображень дозволяє пришвидшити цей процес, але час перебору залишається достатньо великим. Ідентифікація людини має особливості, що пов'язані з постійною зміною зображення обличчя внаслідок зміни ракурсу, іміджу, вікових змін та внаслідок стану здоров'я. Тому швидка та надійна ідентифікація об'єктів у кіберпросторі, включаючи людину, потребує подальших досліджень. На сьогодні все більше людей потребує надійної біометричної ідентифікації для можливості роботи з різноманітними інформаційними системами. Можна назвати багато таких систем:мобільний банкінг, система відеоспостереження на автобанах, система електронного уряду та інші.Таки системи характеризуються великою кількістю учасників,так що їх можна називати масовими. При впровадженні масових систем біометричної ідентифікації доводиться йти на компроміс між швидкодією та результативністю (якістю розпізнавання). Таким чином, є необхідність у розробці масових систем біометричної ідентифікації, які б відповідали сучасним вимогам швидкодії та результативності. На сьогоднішній день відомо декілька алгоритмів утворення перцептивногохешу з зображень, наприклад SimpleHash [1], DCT BasedHash [2], RadialVarianceBasedHash [2], [3] та Marr-Hildreth OperatorBasedHash [2], [4].Основні етапи алгоритму пошуку аналогічної фотографії в базах даних, включаючи утворення перцептивного хешу, є наступними:

1. Зменшення зображення до потрібного розміру в пікселях.
2. Зменшення інформативності зображення (перехід до зображення в градаціях сірого) та утворення хешу.
3. Порівняння хешей двох фото шляхом обчислення відстані між ними (відстань Хемінга). Прийняття рішення про ідентифікацію.

Для оптимізації ідентифікаційв даній роботі запропоновано наступну процедуру (розглянемо її на прикладі фото людей). Фотографія людини зменшується до трьох розмірів: 8*8 пікселів, 4*4 пікселя та 2*2 пікселя. З кожної матриці будується перцептивнийхеш за середнім. Отримаємо три різних за розмірністю бінарних матриці. Зменшення кількості пікселів в розмірі фото відповідає за укрупнення контурів зображення. Біометричний шаблон складається з трьох частин різної довжини. Перша відповідає найменшій матриці 2*2, друга – матриці 4*4, і найдовша відповідає матриці 8*8. На рис.1 зображено зменшені до різних розмірів фото чотирьох різних осіб, які умовно названі Особа1, Особа2, Особа3, Особа4, а в таблиці 1 записані відповідні біометричні шаблониПослідовність нулів та одиниць перцептивногохешу групується по чотири та записується у вигляді шістнадцяткової послідовності. У такому вигляді біометричний шаблон зберігається в базах даних. Розмір такого шаблону складає 84 біти.

Група I утворюється з бінарної матриці 2*2, група II утворюється з бінарної матриці 4*4, група III – відповідно з матриці 8*8. При пошуку первинного біометричного шаблону, якій відповідає заданому вторинному, в базі даних потрібно послідовно порівнювати значення груп I, II та III. Різні значення в групах I та II однозначно свідчать на користь того, що порівнювані шаблони належать різним людям. Такі шаблони можна далі не порівнювати. Якщо в групі III різниця невелика (не більше 5), це означає, що шаблони належать одній людині. Проведемо оцінку зменшення часу пошуку потрібного об'єкту. Нехай потрібно знайти одне з N зображень.

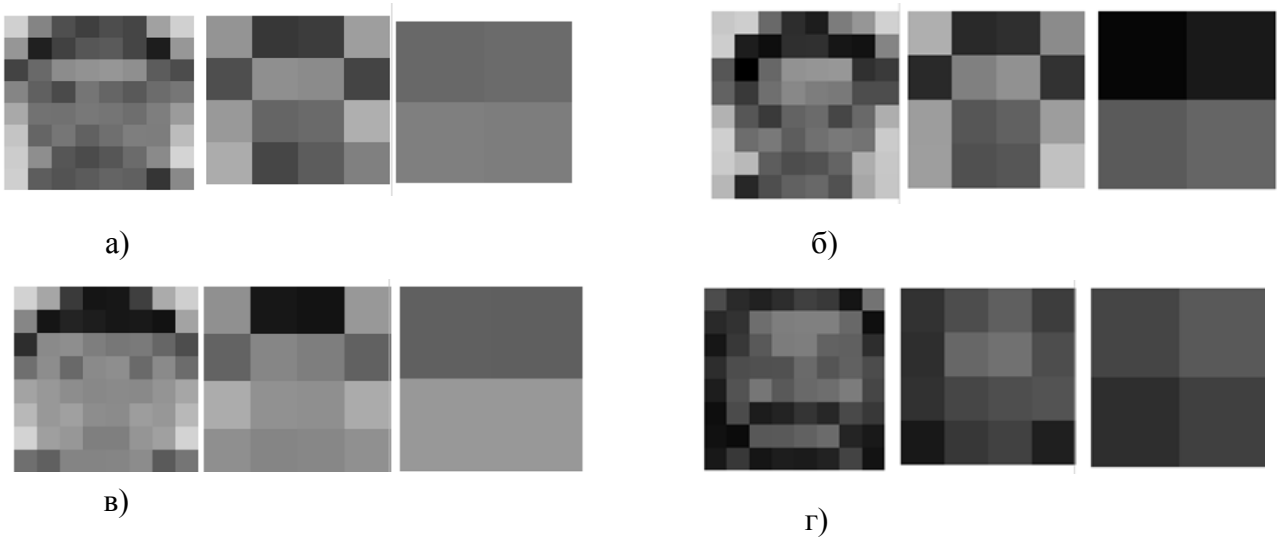


Рис.1. Зображення чотирьох осіб, зменшені до розмірів 8*8, 4*4, 2*2 пікселів.
а) – Особа 1, б) – Особа 2, в) – Особа 3, г) – Особа 4.

Таблиця 1. *Біометричні шаблони, що утворені з бінарних матриць*

№	I	II				III															
Особа 1	3	9	6	9	9	C	3	8	1	3	C	9	1	9	B	A	7	C	3	8	1
Особа 2	3	9	6	9	9	C	7	8	1	1	C	1	C	8	1	A	F	C	3	8	3
Особа 3	3	9	6	F	F	C	3	8	1	7	0	5	A	F	F	F	F	F	F	3	C
Особа 4	C	6	7	7	0	8	1	3	E	3	E	7	F	7	F	4	2	3	C	0	0

Для хешу, що містить 64 пікселі, час пошуку пропорційний величині 64N. Для складеного з груп 2*2, 4*4, 8*8 пікселівхешу цей час буде пропорційний сумі $4N + 16\alpha N + 64\beta N$, де α та β – відношення кількості розпізнаних (прийнятих до вірних) на рівні 4*4 та 8*8 хешей до загальної кількості зображень N. Для реальних об’єктів величини α та β значно менші за одиницю. Таким чином, час пошуку за запропонованим алгоритмом менше часу за вже існуючим алгоритмом у $(4N+16\alpha N+64\beta N)/64N$разів. Для подальшого дослідження представляє інтерес оцінка величин α та β для різних типів об’єктів, виходячи з практичних даних.

Висновки.

Запропоновано у якості біометричного шаблону використовувати послідовність перцептивних хешей, отриманих для зображення, яке зменшене до 8*8 пікселів, 4*4 пікселі та 2*2 пікселі. Довжина шаблону складає 84 біти. Структура біометричного шаблону дозволяє проводити швидкий пошук серед великого масиву шаблонів. Час пошуку потрібного об’єкту може бути суттєво зменшеним.

Слід відмітити перспективність таких біометричних шаблонів для застосування у платіжних системах. Кожний банкомат у цілях безпеки вже оснащений відеокамерою, яку можна використати для біометричної автентифікації. Дана технологія підходить також для мобільного банкінгу на основі смартфонів.

Використана література.

1. Simpleand DCT perceptual hash-algorithms. [electronic resource] - [access] http://www.hackerfactor.com/blog/index.php?/archives/432-Looks-Like-It.html (online).

2. Egmont-Petersen M., deRidder D., Handels H. "Imageprocessing withneuralnet works - a review". Pattern Recognition 35 (10), pp. 2279–2301(2002).

3. Standaert F.X., Lefebvre F., Rouvroy G., Macq B.M., Quisquater J.J. and Legat J.D.: Practicalevaluationof a radialsofthashalgorithm. In Proceedings of the International Symposiumon Information Technology: Codingand Computing (ITCC), vol. 2, pp. 89-94. IEEE, Apr. 2005.

4. ZengJie. A Novel Block-DCT and PCA Based Image Perceptual Hashing Algorithm. IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 3, January 2013.

Васянович Виталий Васильевич, *аспирант,*
Национальный авиационный университет

ИНТЕЛЛЕКТУАЛЬНЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Интеллектуальные технологии нашли широкое применение в вопросах информационной безопасности. В частности, без их участия не обходится построение ни одной из систем контроля и управления доступом (СКУД). Современные СКУД на объектах информационной деятельности используют биометрическую идентификацию по изображению лица человека. Распознавание лиц представляет собой бесконтактный и, возможно, наиболее естественный способ установления личности и, в отличие от других способов, может быть осуществлено даже без ведома испытуемого.

Как показывает практика, СКУД имеет один существенный недостаток – возможность подмены злоумышленником изображения реального человека его портретом, то есть попытка выдать портрет за реального человека [1]. Одним из методов устранения данного недостатка получение изображения с нескольких камер с последующим формированием 3D портрета [1,2]. Однако 3D распознавание является достаточно трудоёмким и дорогостоящим методом. В докладе предлагается более дешевый метод устранение недостатка, описанного выше, а именно – анализ траекторий движения характерных точек на изображении лица человека, получаемых с уже используемых камер наблюдения [3]. Для детектирования лица на изображении применяется алгоритм, работающий на основе поиска по цвету. Для этого используется свойство хроматических компонент цветового пространства YCbCr видеокамеры для цветных изображений (цвет лица имеет постоянный оттенок, который не совпадает с цветом фона). Применяя данный метод, получаем оконтуренное лицо на изображении (рис. 1).

Рис.1. Результат детектирования лица человека на изображении

Для поиска характерных областей, а именно областей глаз, носа и рта, используется метод интегральных проекций [4], который состоит из двух этапов: превращения цветного изображения лица в черно-белое (двух цветное, пиксель принимает два значения 0 или 1) изображение для построения интегральных проекций областей лица и выделения контрольных областей. На рис. 2 представлен результат анализа по выделению характерных фрагментов на изображении лица человека. Локализации контрольных точек осуществляется с помощью построения гистограмм яркостей каждой из выделенных областей. Для этого выделенные области поворачиваются на 90 градусов, вследствие чего матрицы, размером (M,N) преобразуются в матрицы, размером (N,M). После этого происходит сравнение каждого элемента строки матрицы, размером (N,M) с пороговым значением, которое устанавливается экспериментальным путем, и суммирование количества элементов, превышаю щих пороговое значение. В нашем случае пороговое значение было установлено равным 150. В результате сравнения и суммирования получаем матрицу, размером (N,2), где N – количество строк матрицы (N,M), 2 – количество столбцов, первый из которых содержит

номера строк от 1 до N, второй – значения сумм элементов срок матрицы (N,M), превышающих пороговое значение, для каждой строки соответственно.

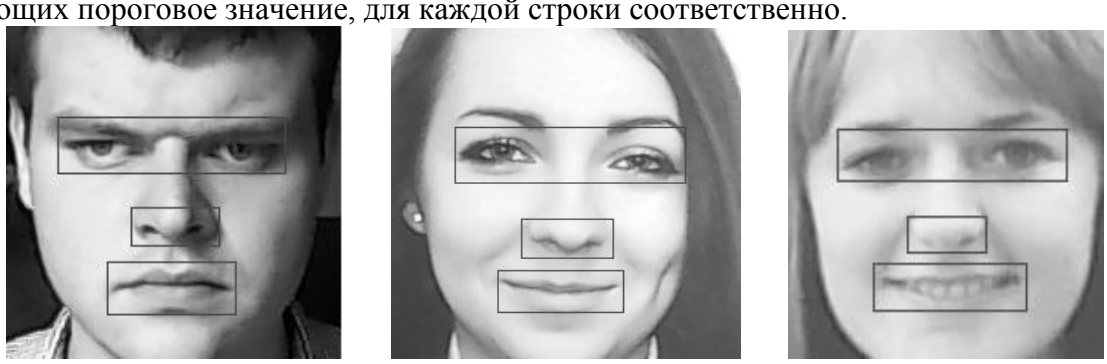


Рис.2. Характерные фрагменты на изображении лица

По результатам выполнения первых двух этапов, строятся гистограммы яркостей изображений характерных областей, которые будут служить для локализации контрольных точек на лице человека (рис. 3).

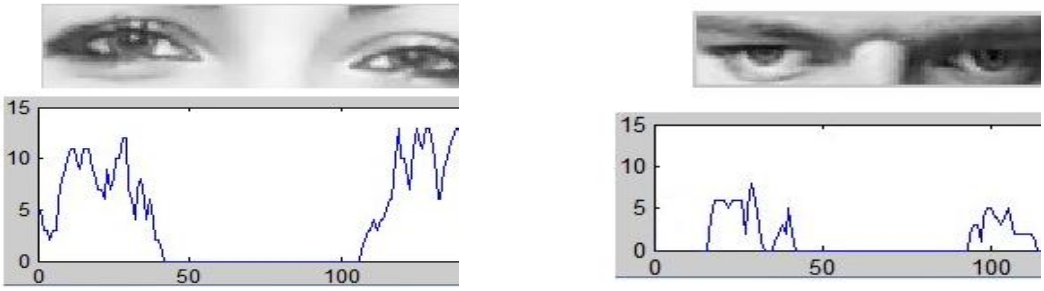


Рис.3. Гистограммы яркостей выделенных фрагментов

Далее, с помощью построенных гистограмм, определяются места расположения контрольных точек на изображении лица человека, а именно: уголки глаз, края крыльев носа, уголки рта. Вследствие сопоставления гистограмм с фрагментами выделенных областей и восстановления исходных изображений, на выходе получаем изображения лица человека с локализованными контрольными точками (рис. 4).

Рис.4. Выходные изображения с локализованными контрольными точками.

Следующим этапом является построение траекторий движения контрольных точек. Для построения траекторий движения контрольных точек (КТ) входная пара

видеопоследовательностей (реального человека и его портрета) разбивается на кадры. Для каждого из кадров применяется вышеописанный алгоритм, координаты каждой из точек записываются в файл [5], вследствие чего реализуется построение графиков, отображающих траектории движения контрольных точек (рис. 5).

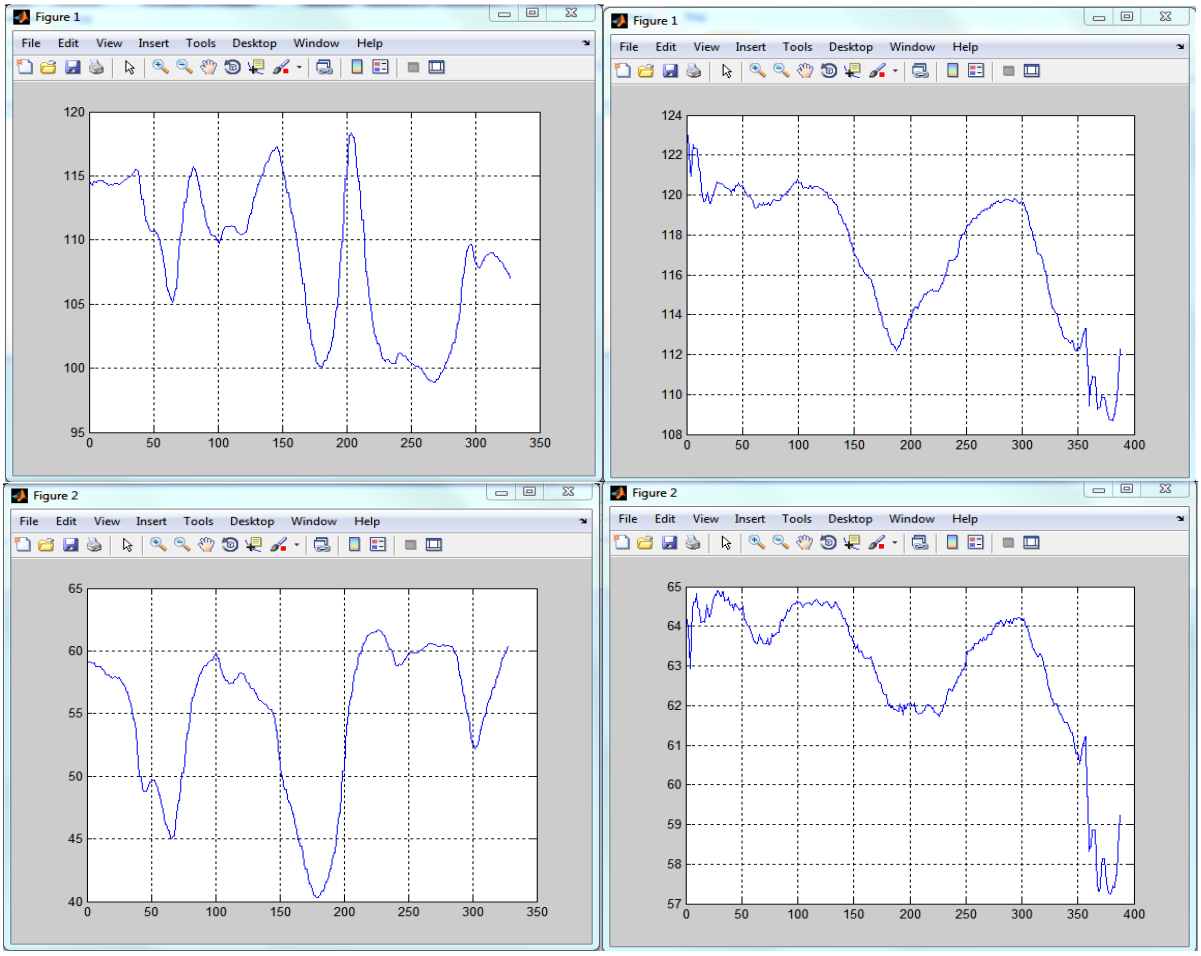


Рис. 5. Траектории изменения расстояний между КТ реального человека (слева) и портрета (справа)

В ходе исследований определено, что более эффективным является анализ изменения расстояний между соответствующими контрольными точками. Очевидно, что характеры изменения расстояний между контрольными точками реального человека и портрета существенно различаются. В настоящее время проводится разработка математического описания алгоритма по определению «реального человека» или «портрета» на изображении.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. 3D программа распознавания лиц [Электронный ресурс] − 2012. Режим доступа: http://www.youtube.com/watch?v=sXMV2TD8WYP

2. Манолов А.И. Некооперативная биометрическая идентификация по 3D-моделям лица с использованием видеокамер высокого разрешения [Электронный ресурс] / А.И. Манолов, А.Ю. Соколов // Труды 19-й Международной конференции по компьютерной графике и зрению "ГрафиКон 2009", (Москва, 5 – 9 октября 2009 г.). – М.: МАКС ПРЕСС, 2009. – Режим доступа: http://gc2009.graphicon.ru/en/proceedings

3.Швец В. А. Выделение характерных фрагментов на изображении лица человека [Текст] / В.А. Швец, В.В. Васянович, Т.В. Нимченко//Захист інформації.–2015.–№1, Том 17.–С.27– 31.

4. Лукьяница А.А., Шишкин А.Г. Цифровая обработка видеоизображений / А. А. Лукьяница, А. Г. Шишкин. - М.: "Ай-Эс-Эс Пресс", 2009. - 518 с.

5.Гонсалес Р. Цифровая обработка изображений в среде MATLAB / Р. Гонсалес, Р. Вудс, С. Эддинс. М.: "Техносфера", 2006. − 616 с.

Глущук Юрій Олексійович,
Ханько Ярослав Богданович, *аспірант,*
Національний авіаційний університет

СУЧАСНІ НАПРЯМКИ РОЗВИТКУ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ СЕРВІСІВ

Пріоритетний розвиток банківської системи та становлення інших кредитно-фінансових інститутів відіграє ключову роль у формуванні економічного розвитку держави. Зокрема, для успішного функціонування банків та їх позиціонування на ринку, необхідно чітко сформувати та управляти системою банківських послуг. Проникнення інформаційних технологій на всі рівні буденного життя докорінно змінило якість обслуговування та шляхи надання сервісів клієнтам фінансових організацій (банків). Готівковий обіг все більше витісняється безготівковим завдяки розповсюдженню платіжних карток та системам дистанційного банківського обслуговування (ДБО). Стрімкий розвиток систем ДБО сьогодні дозволяє виконувати майже всі операції зі своїм банківським рахунком не відходячи від комп'ютера. Задля прискорення обслуговування клієнтів, банки почали розміщувати у своїх відділеннях і торгових точках термінали самообслуговування (ТСО). ТСО служать для надання стандартних сервісів, таких як, внесення платежів по кредиту, поповнення депозиту, оплата комунальних платежів тощо. Таким чином, стратегічним напрямком розвитку надання банківських сервісів є розвиток та удосконалення дистанційних та інтерактивних каналів. Прикладом повністю «електронного» банку може служити російський Тінькофф Банк або український БітКредіт. Не варто забувати про вихід на ринок платіжних систем компанії Apple, з інтегрованими платіжними функціями, а в майбутньому компанії Google, які постійно сприяють розширенню та спрощенню доступу, а також управлінню коштами на банківських рахунках клієнтів. За сучасних умов у банківській практиці почали впроваджуватись нові технології обслуговування фізичних та юридичних осіб, які надають можливість проведення банківських операцій вдома («homebanking»), в офісі тощо, повсюди, де це зручно клієнту. На сьогодні можна відзначити наступні різновидності віддаленого банкінгу: tele-банкінг, video-банкінг, Internet-банкінг, PC-банкінг, GSM-банкінг (SMS-банкінг), які суттєво «полегшують» життя клієнтів, надаючи можливість віддаленого керування рахунками цілодобово, з будь-якого куточку світу, 7 днів на тиждень за наявності підключення до мережі Інтернет. Також варті уваги такі банківські послуги як:

- *інтернет-еквайринг* – прийом до оплати платіжних карток через мережу Інтернет із використанням спеціально розробленого та надійно захищеного WEB-інтерфейсу, що дозволяє здійснити розрахунки в будь-який час та у будь-якому місці;
- *факторинг* – фінансування поставок товарів або надання послуг, що не вимагає оформлення застави і страхування; контроль своєчасності оплати товарів та послуг покупцем згідно з контрактом; можливість надання відстрочки платежу своїм клієнтам.

Ще однією послугою, яку можна виділити в інновації, є *кеш-менеджмент* (від англ. cash – готівкові кошти). Це система управління грошовими потоками та залишками на рахунках юридичних осіб з метою їх оптимізації, а також включає заходи щодо розвитку розрахунково-платіжних технологій. Кеш-менеджмент дозволяє клієнтам зменшити витрати й ефективно управляти своїми фінансовими потоками. Щодо перспективного розвитку напряму банківських послуг, то варто виділити надання *соціально орієнтованих банківських послуг* (або socialbanking – соціальний банкінг). Сьогодні – це інноваційна активність банків, спрямована на впровадження продуктів і послуг, що сприяють забезпеченню стабільного та безпечного соціально-економічного розвитку суспільства. Оскільки, сучасні технології використовуються в роботі банків, то при їх створенні їм має бути притаманний: «стратегічний ефект» приросту клієнтської бази, зацікавлення значимих персон, зменшення витрат на здійснення банківських операцій при оптимальному рівні операційного ризику і операційних затрат. Інноваційною технологією, яка вже сьогодні проходить випробування,

можна назвати безпровідну технологію *NFC* (Near Field Communication). NFC можна дослівно перекласти як «зв'язок в ближньому полі», в основі якого лежить використання ідеології передачі даних радіоканалом на короткій відстані. NFC працює по аналогії з WI-FI і Bluetooth. Вона забезпечує зручну, надійну та захищену передачу даних радіоканалом на короткі відстані між різними електронними пристроями. Найпоширенішим в світі пристроєм із NFC-інтерфейсом сьогодні є мобільні телефони, які можна використовувати в якості банківської пластикової картки для роботи з банкоматами. Клієнт ставить телефон біля банкомату, який ідентифікує особу власника телефону і зчитує інформацію прямо з нього. Однією із найголовніших переваг використання таких телефонів є те, що вони можуть зберігати інформацію про декілька банківських карток, що дозволяє споживачу не носити з собою пачку пластикових карток.

Ефективність діяльності та конкурентоспроможність будь-якого банку в більшій мірі забезпечується впровадженням новітніх послуг фінансових інститутів, таких як ДБО, факторинг, еквайринг, центри самообслуговування, кеш-менеджмент, соціально орієнтовані послуги та використання інноваційних технологій. Їх перевагами використання є зменшення часу обслуговування клієнтів, можливість клієнтів управляти своїми операціями, полегшення роботи співробітників банку, розширення кола клієнтів, забезпечення переваг над конкурентами та інші. Таким чином, тільки комплексне використання різних технологічних рішень і організаційних заходів дозволить забезпечити високий рівень безпеки при роботі в системах ДБО і, тим самим, підвищити якість обслуговування клієнтів.

Організація телекомунікаційних взаємодій – серйозна проблема, але незважаючи на вже досягнутий рівень розвитку Інтернет-послуг, цей напрямок найближчим часом буде тільки розвиватися і стрімко зростати. Практично всі мережеві технології, які з'являються на ринку праці, можуть бути взяти фінансовими інститутами на озброєння. Неминучими є процеси їх інтеграції в рамках національних і світових банківських спільнот. Але це безсумнівно забезпечить стале зростання якості банківських послуг, від яких виграють як банк, так і його клієнти.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1.Закон України «Про фінансові послуги та державне регулювання ринків фінансових послуг» від 12 липня 2001,№2663.Режим доступу:http://zakon2.rada.gov.ua/laws/show/2664-14

2.Андреева А.В. Роль финансовых инноваций в развитии рынка банковских услуг/А.В.Андреева // Банковские услуги. – 2010. – № 6. – С. 31-35.

3.Бархатов И.В. Особенности инновационных банковских услуг / И.В. Бархатов // Экономика/ Вестник Челябинского госуниверситета.–2011.–№32 (247).–Вып.34.– С. 130-135.

4.Босак О.В.Інноваційна діяльність як основний чинник підвищення конкурентоспроможності банку / О.В. Босак // Економіка, планування і управління галузі : Науковий вісник НЛТУ України. – 2009. – Вип. 19.5. – С. 131-136.

5.Вовчак О.Д. Кредит і банківська справа: Підручник /О.Д. Вовчак, Н.М. Рущишин, Т.Я. Андрейків. – К. : Знання, 2008. – 564 с.

6.Козка А.І. Сутність та зміст банківських інновацій. – [Електронний ресурс] / А.І. Козка // Економікс. – 2009. – Режим доступу: http://www.rusnauka.com/14ENXXI_2009/Economics/45244.doc.htm

7.Костюченко О.А. Банківське право: підручник /О.А. Костюченко. – К.: ВД «Професіонал», 2002.–544с.

8.Охлопков А.В. Банковские инновации и особенности их реализации в современном банковском секторе России. – [Электронный ресурс] / А. В. Охлопков. – Режим доступа: http://www.ini21.ru/arhiv/1-2-11/1217.php

9.Полищук А.И. Коммерческие банки: новые услуги и инновационные технологии коммуникации. – [Электронный ресурс] / А.И. Полищук // Бизнес и банки. – 2010.–С.10-11. – Режим доступа: https://www.i-free.com/industry/ articles/572

Наукове видання

СТАН ТА УДОСКОНАЛЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

VII Всеукраїнська науково-практична конференція

09 – 12 червня 2015 року

ЗБІРНИК НАУКОВИХ ПРАЦЬ

(*українською та російською мовами*)

Відповідальний за випуск

Михалишин Б.Є.

Підписано до друку 28.05.2015. Папір офсетний. Формат 60×84$^{1}/_{16}$.
Гарнітура Таймс. Друк офсетний. Ум. друк. арк. 6,8.
Обл.-вид. арк. 8,9. Тираж 50 прим. Зам. № 3680.

Віддруковано в друкарні ТОВ «Ділова інформація»,
м. Миколаїв, вул. Декабристів, 1-А, тел. (0512) 50-01-44