МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ-2014

IV ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ З МІЖНАРОДНОЮ УЧАСТЮ

22 – 23 грудня 2014 року

(Національний університет кораблебудування
Інститут автоматики та електротехніки
просп. Леніна, 3)

МАТЕРІАЛИ

МИКОЛАЇВ • НУК • 2014

УДК 004
У-45

Сучасні проблеми інформаційної безпеки на транспорті: Матеріали всеукраїнської науково-практичної конференції з міжнародною участю. – Миколаїв: НУК, 2014. – 202 с.

У збірнику подані матеріали 4-тої Всеукраїнської НПК "Сучасні проблеми інформаційної безпеки на транспорті".

Розглянуті питання теорії та практики систем інформаційної безпеки транспортних засобів і систем, захисту інформації в каналах зв'язку та глобальних мережах передачі даних, захисту інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, правові аспекти діяльності в галузі інформаційної безпеки, а також питання підготовки кадрів у галузі знань «Інформаційна безпека».

Збірник може бути корисним для наукових співробітників, викладачів, інженерів та студентів.

ОРГАНІЗАТОРИ:

1. Міністерство освіти і науки України
2. Інститут інноваційних технологій і змісту освіти
3. Національний університет кораблебудування імені адмірала Макарова, Інститут автоматики і електротехніки (ІАЕ)
4. Управління Державної служби спеціального зв'язку та захисту інформації України в Миколаївській області
5. Національний авіаційний університет
6. Академія наук суднобудування України
7. Морська академія В'єтнаму
8. ТОВ «Науково-виробнича фірма «Топаз»
9. ТОВ «БЕЗПЕКАІНФОСЕРВІС»
10. Науково-технічний центр «Квант»

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

Відповідальний за випуск Трибулькевич В.В.

СЕКЦІЯ 1. ІНФОРМАЦІЙНА БЕЗПЕКА ТРАНСПОРТНИХ ЗАСОБІВ І СИСТЕМ

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МОБІЛЬНИХ ПРИСТРОЯХ НА БАЗІ ОС ANDROID

Автор: *Р.В. Баронов, Головне управління Державної служби спеціального зв'язку та захисту інформації України у Миколаївській області, м. Миколаїв*

В роботі розглянуто сучасні тенденції розвитку PDA(Personal Digital Assistant) пристроїв, їх вразливості та проблеми пов'язанні з забезпеченням інформаційної безпеки при використанні планшетів та смартфонів. Розглянуто способи протидії загрозам інформаційної безпеки та методи її забезпечення.

Ключові слова – PDA, Android пристрої, інформаційна безпека, потенційно небезпечне ПЗ.

СУЧАСНІ ТЕНДЕНЦІЇ РОЗВИТКУ PDA ПРИСТРОЇВ

З появою телефонів та планшетів з використанням операційних систем компаній Apple та Google почався новий етап розвитку портативних пристроїв. Продуктивність апаратної частини сучаних портативних пристроїв можна порівняти с персональними комп'ютерами за якими працювали менш ніж 10 років назад.

Сучасні PDA пристрої на базі ОС Android від Google мають чотирьохядерні процесори з робочою частотою 1,5 ГГц (рішення на базі процесорів Nvidia Tegra 3), окрім цього більша частина пристроїв на слабкіших платформах повністю здатні забезпечити виконання функцій офісного ПК.

Стимулювання та сприяння розвитку ринку програмного забезпечення для мобільних ОС має дуже великий вплив на поширення та просування смартфонів та планшетів, що частково замінюють ПК та ноутбуки та, ймовірно, з часом лишать їм лише професійний сегмент для користувачів, які потребують від ПК виконання специфічних задачі з високими вимогами до апаратної частини.

Австралійській розробник Метт Квен (Matt Kwan) розробив програмний продукт «X-server», який вже зараз користувачі Android можуть безкоштовно скачати з Інтернет магазину Google Play.[1]

XServer реалізує протокол X11 на Android пристроях, тобто дозволяє відображати на дисплеї планшету/смартфону інтерфейс програми яка працює на Unix машинах у мережі.

Інтеграція мобільних пристроїв в системи керування процесами в установах та організаціях створює певні проблеми, пов'язані з ефективним захистом конфіденційної інформації, що циркулює в системі.

ВИБІР ОС

Першим питанням постає правильний операційної системи, яка зможе вдало вмістити водночас зручність для користувача та дотримання вимог з безпеки.

Наприклад, у 2011 році в армії США після проведеного тестування були прийняті в експлуатацію планшети на базі ОС Android для зберігання та обробки таємної інформації. Причиною такої довіри до пропріє тарної операційної системи може слугувати «відкритість» програмного коду ОС, що доступний для аналізу на предмет вразливостей, на відміну від «закритих» для аналізу iOS та Windows.

Зокрема, про недоліки в системі безпеки iOS можуть свідчити випадки прихованої відправки до корпоративних серверів Apple персональних даних користувачів, таких як їх місцезнаходження.

До конструктивних недоліків Windows 7 можна віднести підтримку тільки процесорів з архітектурою x86, внаслідок чого висуваються додаткові вимоги до таких пристроїв (тепловіддача, маса пристрою та менший час автономної роботи).

ВРАЗЛИВОСТІ ПОВ'ЯЗАННІ З ВИКОРИСТАННЯМ ANDROID ПРИСТРОЇВ

На даний час більшість вразливостей безпеки Android ОС базуються на шкідливих діях встановлених додатків. Реалізується це двома шляхами:

1. Внаслідок неуважності користувачів, які встановлюють програмне забезпечення на свій пристрій (при інсталяції ПЗ операційна система потребує згоди користувача на надання переліку допустимих дій та використання ресурсів пристрою);
2. Внаслідок використання шкідливого ПЗ («троянів») що інтегруються до легітимного ПЗ, що розповсюджується через web, альтер-

нативні Інтернет магазини та репозиторії, також існує ймовірність отримати вражене ПЗ з офіційного Інтернет магазину, враховуючи навіть політику Google щодо перевірки ПЗ для Google Play перед його публікацією.[2]

Окремо слід виділити можливість втрати чи крадіжки портативного пристрої та подальшого його використання в інтересах третіх осіб.

ЗАСОБИ ПРОТИДІЇ

Інформування користувачів здатне підвисити ймовірність захисту від вірусних загроз, але при наявній можливості бажано адміністративним шляхом обмежити здатність користувачів встановлювати додаткове ПЗ.

Реалізація даної схеми можлива шляхом встановлення на кожному Android пристрої необхідного ПЗ (наприклад, Root Uninstaller з подальшим блокуванням можливості самостійної інсталяції додатків.

Захист від шкідливих додатків можливо забезпечити шляхом використання програм комплексного захисту за допомогою яких можливо організувати криптографічний захист інформації, сканування на віруси, функції мережного екрану, віддалене адміністрування та інші (Kaspersky mobile security, ESET mobile security, Avast Mobile Security[3]).

Серед переваг таких комплексних програм безпеки є встановленні в них модулі програм типу «антикрадій» які дають можливість віддалено виконувати визначений перелік команд на пристрої вразі його втрати чи крадіжки. (блокування пристрою, отримання GPS координат місця знаходження пристрою, форматування пристрою зберігання інформації).

Ефективність останнього пункту підтверджується дослідженням компанії Symantec[4] 89% людей, які знайшли телефон, оглядають персональну інформацію, 83% – корпоративну та 70% всю. Заміною комплексних рішень може слугувати обміркований вибір кожного з необхідних захисних компонентів з врахуванням потреб компанії.

Головними критеріями для вибору встановлюють забезпечення неможливості користувача змінювати налаштування програми, робота програми у фоновому режимі та маскування, адже при виявленні захисного ПЗ зловмисник здатен прийняти міри для уникання засобів захисту.

Для більшої безпеки можливо розробити власну версію модифікованої прошивки для планшетів. Така прошивка може вміщати в собі

необхідне встановлене та налаштоване ПЗ, а також пакет необхідних службових утиліт. Для уникнення можливості форматування внутрішнього носія шляхом внесення незначних змін до ядра ОС можливо обрати альтернативну файлову систему.

ВИСНОВКИ

Роль портативних пристроїв в інфраструктурі організацій вже сьогодні створює небезпеку для критичних даних. Вказаний ефект підсилюється відкритою можливістю неконтрольованого встановлення програмних додатків з боку користувача.

Для уникнення інцидентів з використанням як методів соціальної інженерії, так і суто технічних приведено загальні рекомендації з налаштування та обладнання додатковими утилітами для ускладнення несанкціонованих дії зловмисників щодо вразливої інформації.

Список літератури:

1. X-сервер для Android – [Електроний ресурс] «Тематические Медиа», – Режим доступу: http://habrahabr.ru/post/139705/ вільний, Заголовок з екрану, мова російська.

2. Эволюция угроз безопасности Android за последний год – [Електроний ресурс] «Тематические Медиа», – Режим доступу: http://habrahabr.ru/post/130612/ вільний, Заголовок зекрану, мова російська.

3. Обзор Avast Mobile Security для Android [Електроний ресурс] «Тематические Медиа», -Режим доступу: http://habrahabr.ru/post/140139/вільний, Заголовок з екрану, мова російська.

4. The Symantec Smartphone Honey Stick Project- [Електроний ресурс] Symantec Corporation, авор Скотт Врайт, – Режим доступу: http://www.symantec.com/content/en/us/about/ presskits/b-symantec-smartphone-honey-stick-project.enus.pdf вільний, Заголовок з екрану, мова англійська.

ОСОБЕННОСТИ РАЗРАБОТКИ СУИБ СУДНА

Авторы: *Е.А. Баронова, ст. преподаватель; С. Агакишиев, студент, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев*

Обеспечение безопасности мореплавания – сложная многокритериальная задача. Ежегодно повышается количество аварийных ситуаций, случаев и происшествий с пассажирскими и торговыми судами. Одним из главных факторов повышения аварийности, ареста и захвата судов определено отсутствие системных решений по информационной безопасности судоходства, установлена недостаточность, недостоверность и несвоевременность обеспечения судоводителей необходимой информацией для безопасного управления судном. В первую очередь это связано с повышением степени автоматизации, информатизации на судах, с интеграцией в единую систему разнородных систем, обеспечивающую управление судном с ходового мостика одним оператором. Сложность для судовых систем управления и обработки информации состоит в том, что необходимо объединить в единую систему разнообразные по быстродействию системы, в том числе жесткие и мягкие системы реального времени. Это, в свою очередь, характеризует аппаратные средства системы, методы обеспечения надежности, живучести и распределения вычислительных ресурсов и приводит к необходимости внедрения на судах систем управления информационной безопасностью.

Основная цель работы – повышение эффективности управления информационной безопасностью на судах за счет учета особенностей построения СУИБ судна.

Обеспечение информационной безопасности судна в достаточной степени возможно при условии создания системы управления информационной безопасностью (СУИБ) судна в соответствии с международным стандартом ISO 27001 и автоматизации ее.

Для достижения цели необходимо решить проблемы:

Необходимость создания СУИБ отсутствует в требованиях нормативных документов по мореплавания.

Международные стандарты не содержат рекомендаций по выбору какого-либо аппарата оценки риска, а также синтеза мероприятий, средств и сервисов безопасности, используемых для минимизации рисков.

Создание СУИБ судна требует системного подхода с учетом всех особенностей судна как ОИД. Необходимо рассматривать СУИБ судна как элемент СУИБ ВТК и как элемент СУБ судна. Кроме того необходимо учитывать, что построение СУИБ судна включает все этапы жизненного цикла судна от проектирования до утилизации. Необходимо обоснование критериев, которые позволят оптимизировать СУИБ.

Анализ информации, которая нуждается в защите, с учетом наличия на судах автоматических, автоматизированных, информационно-управляющих, специальных системам и комплексов, интегрированных систем управления и систем поддержки принятия решений. Разработка рекомендаций, процедур, технологий и методик анализа информации и потоков информации на судне.

Создание на судах в соответствии с Международным кодексом по управлению безопасностью (МКУБ) систем управления безопасностью (СУБ). Вопросы управления безопасностью движения судов должны рассматриваться с учетом информационной безопасности судна, то есть с обеспечением целостности, доступности и конфиденциальности информации, которая циркулирует на судне. Таким образом, СУИБ судна целесообразно интегрировать с СУБ. На судне необходимо проводить периодический внутренний аудит и мониторинг ИБ. Оценка зрелости процессов ЗИ является показателем эффективности СУИБ. В обобщенном виде для определения уровня эффективности СУИБ судна не обходимо выполнить следующие работы:

– определить перечень информации, подлежащей защите;
– определить перечень судовых систем, в которых эта информация обрабатывается;
– определить группу экспертов для проведения внутреннего аудита ИБ;
– определить перечень процессов ЗИ, осуществляемых на судне;
– с помощью экспертной системы провести определение текущих уровней зрелости существующих ПЗИ и соответствия текущей зрелости целевым ориентирам;

– провести формирование рекомендаций по повышению зрелости ПЗИ, которые могут быть использованы для повышения эффективности СУИБ судна.

Определение критериев выбора методов сопровождения, мониторинга и управления рисками, управления инцидентами информационной безопасности на судах, создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное прекращение посягательств на ресурсы на основе правовых, организационных и технических мероприятий и средств обеспечения безопасности необходимо максимально автоматизировать и создать для судна систему поддержки принятия решений по управлению информационной безопасностью.

Выводы:

Для обеспечения необходимого уровня информационной безопасности судна не обходимо создать СУИБ судна, интегрированную с СУБ и автоматизировать ее.

Список литературы:

1. Баронова О.А. Сучасні завдання інформаційної безпеки судна як інтелектуальної споруди // Матеріали Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». – Миколаїв: НУК, 2011.- С.28-30.

АДМІРАЛ МАКАРОВ – ЗАСНОВНИК РАДІОЗВ'ЯЗКУ ТА РАДІОРОЗВІДКИ НА ФЛОТІ

Автори: *О.А. Баронова, ст. викладач; В.С. Блінцов, д.т.н., проф., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Віце-адмірал С.Й. Макарова народився 27 грудня 1848 року (8 січня 1849 р. по старому стилю) у Миколаєві, російський флотоводець, океанограф, полярний дослідник, кораблебудівник, його ім'я носить Національний університет кораблебудування.

Серед низки видатних військово-організаційних, наукових та інженерних здобутків адмірала Макарова незаслужено мало місця відводиться його унікальному вкладу у створення і впровадження у морську практику проривного на кінець 19-го сторіччя відкриття – радіозв'язку.

Коли Макаров був призначений молодшим флагманом Балтійського флоту і оселився в Кронштадті, в будівлі Морського інженерного училища, він познайомився з викладачем О. С. Поповим. У цей час Попов виконував свої перші дослідження з бездротовим телеграфом і, виходячи з можливості використання цього технічного засобу у військово-морській справі, між ними зав'язалася дружба. Макаров серед російських моряків один з перших зміг оцінити винахід Попова і усвідомити значення і цінність цього відкриття для флоту.

Перше серйозне практичне випробування бездротового телеграфу відбулося 24 січня 1900, за ініціативи Макарова на виконання місії з встановлення зв'язку між островом Гогланд (біля якого сів на мілину броненосець «Генерал – адмірал Апраксин») і материком був запрошений А.С. Попов зі своїм винаходом . Після встановлення необхідного обладнання вже 25 січня була передана перша в історії радіограма на далеку відстань, а саме на 43 версти (майже 46 км). Передана вона була начальником Головного морського штабу адміралом Авелану, адресувалася вона командиру «Єрмака» М.П. Васильєву, у ній йшлося: «Около Лавенсаари оторвало льдину с пятьюдесятью рыбаками. Окажите немедленно содействие спасению этих людей. Авелан.»

Макаров не тільки першим оцінив переваги винаходу Попова, а й одним з перших заявив про пріоритет російського вченого в боротьбі з Марконі.

Використання бездротового телеграфу для передачі повідомлень у військових цілях не було доцільним, оскільки прилад випромінював сигнал в досить широкому спектрі частот. Використання для радіоприйому настільки ж простих і, як наслідок, настільки ж широкосмугових пристроїв дозволяло прослуховувати роботу таких передавачів практично будь-якими приймачами, що перебували в зоні зв'язку. Ця обставина зумовила вельми ранню постановку проблеми забезпечення прихованості і конфіденційності радіозв'язку. Проблема частково вирішилась після того, як антену і іскровий розрядник стали виділяти в окремі коливальні контури з'єднання. Схема стала більш частотно виборчою, але все одно при бажанні будь-який приймач, що знаходився в області передачі сигналу, поставивши собі за мету перехопити його,

міг зробити це. Телеграфи використовували в основному в якості пристроїв для виявлення супротивника, так як вони мали широкий спектр частот та ненаправлений прийом, яким вони автоматично виявляли сигнали радіостанцій супротивника, якщо дозволяла зона дії ворожого телеграфу. Дистанції виявлення супротивника істотно залежали від висоти підйому антенної мережі і взаємного налаштування передавальної і приймальної станцій, від потужності передавача, величина якого легко регулювалася зміною числа або довжини іскрових проміжків, а також від ряду інших факторів, могли становити для даного типу апаратури від 20 до 70 миль при прийомі "на стрічку" і до 90 миль і більше при прийомі "на телефон".

Маловідомим фактом є макаровський таємний наказ № 27 від 7 березня 1904 року, який він віддав як командувач Тихоокеанським флотом Росії під час російсько-японської війни. Його головний зміст наводиться нижче.

«Принять к руководству следующее:

1. Беспроволочный телеграф обнаруживает присутствие, а поэтому теперь же поставить телеграфирование это под контроль и не допускать никаких отправительных депеш или отдельных знаков без разрешения командира, а в эскадре — флагмана. Допускается на рейдах, в спокойное время, поверка с 8 до 8.30 утра.

2. Приемная часть телеграфа должна быть все время замкнута так, чтобы можно было следить за депешами, и если будет чувствоваться неприятельская депеша, то тотчас же доложить командиру и определить, по возможности заслоняя приемный провод, приблизительно направление на неприятеля и доложить об этом.

3. При определении направления можно пользоваться, поворачивая свое судно и заслоняя своим рангоутом приемный провод, причем по отчетливости можно судить иногда о направлении на неприятеля. Минным офицерам предлагается произвести в этом направлении всякие опыты.

4. Неприятельские телеграммы следует все записывать, и затем командир должен принять меры, чтобы распознать вызов старшего, ответный знак, а если можно, то и смысл депеш.».

Цей лист є першим офіційним документом у галузі радіорозвідки, таким чином Макаров є родоначальником цієї галузі. Успішна реалі-

зація цих положень принесла багато користі під час російсько-японської війни.

Показовим прикладом є використання суднової радіостанції в якості виявителя ворожих судів на крейсері "Новік". Для навантаження вугілля та оперативного ремонту котлів крейсеру довелося зайти 7 серпня 1904 у Корсаківський порт на о. Сахалін, де його наздогнали крейсери "Цусіма" і "Чітосе". Пильний моніторинг радіоприймальної вахти дозволив майже за 2 години до приходу виявити японські кораблі по їх радіопереговорам, що забезпечило командиру "Новіка" можливість своєчасно припинити всі роботи, підняти пари і вийти для бою в море, уникнувши таким чином раптового захоплення корабля супротивником.

Після видання Наказу № 27 менше ніж через місяць російським морякам вперше вдалося застосувати навмисні радіоперешкоди для порушення радіозв'язку противника, дезорганізувати управління стрільбою японських кораблів по місту і внутрішньому рейду.

Як сам факт створення перешкод, так і їх висока ефективність однозначно підтверджуються офіційними японськими джерелами з історії російсько – японської війни.

СУЧАСНІ ЗАДАЧІ ОРГАНІЗАЦІЇ БЕЗПЕКИ ТОРГІВЕЛЬНОГО СУДНА

Автор: *В.С. Блінцов, д.т.н., проф., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Торгівельні судна є традиційною мішенню для нападу з боку піратів під час їх перебування в акваторіях узбережжя Сомалі, в Арабському морі та деяких інших акваторіях Світового океану. Тому завдання протидії морським піратам є актуальною. Попередній аналіз показує, що успішний розв’язок цього завдання має ґрунтуватись на наступних чинниках:

дій капітанів суден та їх екіпажів;

дій судновласників;

організації взаємодії з міжнародними військово-морськими структурами.

До першої групи чинників відносяться:

– заходи щодо попередньої реєстрації судна перед виходом у море у військових структурах протидії піратству – Оперативному центрі морської охорони Об'єднаного Королівства (UKMTO), Координаційному центрі ВМС США та Коаліційних Об'єднаних морських сил (MARLO) та Центрі морської охорони Сил ЄС «ATALANTA» (MSCHOA) [1]; при цьому, в обов'язковому порядку капітани суден мають надавати військовим структурам плани своїх маршрутів з часовими координатами переміщень;

– організації подання своєчасних доповідей капітанів суден про перебіг подій в оперативному центрі UKMTO відповідно до встановлених форм звітності;

– встановлення та дотримання екіпажами заходів самозахисту суден (розробка і впровадження порядку організації самозахисту судна та його екіпажу (встановлення металевих бар'єрів по бокам судна, водометів тощо, підтримання високої швидкості руху судна для ускладнення висадки на нього піратських груп, використання екіпажами суден несприятливих погодних умов, що ускладнює дії піратів на невеликих човнах, ретельний контроль обстановки у зонах дій з визначенням піратських груп по ходу маршрутів.

Важливим додатковим заходом є вивчення типових схем дій піратів при нападах на судна:

– вивчення тактики дій піратів (застосування пари швидкохідних моторних човнів зі швидкістю ходу не менш 25 миль\год. і потужністю понад 60 к.с.; захід піратських човнів здійснюється з обох боків від комерційного судна; атаки здійснюються у денний час, однак, були окремі випадки проведення піратських атак і вночі);

– вивчення типів та форми застосування та піратських суден (класифікація піратських суден наведена у табл. 1).

Важливою складовою безпеки судна в морі є дотримання порядку організаційних заходів взаємодії компаній судновласників з військовими структурами перед виходом суден у плавання, подання заявок на вихід у небезпечні райони судноплавства та отримання від військових структур координат безпечного проходу – Міжнародновизнаних транзитних коридорів (IRTC).

Таблиця 1. Класифікація піратських суден:

№ п/п	Тип судна	Переваги використання	Недоліки (слабкі місця) використання
1	Малорозмірні швидкомоторні човни	Велика швидкість	Обмеженість радіусу дії та екіпажу на борту – як правило не більше 2 піратів
2	Середньо розмірні рибацькі судна	Наявна база для розміщення достатньої кількості особового складу, можливість транспортування до двох швидкомоторних човнів, термін перебування у морі – до 15 днів	Обмеженість радіусу дії до 100 км. від узбережжя, відсутність достатніх засобів захисту, невелика швидкість
3	Великорозмірні судна – використовуються захоплені піратами комерційні судна	Наявна база для розміщення великої (до 50 чол.) кількості особового складу, можливість транспортування на борту великих запасів продовольства та зброї, відсутність візуального контролю наявності зброї на борту, приховане (під виглядом комерційних суден) переміщення та підхід до інших суден, велика швидкість та радіус дії, термін перебування у морі – до 1 року	Необхідність наявності на борту кваліфікованого екіпажу зі знанням навігаційної техніки, необхідність значних запасів палива, вразливість протидії військовим кораблям міжнародних анти піратських сил

Узагальнений алгоритм дій перед виходом суден у рейс через небезпечні акваторії передбачає:

– реєстрацію виходу та судна на веб-сайті оперативного центру MSCHOA;

– отримання вихідних даних обстановки в районах судноплавства від оперативних центрів MSCHOA та НАТО;

– підготовку судна до виходу в море, відпрацювання планів готовності до дій у надзвичайних умовах;

– організацію цілодобового спостереження за обстановкою у зоні судноплавства, у тому числі з використання веб-ресурсів міжнародних військових структур;

– участь у формуванні морських конвоїв;

– встановлення бортових дротових перешкод фізичному проникненню піратів на судно;

– організацію практичної підготовки екіпажу до дій у надзвичайних умовах (оголошення тривоги, оповіщення військових структур про приближення піратів, дії екіпажу за планами самооборони, збільшення швидкості руху тощо, дії екіпажу при висадці піратів на борт судна, можливі варіанти використання «Цитаделі» – місця безпечного перебування екіпажу та ведення оборонних дій, дії екіпажів при втручанні військових сил);

– підтримання взаємодії з міжнародними військовими структурами, забезпечення своєчасного надходження звітних доповідей про стан свого перебування в море.

Важливою складовою забезпечення безпеки судна є дотримання вимог з інформаційної безпеки. До головних чинників тут слід віднести:

– обмеження розповсюдження інформації про маршрут судна; пірати використовують інформаторів в ключових портах, де судна здійснюють завантаження перед наступним транзитом через Аденську затоку (порти у Дубаи, Кенії, Ємені й Шрі-Ланці); захоплення деяких суден дають підстави припустити, що можуть бути інформатори також в інших країнах і в таких вузьких місцях як Суецький канал;

– пірати при координації нападів успішно використовують радари, супутникові системи зв'язку й пристрої GPS; існує також імовірність одержання інформації за допомогою різних технічних засобів перехоплення.

Виходячи з цього, судновласники повинні робити все можливе, щоб надавати інформацію про вантажі, час плавання, маршруті й місця призначення, тільки за принципом "що дозволено знати".

Таким чином, сучасні задачі забезпечення безпеки торгівельного судна охоплюють організаційні, технічні та інформаційні аспекти.

Список літератури:

1. Best Management Practices for Protection against Somalia Based Piracy (BMP4, Version 4 – August 2011). – Edinburgh, Scotland, UK. – Witherby Publishing Group Ltd, 2011. – 95 pp.

КОНЦЕПЦІЯ СТВОРЕННЯ БАГАТОСЕНСОРНОЇ СИСТЕМИ ОХОРОНИ АКВАТОРІЇ ПОРТУ

Автори: *О.В. Блінцов, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв; П.В. Майданюк, Головне управління Державної служби спеціального зв'язку та захисту інформації України у Миколаївській області, м. Миколаїв*

В акваторіях портів України розміщуються «критичні» об'єкти інфраструктури, які вимагають спеціальної системи охорони і оборони. Це, у першу чергу, судна або кораблі на якірних стоянках, термінали нафто- або газопроводів, обладнання навігації та звзку тощо. Ефективна охорона й оборона цих об'єктів неможливі організаціїї сучасної системи моніторингу підводної і надводної обстановки на портовій акваторії.

Проникнення в контрольовану зону порту може здійснюватись з використанням невеликих за розміром надводних (човнів, плотів та інших плаваючих засобів з встановленим озброєнням та вибухівкою), підводних об'єктів (підводних апаратів чи водолазів) або повітряних засобів (планерів, парашутів та ін.). Тому актуальним науковим завданням є розробка концепції багатосенсорної системи охорони порту, спроможної здійснювати моніторинг визначених об'єктів критичної інфраструктури в межах визначеної території, що охороняється. Така система має складатися з командного пункту і окремих датчиків, встановлених в ключових точкаї акваторії, які забезпечують ефектив-

ний захист з суходолу і з моря, особливу увагу приділяючи моніторингу підводної частини району. Забезпечення охорони надводної частини району засноване на застосуванні РЛС середнього радіусу дії, телебачення для низьких рівнів освітленості та інфрачервоних камер.

Розглянемо типові загрози об'єктам портової інфраструктури. Терористи, інші групи чи окремі особи, можуть атакувати цивільні порти та військово-морські бази (далі – ВМБ) та інші об'єкти інфраструктури наступними способами:

надводна атака з використанням пілотованих і безпілотних апаратів, що використовуються для перевезення вибухівки, або викрадених суден та захоплених кораблів, що перевозять небезпечні матеріали (наприклад, танкерів для транспортування нафти чи хімікатів), які можуть бути використані для зіткнення з іншими кораблями (суднами) чи об'єктами портової інфраструктури;

підводна атака з використанням підводних диверсантів, міні підводних човнів (пілотованих чи дистанційно керованих) і вибухових речовин чи морських мін (донних, магнітних чи дрейфуючих);

сухопутних атак з використанням вибухових пристроїв, встановлених на транспортних засобах, смертників, стрілецької зброї, гранат, мінометів, поштових бомб, організації масових заворушень в портах, атак кораблів і суден на якірних стоянках з метою їх захоплення чи взяття в заручники членів екіпажу;

повітряних атак з використанням пілотованих чи безпілотних (дистанційно керованих) апаратів, повітряних куль чи пілотів-смертників;

атак з використанням радіоактивних, біологічних і хімічних речовин (аерозолів, рідин тощо) для забруднення води, харчових продуктів чи здійснення безпосереднього впливу на екіпаж та/або пасажирів;

кібернетичних атак, призначених для пошкодження роботи інформаційних систем і мереж, зламу протоколів системи безпеки, передачі сигналів хибної тривоги, викрадення даних, перекручення та блокування інформаційних потоків, несанкціонованої зміни змісту баз даних.

У країнах Євросоюзу розроблена і широко застосовується норма "Regulation 725/2004" щодо підвищення рівня забезпечення безпеки кораблів і портових споруд і директива "Directive 2005/65/WE" щодо підвищення рівня забезпечення безпеки портів [1]. Система охорони

важливих об'єктів інфраструктури портів (наприклад, термінали нафто- і газопроводів) повинні також відповідати вимогам документу "Marine Terminal Physical Security", де містяться рекомендації щодо забезпечення безпеки терміналів нафтопроводів [2].

Система охорони акваторії порту складається з декількох взаємодіючих компонентів, зокрема [3]:

системи руху суден (VTS), оснащеної РЛС великого радіусу дії для відстеження руху суден у визначеній акваторії; судна, що прибувають, зв'язується з оператором системи, ідентифікує себе і після цього супроводжується в порт призначення;

автоматизованої системи ідентифікації (AIS), яка в автоматичному режимі здійснює розпізнавання судна на основі його унікального радіокоду та інформації, що міститься в базі даних; система відстежує рух суден і наносить їх на електронну мапу, а також, у більш сучасній версії, здійснює їх візуальну ідентифікацію в зоні дії апаратури спостереження.

На даний момент у провідних морських країнах ведуться роботи з інтеграції вищевказаних систем в єдину Систему управління портом (Port Management System, PMS) або Систему інформування та управління рухом суден (Vessel Traffic Management and Information System, VTMIS). Основним завданням таких систем є забезпечення безпечного руху на рейді та у внутрішніх водах.

Сухопутна територія порту, включаючи ворота, огорожі та окремі об'єкти інфраструктури (наприклад трубопроводи чи резервуари), також повинна охоронятись.

Таким чином, система охорони порту повинна включати наступні рішення:

систему радіоелектронного і візуального спостереження для ідентифікації та відстеження руху особового складу, наземних і надводних транспортних засобів з метою забезпечення зовнішньої охорони, перепускного режиму та візуального спостереження за територією;

активні (гідроакустичні станції – ГАС) і пасивні (бар'єри з електромагнітним сенсорами) системи для спостереження за надводною і підводною обстановкою;

активні (на базі безпілотних надводних і підводних апараїв-роботів) системи оперативного реагування на загрози вторгнення, що виявлені.

Основна концепція створення таких систем має включати наступні компоненти:

підсистему радіоелектронного і візуального спостереження з автоматичним виявленням і супроводженням цілей за допомогою РЛС з подальшим застосуванням оптичних засобів спостереження для їх візуальної ідентифікації;

підсистему охоронного телебачення (CCTV) разом з тепловізійними камерами для забезпечення можливості ведення спостереження в денний і нічний час;

підсистему інтеграції зображень, отриманих за допомогою денних і тепловізійних камер спостереження, для отримання зрозумілого для оператора системи вихідного продукту;

підсистему ГАС та електромагнітних бар'єрів для оперативного виявлення фактів несанкціонованого входу у захищену акваторію;

підсистему відображення інтегрованих даних РЛС, візуального спостереження та побудови траєкторії руху цілі на електронній мапі для генерації інформації для цілевказування;

підсистему оперативного реагування на порушення режиму доступу на захищену акваторію у складі безекіпажних надводних та підводних апаратів-роботів та водолазів.

У доповіді наводяться результати аналізу вимог до вказаних підсистем та особливості їх застосування в умовах дії зовнішніх збурень середовища (вітро-хвильових, течі) та маневрування порушника.

Список літератури:

1. Regulation (EC) No 725/2004. Of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (Text with EEA relevance). – Official Journal of the European Union, 29.04.2004. – L129/6- L129/91.

2. Marine Terminal Security Guidelines. – Port of Portland, 2009. – 49 pp.

3. Rhodes B.J., Bomberger N.A. and all, Maritime situation monitoring and awareness using learning mechanisms", Proceedings of IEEE MILCOM 2005 Military Communications Conference Atlantic City NJ USA, 2005.

УДК 004.056.53: 621.397: 629.58

УРАХУВАННЯ АВТОМАТИЧНОЇ ЗМІНИ РЕЖИМУ КАМЕР ВІДЕОСПОСТЕРЕЖЕННЯ З ФУНКЦІЄЮ «ДЕНЬ-НІЧ» В СИСТЕМІ АДАПТИВНОГО ОСВІТЛЕННЯ

Автори: *Ю.І. Касьянов, ст. викладач; А.В. Гавриш, студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

В сучасних системах відеоспостереження широко використовуються кольорові відеокамери з функцією "день-ніч", які працюючи в режимі автоматичної експозиції, при зниженні освітленості до певної межі автоматично переходять в чорно-білий режим [1]. Це дозволяє істотно підвищити чутливість, аж до можливості роботи майже в повній темряві, а також поліпшити роздільну здатність при слабкому освітленні.

Однак, в мобільних підводних системах відеоспостереження з використанням телекерованих підводних апаратів (ТПА), які наразі є невід'ємною частиною комплексної системи захисту морських об'єктів і акваторій, автоматична зміна режиму може приводити до небажаних наслідків – втрати важливої кольорової інформації і проблеми повернення камери в кольоровий режим та суттєвого погіршення якості зображення і ускладнення роботи оператора через виникнення режиму миготіння кольору. З цими проблемами прийшлось зіткнутися співробітникам Національного університету кораблебудування при експлуатації ТПА "Інспектор".

Було проведено експериментальні дослідження відеосистеми ТПА "Інспектор" в умовах лабораторії та дослідного басейну [2, 3]. В результаті візуальних спостережень було зроблено висновки, що: самовільний перехід у чорно-білий режим відбувається в результаті зниження освітленості при направленні відеокамери в зону тіні світильників; автоматична зміна режимів відбувається по гістерезисній характеристиці; режим мигтіння кольору виникає при нестаціонарних умовах зйомки, характерних для зйомки в русі та фронтальному штучному освітленні, коли відбувається швидка різка зміна яскравості

картин у кадрі. Запропоновано: розміщувати світильники на поворотному пристрої відеокамери, щоб виключити її направлення в зону тіні; встановити кольоровий світлий предмет в кінці зони огляду (повороту) відеокамери для можливості її примусового повернення в кольоровий режим; використовувати регульовану систему освітлення; обов'язково проводити експериментальні дослідження відеокамери та відеосистеми в цілому щодо їх можливостей в заданих умовах зйомки.

В [4, 5] описано лабораторні інструментальні дослідження автоматичної зміни режимів відеокамер "день-ніч" при штучному фронтальному освітленні, що є найбільш характерним для роботи ТПА у відсутності природного освітлення (в нічний час, на середніх і великих глибинах тощо). Для проведення досліджень використовувався розроблений на кафедрі електрообладнання суден та інформаційної безпеки Національного університету кораблебудування спеціалізований лабораторний комплекс [6]. Результати досліджень підтвердили гістерезисний характер процесу автоматичної зміни режимів та показали, що моменти переходу (граничні рівні освітленості) та ширина гістерезису залежить від оптичного контрасту фону та розміру об'єкта в кадрі. Одержано графіки вказаних залежностей для двох відеокамер та запропоновано використати ці та аналогічні результати досліджень для побудови адаптивно-регульованої системи освітлення. Відмічено необхідність таких експериментальних досліджень в процесі проектування систем підводного відеоспостереження для підвищення їх якості і ефективності.

Метою даної роботи є розробка концепції і структури адаптивно-регульованої системи освітлення та приведення результатів досліджень до виду, необхідного для використання в даній системі.

Розвиток сучасних систем відеоспостереження іде в напрямку їх інтелектуалізації. Інтелектуальні системи відеоспостереження забезпечують автоматичну обробку та аналіз відеоматеріалу і тим самим виконують автоматичне розпізнавання предметів та осіб, що знаходяться на об'єкті, за яким ведеться відеоспостереження. Головними їх складовими є: підсистема відеозйомки, до якої входять камери відеоспостереження та система штучного освітлення; підсистема сервісних детекторів, що забезпечують автоматичне виявлення погіршення якості зображення та стороннього впливу; підсистема покращення зображення для підвищення якості подальшого розпізнавання; підсистема відео-детекторів, які забез-

печують виконання інтелектуальних завдань; підсистема відео аналітики та прийняття рішень, що виконує головний аналіз відео потоку.

Побудова адаптивно-регульованої системи освітлення повинна вписуватись у загальну концепцію побудови інтелектуальної мобільної системи підводного відеоспостереження. Виходячи з цього пропонується структура системи, представлена на рис.1.

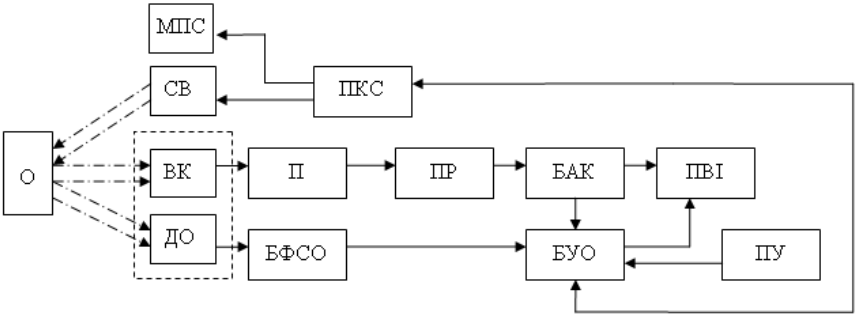


Рисунок 1 – Структурна схема системи адаптивно-регульованого освітлення: О – об’єкт; ВК – відеокамера; СВ – світильники; ДО – датчик освітленості; П – підсилювач відеосигналу; ПР – приймач; БФСО – блок формування сигналу освітленості; ПКС – пристрій керування світильниками; МПС – малопотужний світильник; БАК – блок аналізу кадру; БУО – блок управління освітленістю; ПУ – пульт управління; ПВІ – пристрій відображення інформації

Датчик освітленості ДО розміщується в одному боксі з відеокамерою і служить для вимірювання освітленості на об’єктиві. Блок формування сигналу освітленості БФСО проводить обчислення освітленості на об’єктиві відеокамери. Блок аналізу кадру (БАК) обробляє отриманий від приймача відеосигнал, періодично формуючи та аналізуючи стоп-кадр, і визначає долю об’єкта в кадрі, контраст фону, перераховує відстань до об’єкта зйомки за визначеним розміром об’єкта в кадрі та фокусною відстанню камери. Значення сигналу освітленості на об’єктиві та результати роботи БАК (контраст фону, доля об’єкту в кадрі, відстань до об’єкту) надходять в блок управління освітленістю

БУО, який працює на основі закладених аналітичних залежностей показників якості зображення від умов зйомки, отриманих на основі експериментальних досліджень. За допомогою пункту управління ПУ оператор задає режим регулювання БУО, тобто обирає за яким критерієм виконується оптимізація освітлення: за оптимальною роздільною здатністю, за утриманням кольорового режиму роботи відеокамери або за оптимумом між цими параметрами, за динамічним діапазоном тощо. Пристрій керування світильниками ПКС виконує функцію управління освітленням об'єкта зйомки, шляхом регулювання яскравості світильників. При досягненні максимального світлового потоку світильників, ПКС подає сигнал на БУО про досягнення критичного світлового потоку і неможливість його подальшого регулювання.

Для отримання аналітичних залежностей, що будуть використовуватися при створенні адаптивної системи освітлення в БУО потрібно провести регресійний аналіз даних експериментальних досліджень.

Було проведено регресійний аналіз даних експериментальних досліджень автоматичної зміни режиму відеокамер "день–ніч". Отримані за результатами регресійного аналізу поліноміальні залежності освітленості від долі об'єкту в кадрі для фонів різних контрастів є адекватними (надійними), тобто можуть бути використані при розробці системи адаптивного освітлення і мають аналітичний вид:

$$E\left(x(\%)\right) = A \cdot X \ ,$$

де $A = \begin{pmatrix} A_0 \\ A_1 \\ \cdots \\ A_n \end{pmatrix}$ – матриця коефіцієнтів рівняння регресії; $X = \begin{pmatrix} x^0 \\ x^1 \\ \cdots \\ x^n \end{pmatrix}$ – матриця розміру об'єкта в кадрі; n – ступінь поліному.

Порівняння графіків залежностей, отриманих в результаті регресійного аналізу та експериментальних досліджень для чорного фону представлено на рис.2.

На основі цих залежностей отримано узагальнююче рівняння, яке враховує в собі дві змінні – фон і долю об'єкта в кадрі; виконується це за допомогою регресійного аналізу залежності коефіцієнтів поліномів від контрасту фону. узагальнене рівняння залежності граничної освітленості,

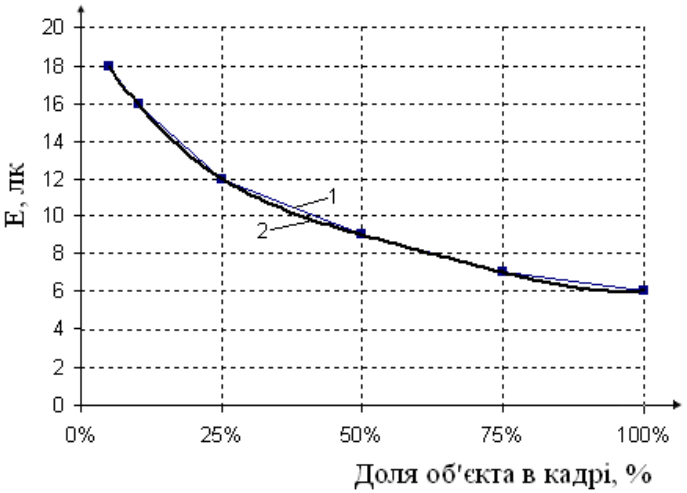


Рисунок 2 – Порівняння залежностей автоматичної зміни режиму з кольорового на чорно-білий для відеокамери «день-ніч» при зйомці на чорному фоні: 1 – крива експериментальних досліджень; 2 – крива, що описується рівнянням регресії

за якою відбувається перемикання режиму, від долі об'єкта в кадрі та контрасту фону має вигляд:

$$E\left(x(\%),K\right)=A_0+A_1\cdot x+A_2\cdot x^2+\ldots+A_n\cdot x^n=(B_{00}+B_{10}\cdot K+B_{20}\cdot K^2+$$
$$+B_{30}\cdot K^3+B_{40}\cdot K^4)+\left(B_{01}+B_{11}\cdot K+B_{21}\cdot K^2+B_{31}\cdot K^3+B_{41}\cdot K^4\right)\cdot x+\ldots+$$
$$+\left(B_{0m}+B_{1m}\cdot K+B_{2m}\cdot K^2+\ldots+B_{nm}\cdot K^n\right)\cdot x^n=\left(B\cdot K\right)\cdot X$$

де $B=\begin{pmatrix}B_{0m}\\B_{1m}\\\ldots\\B_{nm}\end{pmatrix}$ – матриця коефіцієнтів для визначення відповідного ко-

ефіцієнту A_n в рівнянні регресії; $K = \begin{pmatrix} K^0 \\ K^1 \\ \dots \\ K^n \end{pmatrix}$ – матриця контрасту фону по відношенню до білого; $m = 0 \dots n$ – номер коефіцієнту в рівнянні.

Порівняння графіків залежностей одного з коефіцієнтів поліному від контрасту фону, отриманих в результаті регресійного аналізу та експериментальних досліджень представлено на рис.3.

Для побудови адаптивно-регульованої системи освітлення потрібно мати також аналітичні залежності інших показників якості зображення (роздільної здатності, достовірності передачі кольорів, динамічного діапазону тощо) від умов зйомки.

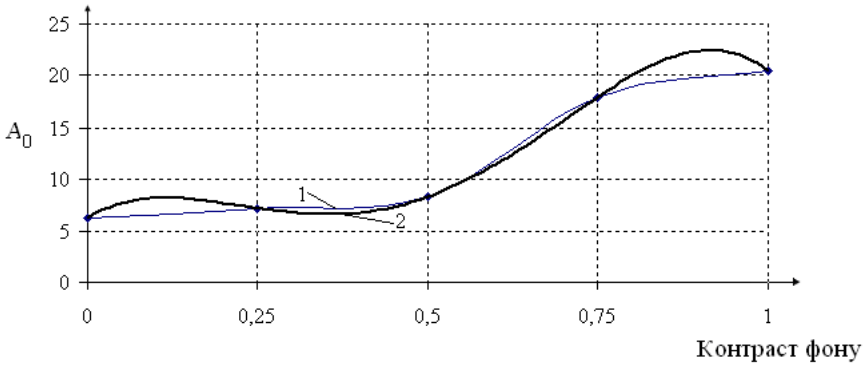


Рисунок 3 – Порівняння залежностей коефіцієнту А0 від контрасту фону: 1 – крива експериментальних досліджень; 2 – крива, що описується рівнянням регресії

Висновок. Одержано аналітичні вирази залежності автоматичної зміни режиму відеокамери "день-ніч" від контрасту фону та розміру об'єкта в кадрі, які можуть бути використані в адаптивно-регульованій системі освітлення інтелектуальної мобільної системи підводного відеоспостереження для забезпечення стабільності кольорового режиму.

Список літератури:

1. Функция "день-ночь" в видеокамерах – взгляд изнутри [Электронный ресурс] // Силикон-Сервис. Системы безопасности. – Режим доступа: http:// www.silicon-s.ru/info/day_night.html.

2. *Блінцов В.С.* Експериментальні дослідження відеосистеми телекерованого підводного апарата для захисту акваторій / *В.С.Блінцов, О.В.Блінцов, Ю.І.Касьянов та ін.* // Вісник Східноукраїнського національного університету імені Володимира Даля, №6 (136), Ч.1. – Луганськ: Видавництво СНУ ім. В.Даля, 2009. – с. 313 – 316.

3. *Касьянов Ю.І.* Оцінка стабільності кольорового режиму камери підводного відеоспостереження / *Ю.І. Касьянов, А.В. Гавриш* // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали II Всеукраїнської конференції з міжнародною участю. – Миколаїв: НУК, 2012.– с. 117 – 121.

4. *Касьянов Ю.І.* Дослідження автоматичної зміни режиму камер відеоспостереження з функцією "день-ніч" / *Ю.І. Касьянов, А.В. Гавриш* // Сучасні проблеми інформаційної безпеки на транспорті: Матеріали всеукраїнської науково-технічної конференції з міжнародною участю. – Миколаїв: НУК, 2013. – С. 46 – 51.

5. *Касьянов Ю.І.* Стабільність кольорового режиму в підводних системах відеоспостереження/ *Ю.І. Касьянов, А.В. Гавриш* // Вісник Східноукраїнського національного університету імені Володимира Даля, №15 (204), Ч.1. – Луганськ: Видавництво СНУ ім. В.Даля, 2013. – с. 77 – 82.

6. *Касьянов Ю.І.* Комплекс засобів для тестування відеокамер та відеосистем телекерованих підводних апаратів / *Ю.І. Касьянов* // Інновації в суднобудуванні та океанотехніці: Матеріали IV міжнародної науково-технічної конференції. – Миколаїв: НУК, 2013. – с. 448 – 450.

УДК 004.773+004.056.5

ЗАХИЩЕНА СИСТЕМА ВНУТРІШНЬО-СУДНОВОГО ЗВ'ЯЗКУ НА БАЗІ КОМП'ЮТЕРНОЇ МЕРЕЖІ СУДНА

Автори: *О.С. Медлярський, студент; В.І. Корицький, аспірант, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Система суднового зв'язку (ССЗ) є комплексом технічних засобів, призначених для забезпечення сигналів тривоги, інших сигналів, а також надійного зв'язку між містком і всіма постами та службами судна. При проектуванні таких систем особливу увагу слід приділяти проектуванню відповідного комплексу засобів захисту мовної інформації, що циркулює в мережі від витоку та/або несанкціонованого доступу. На рис. 1 зображено структуру ССЗ, яка побудована на базі локальної обчислювальної мережі судна з використанням технології VoIP.

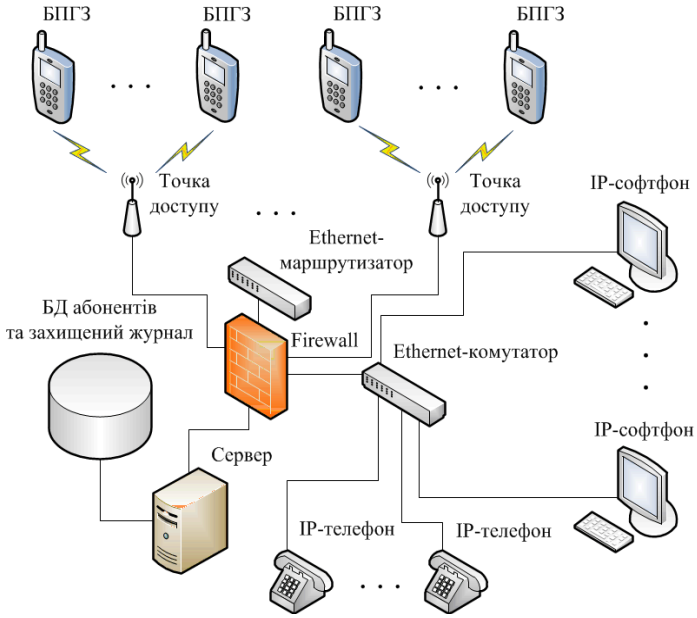


Рисунок 1 – Узагальнена структурна схема захищеної системи внутрішньо-суднового зв'язку

ССЗ являє собою мережу з мобільних та стаціонарних пристроїв голосового зв'язку топології «розширена зірка». Всі елементи мережі з'єднано з маршрутизатором із вбудованим між мережевим екраном (Firewall), що надає можливості запобігти наслідків від більшості атак, що можливі при підключенні зловмисника до іншого мережевого обладнання системи.

Стаціонарна компонента ССЗ представлена дротовими IP-телефонами та комп'ютерами із встановленим клієнтським програмним забезпеченням (IP-софтфонами). Також можлива інтеграція до мережі принтерів та іншого мережевого обладнання.

Мобільною компонентою системи є бездротові пристрої голосового зв'язку (БПГЗ), які з'єднані з дротовою мережею за допомогою Wi-Fi точок доступу. Дане рішення дозволить надати членам екіпажу можливість більш ефективно виконувати поставлені задачі за рахунок усунення необхідності постійного знаходження біля стаціонарного пристрою.

В процесі проектування комплексу засобів захисту ССЗ на базі положень, викладених в [1] та [2] був визначений оптимальний функціональний профіль захищеності системи зв'язку. На базі критеріїв даного профілю було розроблено апаратно-програмну конфігурацію ССЗ, склад якої представлений на рис. 2. На схемі зображено канал передачі мовної інформації типу «точка-точка» (абонент-сервер-абонент). Апаратне забезпечення абонента використовується для захвату та відтворення голосових даних у реальному режимі часу. Відповідне програмне забезпечення реалізує функції захисту даних від НСД, обробку дій користувача та інформаційний обмін із сервером.

ПЗ серверної частини системи організовано за модульним принципом. Обмін голосовими та службовими даними здійснюється засобами операційної системи. Модуль ідентифікації та автентифікації призначений для здійснення процедур ідентифікації та автентифікації абонентів, які хочуть приєднатись до захищеної системи голосового зв'язку. Модуль забезпечення конфіденційності представлений програмним інтерфейсом, який реалізує функції шифрування/дешифрування інформації. В якості основного модулем використовується симетричний алгоритм шифрування AES.

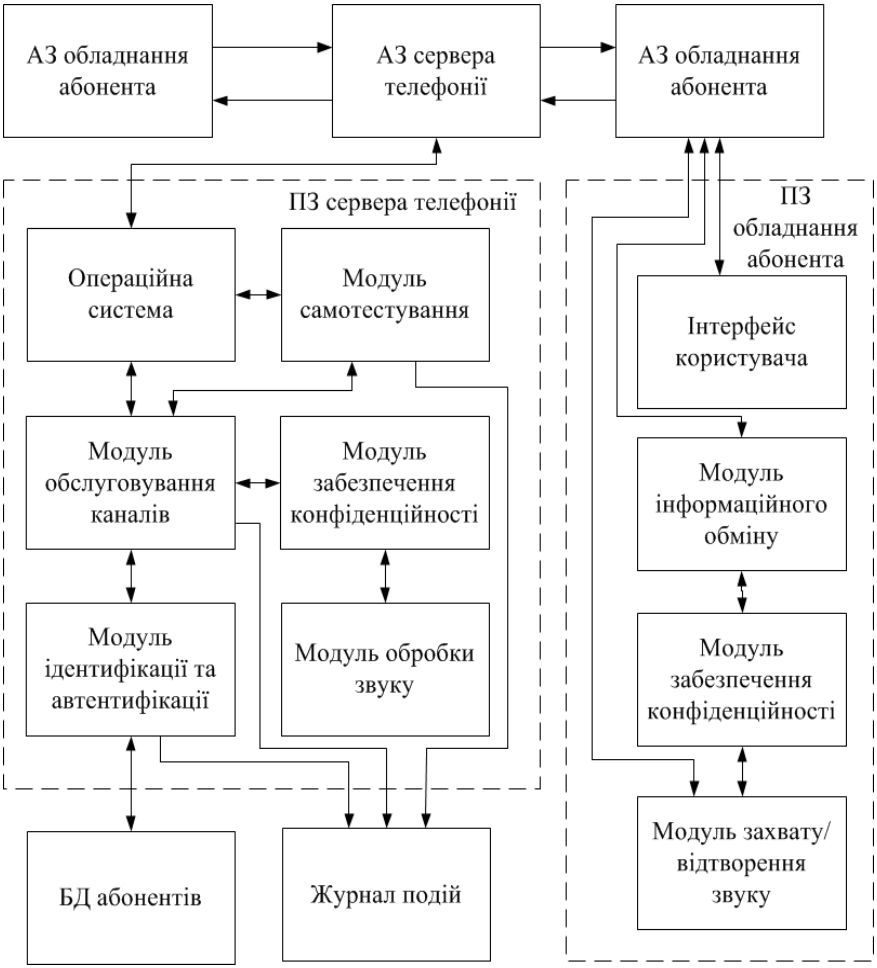


Рисунок 2 – Апаратно-програмна конфігурація системи суднового зв'язку

Висновки Розроблена ситстема реалізує мережу VoIP, трафік в якій захищено за допомогою потокового шифрування на основі симетричного алгоритму. Особливістю системи є можливість використання у її складі бездротових пристроїв голосового зв'язку із вбудованими алгоритмами захисту мовної інформації від несанкціонованого доступу.

Список літератури:

1. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу / Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – Офіц. Вид-во. – Київ, 1999. – 22 с.
2. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу / Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – Офіц. Вид-во. – Київ, 1999. – 59 с.

УДК 004.056

МЕТОДИКА ВИБОРУ МЕТОДУ ФОРМУВАННЯ ФУНКЦІЙ НАЛЕЖНОСТІ ДЛЯ ПРИКЛАДНИХ ЗАДАЧ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Автор: *М.В. Турти, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Вступ. В інформаційній безпеці нечіткі дані широко застосовуються при оцінюванні ефективності систем захисту, побудові систем моніторингу процесів і управління. Якщо відповідна система передбачає розпізнавання об'єктів, процесів та ситуацій, то первинною задачею для такої системи є побудова нечітких еталонів, що можуть бути представлені в різних формах, зокрема, у формі нечіткого числа. На даний час існують різноманітні методи побудови функцій належності (ФН) [1, 2], що характеризуються особливостями алгоритмів отримання та обробки експертних даних і здатні формувати ФН з певними властивостями, однак рекомендації щодо вибору методу формування ФН для певних прикладних задач наявні тільки для окремих методів і не мають систематизованого характеру [3-5].

Метою даної роботи є розробка методики вибору методу формування функцій належності для прикладних задач інформаційної безпеки.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

– проаналізувати галузі застосування нечітких еталонів (НЕ) в інформаційній безпеці;

– визначити вимоги до ФН, обумовлені специфікою застосування НЕ в різних галузях інформаційної безпеки;

– визначити критерії і розробити методику вибору методу формування функцій належності для прикладних задач інформаційної безпеки.

Основна частина.

Спектр задач обробки нечітких еталонів, що розв'язуються в інформаційній безпеці, визначається галузями застосування автоматизованих систем, що передбачають формування, обробку і отримання висновків щодо об'єктів і процесів систем захисту інформації за допомогою нечітких знань, зокрема, еталонів. Найчастіше нечіткі еталони використовуються в наступних системах:

– в системах оцінювання ефективності окремих технічних і криптографічних засобів захисту інформації, а також комплексів засобів захисту;

– в біометричних криптографічних системах для біометричної автентифікації, в яких ключ закривається біометричних еталоном користувача та зберігається в такому вигляді в базі даних;

– в біометричних криптографічних системах, в яких ключ витягується безпосередньо з біометричних даних користувача і не зберігається в базі даних;

– в криптографічних системах на основі методу «нечітких екстракторів», що дозволяє однозначно відновлювати секретний ключ з неточно відтворюваних біометричних даних і задавати довжину ключа у вигляді параметра;

– в системах «комп'ютерного зору», в яких для фрагментизація зображень зводиться до пошуку еталону на зображенні;

– в автоматизованих системах аналізу програмного забезпечення для виявлення його аномальної (відмінної від еталонної) поведінки на фазах запуску, специфічних дій та завершення роботи;

– в системах моніторингу інформаційної безпеки;

– в системах управління інформаційною безпекою;

– в системах управління окремими технічними засобами захисту інформації.

Основною вимогою до моделей задач обробки нечітких еталонів у цих системах є те, що вони повинні описувати такі операції як об'єднання, різниця, перетинання двох або більше нечітких множин (НМ) при визначенні відповідності об'єкта і образа. Ці операції можуть

бути здійснені різними методами, які базуються на виконанні таких процедур як визначення добутку і доповнення, концентрування і розтягування однієї нечіткої множини в тому випадку, якщо НЕ представляє собою правило, в антиценденті якого використовуються нечіткі свідоцтва.

Операції над окремими нечіткими множинами, що дозволяють визначити їх окремі характеристики (наприклад, центр тяжіння, толерантність чи полімодальність, носій тощо), можуть бути використані в системах контролю доступу і криптографічних системах.

В системах контролю доступу, системах моніторингу інформаційної безпеки, системах управління, які базуються на процедурах порівняння нечітких параметрів об'єкта і раніше сформованих нечітких еталонів в режимі реального часу критеріями якості НЕ можна визнати параметри, що впливають на швидкість отримання нечітких характеристик об'єкта і швидкість виконання процедур порівняння, їх здатність забезпечувати визначеність висновку процедур порівняння і можливість використання одного НЕ, сформованого експертним шляхом, в різних системах з різними методами обробки. Крім того, слід враховувати швидкість створення самого НЕ, що визначається кількістю даних, які повинні бути отримані експертним шляхом, швидкістю опитування експертів та кількістю елементарних процедур, які мають бути виконані при формуванні НЕ за певним методом, а також прозорість процедур методу та його вимоги до обчислювальних ресурсів, зокрема, задіяний обсяг пам'яті.

Швидкість отримання нечітких характеристик об'єкта визначається кількістю цих характеристик, швидкістю їх вимірювання, точністю вимірювань та кількістю елементарних процедур, що виконуються при визначенні ФН певним методом.

Швидкість отримання висновку щодо відповідності чи невідповідності ФН об'єкта та НЕ визначається кількістю застосованих методів порівняння, методом отримання узагальненого висновку на основі висновків за окремими методами, кількістю елементарних процедур, що виконуються при порівнянні функцій належності за кожним із застосованих методів порівняння. При цьому кількість елементарних процедур для деяких методів порівняння суттєво зростає, якщо характеристики об'єкта вимірюються незалежно від параметрів НЕ, що зберігається в пам'яті системи, напри-

клад, незалежно від визначених координат носія НМ чи від визначених α –рівнів, оскільки тоді повинні виконуватися додаткові процедури, наприклад, розбивання НМ на α –рівневі підмножини, розрахунок координат носія при певних значеннях ФН чи розрахунок значень ФН при певних координатах носія НМ. Таким чином, додатковою вимогою до методів формування ФН об'єкта в таких системах є їх узгодженість з методами порівняння і методами формування НЕ в плані мінімізації кількості елементарних операцій додаткових перетворень.

Якщо НЕ використовується в адаптовній системі, яка призначена для вирішення задач класифікації, тобто автоматично утворює нові НЕ, то метод визначення їх ФН має бути узгодженим як з методами створення діючих НЕ, так і з методами ідентифікації ситуації, коли дані об'єкта не можуть бути визнані подібними до жодного НЕ з бази і виникає потреба формування нового НЕ. В таких системах вимоги щодо швидкості формування НЕ є підвищеними, оскільки дія відбувається в реальному часі, і визначається кількістю даних, за якими формується НЕ, та швидкістю їх отримання, кількістю елементарних процедур, які мають бути виконані при формуванні НЕ за певним методом, а також вимоги методу до обчислювальних ресурсів, зокрема, задіяний обсяг пам'яті.

Розроблена методика вибору методу формування функцій належності для прикладних задач інформаційної безпеки містить наступні етапи:

1. Аналіз прикладної задачі і визначення вимог до функцій належності, обумовлених її специфікою, зокрема:
   - вимог до мінімізації обсягу пам'яті;
   - вимог до максимізації швидкості визначення ФН;
   - вимог до мінімізації тривалості діалогу з експертами;
   - вимог до спектру виконуваних операцій з нечіткими множинами;
   - вимог до швидкості виконання операцій з нечіткими множинами;
   - вимог щодо наявності у ФН певних властивостей з точки зору швидкості виконання операцій з нечіткими множинами і обсягу використовуваної пам'яті;
   - вимог, обумовлених узгодженістю та адаптацією системи.
2. Ранжування визначених вимог до ФН будь-яким методом, наприклад методом попарного порівняння на рангових оцінках [4].
3. При наявності вимог до властивостей ФН – визначення методів, що дозволяють сформувати ФН із заданими властивостями.

4. Оцінка визначених у п.3 методів формування ФН з точки зору вимог до швидкості визначення і обробки ФН; обсягу пам'яті, задіяної при формуванні та обробці нечітких множин; мінімізації тривалості діалогу з експертами. Оцінка швидкості визначення і обробки ФН та тривалості діалогу з експертами може здійснюватися за кількістю виконуваних елементарних процедур, а оцінка обсягу пам'яті – за кількістю і типами вхідних, проміжних і вихідних даних. Отримані оцінки мають вигляд функцій від кількості експертів та кількості елементів НМ.

5. Отримання вектору пріоритетів методів формування ФН з врахуванням вагових коефіцієнтів вимог.

Висновки. В даній роботі на основі аналізу особливостей вимог до ФН, обумовлених специфікою застосування НЕ в різних галузях інформаційної безпеки, визначені критерії вибору методу формування функцій належності для прикладних задач інформаційної безпеки і розроблена відповідна методика.

Список літератури:

1. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: "МК-Пресс", 2006. – 320 с.

2. Турти М.В. Теорія однозначних нечітких систем та нейронні мережі: Монографія. Частина 1. – Миколаїв: Вид-во Європейський університет, Миколаївська філія, 2007. –140 с.

3. Ротштейн А.П. Интеллектуальные технологии идентификации. – Винница: «Универсум Винница», 1999.- 320 с.

4. Турти М.В. Використання однозначної нечіткої логіки в системах технічного захисту інформації //Вісник Східноукраїнського національного університету ім.В.Даля.- 2009.- №6(136).- Ч.1.- С.104-109.

5. Турти М.В. Процедура формування нечітких еталонів на основі попарних порівнянь //Вісник Східноукраїнського національного університету ім.В.Даля. – Луганськ: Вид-во СНУ ім.В.Даля, 2013. – №15(204).- Ч.1. – С.204-209.

СЕКЦІЯ 2. ЗАХИСТ ІНФОРМАЦІЇ НА ОБ’ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ ТА В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

МЕТОДИ БОРОТЬБИ З БОТ-МЕРЕЖАМИ ПРИ РОЗПОДІЛЕНИХ АТАКАХ НА ВІДМОВУ В ОБСЛУГОВУВАННІ

Автори: *С.В. Дмитриченко; Р.В. Баронов, Головне управління Державної служби спеціального зв’язку та захисту інформації України у Миколаївській області, м. Миколаїв*

В роботі представлені результати аналізу методів боротьби з бот-мережами. Наведено огляд методів розповсюдження шкідливого коду на комп’ютери жертв, які стають частиною бот-мережі, розглянуто методи боротьби з такими мережами.

Ключові слова – бот-мережа, розподілена відмова в обслуговуванні.

ВСТУП

У сьогоденні в мережі Інтернет спостерігається очевидна тенденція до поширення зловмисниками так званих бот-мереж.

Бот-мережі (від англ. botnet – robot і network), по суті, дозволяють об'єднати в самостійну мережу обчислювальні потужності великої кількості вразливих комп’ютерів. Метою даного об'єднання є виконання таких дій як пошук уразливих хостів, реалізація атак типу “розподілена відмова в обслуговуванні” (DDoS), розсилання “спаму”, одержання конфіденційної інформації.

Функціонування бот-мереж характеризується одночасними діями великої кількості бот-агентів в інтересах зловмисника. У більшості випадків зловмисник одержує повний контроль над ресурсами інфікованого комп'ютера й може їх безперешкодно використовувати [1,2,3].

МЕТОДИ РОЗПОВСЮДЖЕННЯ БОТ-МЕРЕЖ

Якщо розглянути типи поширення бот-мереж, то їх практично не відрізнити від поширення звичайного шкідливого програмного забезпечення «malware». Сам же бот являє із себе програмний код або вже скомпільовану програму, яка інтегрується в цільову систему шляхом реалізації її вразливостей.

Тіло бота може робити ін'єкції в системні процеси, тим самим приховуючи свою присутність у системі імітуючи службовий сервіс.

Для приховування своїх дій вони також можуть використовувати rootkit технології, які дозволяють сховати дії механізму віддаленого управління (Remote Administration Tool, RAT) від користувачів.

Шкідливе програмне забезпечення є найбільш поширеним на системах сімейства Windows внаслідок особливостей системної архітектури.

Система дозволяє процесам мати доступ до області пам'яті інших додатків, читати їх і змінювати. Зовнішні засоби захисту, такі як антивіруси або мережеві екрани допомагають захиститися всього лише від відомих видів загроз. Незважаючи на вдосконалення систем захисту ОС сімейства Microsoft Windows, ймовірність реалізації загроз залишається досить високою.

Окрему ланку займають методи соціальної інженерії, коли шляхом модифікації або повної підміни програмного коду легітимного ПЗ можливо переконати користувача власноруч завантажити, та запустити шкідливий додаток з наданням йому привілейованих прав доступу до системи.

Аналіз останніх вразливостей різного роду найбільш популярних веб-браузерів (Internet Explorer, Mozilla Firefox, Opera, Safari, Google Chrome) слід зазначити, що використання помилок в системі їх захисту можливо реалізувати деякі з зазначених загроз.

МЕТОДИ ЗАХИСТУ ВІД БОТ-МЕРЕЖ

Найпоширенішим методом розповсюдження бот- мереж є використання шкідливих додатків – «черв'яків» (англ. "worms"), на протидію яким виділяються наступні методи захисту:

– попередження та еврістика – уникнення зараження шкідливим ПЗ
– лікування – після того, як зараження відбулось
– стримування – зниження можливостей взаємодії між зараженими і вразливими клієнтськими комп'ютерами

Лікування звично використовується на хостах, в той час як на мережевому устаткуванні використовуються методи попередження і стримування:

1. Механізми, засновані на "дроселюванні/регулюванні вірусів".
2. Основною ідеєю є відсіювання підозрілих хостів з занадто частими звертаннями до хосту. Кожен раз при запиті аналізується, чи був

вже схожий запит. Якщо запит новий і черга затримки обробки запитів дуже велика – то обмежувач запитів ігнорує нові запити.

3. Механізми, засновані на інтелектуальному аналізі невдалих з'єднань. Алгоритм аналізу базується на AIS (Artifical Immune System – штучна імунна система, англ.). Якщо відбувається нормальне з'єднання (TCP SYN/ACK) – то лічільник зменшується. Як тільки проходить перше невдале з'єднання з підробної адреси до адреси назначення – адреса записується і пакет ігнорується. Нормальна мережева активність теж зменшує лічільник. Механізм обнуляє лічільник кожні три дні.

4. Механізми, засновані на методі "порогового випадкового прохождения" (Threshold Random Walk) (Nagaonkar , Mchugh, 2008)

5. Механізми обмеження інтенсивності з'єднань на основі кредитів довіри.

6. (Credit Base-based Rate Limiting) Також загрозою може бути використання несертифікованого ПО, що може як робити систему хоста вразливою до зовнішніх атак, так і містити бот-код.

ВИСНОВКИ

На сьогоднішній день ботнети є одним з основних джерел нелегального заробітку в Інтернеті і грізною зброєю в руках зловмисників.

Чекати, що кіберзлочинці відмовляться від настільки ефективного інструменту, не доводиться, і експерти з безпеки з тривогою дивляться в майбутнє, очікуючи подальшого розвитку ботнет-технологій. Небезпека ботнетів посилюється тим, що їх створення і використання стає все більш простим завданням, з якою в найближчому майбутньому будуть в змозі впоратися навіть школярі, в той час як ціни на розвинутому і структурованому ботнет-ринку досить помірні.

У побудові міжнародних ботнетів можуть бути зацікавлені не тільки кіберзлочинці, а й держави, готові використовувати бот-мережі як інструмент політичного тиску та ведення кібернетичних війн. Крім того, можливість анонімно управляти зараженими машинами незалежно від їх географічного знаходження дозволяє провокувати конфлікти між державами: досить організувати кібератаку на сервери однієї країни з комп'ютерів іншої.

Список літератури:

1. Коновалов А.М., Шоров А.В. «Моделирование противодействия бот-сетей и механизмов защиты от них», СПИИРАН, материалы конференции РусКрипто'2011 – 36 с.
2. Грайворонський М. В., Новіков О. М. Г14 Безпека інформаційно-комунікаційних систем. – К.: Видавнича група ВНУ, 2009. – 608 с.
3. Биячуев Т.А. – Безопасность корпоративных сетей. – СПб, СПб ГУ ИТМО, 2004.- 161 с.

УДК 004.056.5: 534.7/.8

АДАПТАЦІЯ МОДУЛЯЦІЙНОГО МЕТОДУ ВИЗНАЧЕННЯ РОЗБІРЛИВОСТІ МОВИ ДО ЗАДАЧ ОЦІНКИ ЗАХИЩЕНОСТІ МОВНОЇ ІНФОРМАЦІЇ

Автори: *Ю.І. Касьянов, ст. викладач; Т.О. Кубарєва, студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Захист мовної інформації досягається проектно-архітектурними рішеннями, проведенням організаційних і технічних заходів. Використання тих або інших методів і засобів визначається характеристиками об'єкта захисту й апаратури розвідки, умовами її ведення, а також вимогами, що висуваються до захищеності мовної інформації. Важливою задачею при цьому є об'єктивна оцінка ефективності цих заходів та ступеня захищеності, яка проводиться при атестаційних випробуваннях та в процесі оперативного контролю [1, 2].

Оскільки суттєвий вплив на погіршення сприйняття мовної та іншої акустичної інформації мають різного роду шумові завади, і методи захисту акустичної інформації основуються на забезпеченні такого співвідношення між корисним сигналом і шумом, при якому сприйняття інформації в певній мірі було би неможливим, то в якості критерію захищеності використовують відповідність нормам відношення сигнал/шум, виміряного в контрольних точках можливого знімання інформації [3].

Однак, останнім часом набуває широкого вжитку критерій розбірливості мови, який більш точно відображає сприйняття смислової

складової мовного повідомлення й ефективність прийнятих заходів захисту мовної інформації існуючим загрозам. Тому, розробка, удосконалення і адаптація методів оцінки розбірливості мови для задач захисту мовної інформації наразі є дуже актуальною задачею.

Вважається, що найбільшою точністю і оперативністю володіють методи, в основу яких покладена формантна теорія мови. На базі цих методів російськими вченими створено методику оцінки захищеності мовної інформації [4, 5], яка рекомендована Гостехком Росії до використання.

Але формантні методи не дозволяють враховувати вплив реверберaційної завади на розбірливість мови, що важливо для приміщень зі значним часом реверберації, наприклад: актових та конференц-залів, де подається інформація з обмеженим доступом. В цьому плані перспективним є використання модуляційних методів визначення розбірливості мови, які враховують вплив не тільки шумових завад, але і завад у вигляді реверберації [6, 7].

Метою даної роботи є адаптація модуляційного методу визначення розбірливості мови до задач захисту інформації та розробка методики досліджень акустичної захищеності мовної інформації по критерію розбірливості мови модуляційним методом.

Суть модуляційних методів полягає в тім, що мовний сигнал розглядається як широкосмуговий шумовий сигнал (90...11200 Гц) зі спектром довготривалої мови, модульований іншим сигналом з низькою частотою (0,63…16 Гц), яка визначається швидкістю вимови фонем (швидкістю артикуляції). Вплив як шуму, так і реверберації при проходженні мовного сигналу по каналу передачі призводить до зниження глибини модуляції корисного сигналу і зниженню його розбірливості. Після проходження по каналу передачі (витоку) мовної інформації сигнали вимірюються і визначається функція передачі модуляції, з якої визначають відношення сигнал/шум та розбірливість мови.

Існує кілька модуляційних методів: STI та STIr (модифікований STI), RASTI (швидкий STI), STITEL (STI для телекомунікаційних систем), STIPA (STI для систем звукопідсилення) [8].

Методика, що пропонується, включає 4 етапи (рис.1).

Зміст організаційного та аналітичного етапів аналогічний існуючим сертифікованим методикам контролю захищеності мовної інформації.

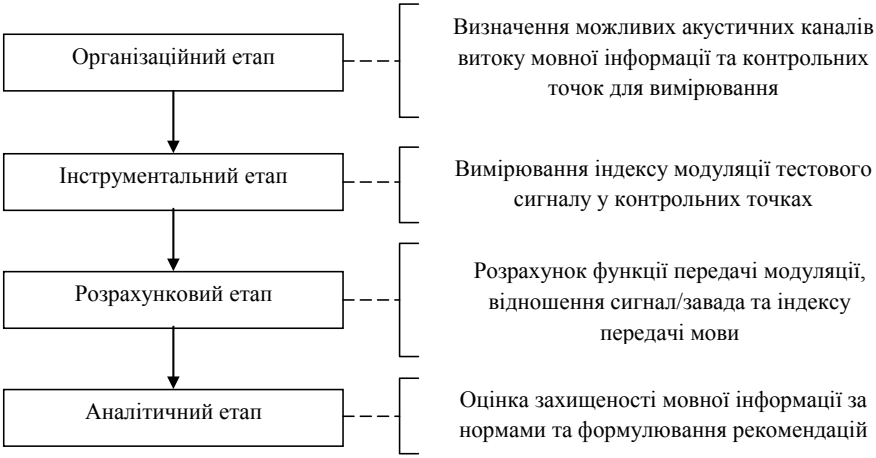


Рисунок 1 – Етапи оцінки акустичної захищеності мови при використанні модуляційних методів

При розробці інструментально-розрахункових процедур методики враховано наступні моменти:

– час та кошти на проведення спеціальних досліджень, а тим більш на контрольні випробування, захищеності виділених приміщень від витоку мовної інформації, як правило, є обмеженими;

– згідно з нормами захищеності мовної інформації рівень корисного сигналу в контрольних точках повинен бути нижче рівня фонового шуму, що відповідатиме дуже малим коефіцієнтам модуляції сумарного сигналу і може зробити недопустимою точність їх визначення.

Повна версія методу STI передбачає вимірювання по 14 частот модуляції з третьоктавним інтервалом, починаючи з 0,63 Гц, для 7 октавних смуг мовного діапазону з середньогеометричними частотами 125; 250; 500; 1000; 2000; 4000 і 8000 Гц (загалом 98 варіантів), що є мало прийнятним при дефіциті часу. Тому до використання взято метод RASTI відповідно до стандарту IEC 268-16. Це дозволило скоротити кількість варіантів до 9-ти (табл. 1).

Таблиця 1 – Множина частот метода RASTI

Центральні частоти смуг	500 Гц	2 кГц
Частоти модуляції, Гц	1; 2; 4; 8	0,7; 1,4; 2,8; 5,6; 11,2

Етап інструментальних вимірювань полягає у генерації тестового акустичного сигналу за допомогою апаратного чи програмного генератора ГТС (рис.2) з регульованим спектром та амплітудною модуляцією та вимірюванні коефіцієнта модуляції сигналу в контрольній точці. Вимірювання можна виконувати осцилографом ОС, підключеним до вимірювального мікрофона МКФ через вимірювальний підсилювач ВП та блок октавних фільтрів БОФ. Рівень фонового шуму вимірюється шумоміром ШМ.

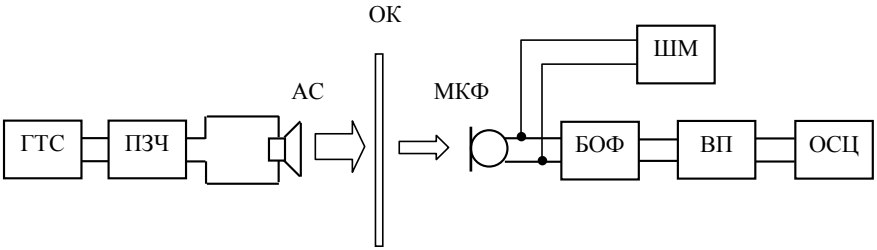


Рисунок 2 – Схема лабораторної установки

Рівень інтенсивності тестового сигналу повинен бути в октавній смузі з середньогеометричною частотою 500 Гц на 1 дБ, а в октавній смузі з середньогеометричною частотою 2 кГц на 10 дБ нижче інтегрального рівня мови, характерного для даного приміщення (вимірюється шумоміром). Тим самим для даних двох октавних смуг забезпечується відповідність спектра тестового сигналу спектру довготривалої мови. Коефіцієнт модуляції тестового сигналу $M_т = 1$.

На розрахунковому етапі визначаються масив індексів передачі модуляції та масив ефективних відношень сигнал/завада для усіх варіантів тестового сигналу (функція передачі модуляції), усереднені ефективні відношення сигнал/завада для октавних смуг, інтегральне відношення сигнал/завада та індекс передачі мови (розбірливість мови).

Схема алгоритму інструментально-розрахункових етапів приведена на рис.3.

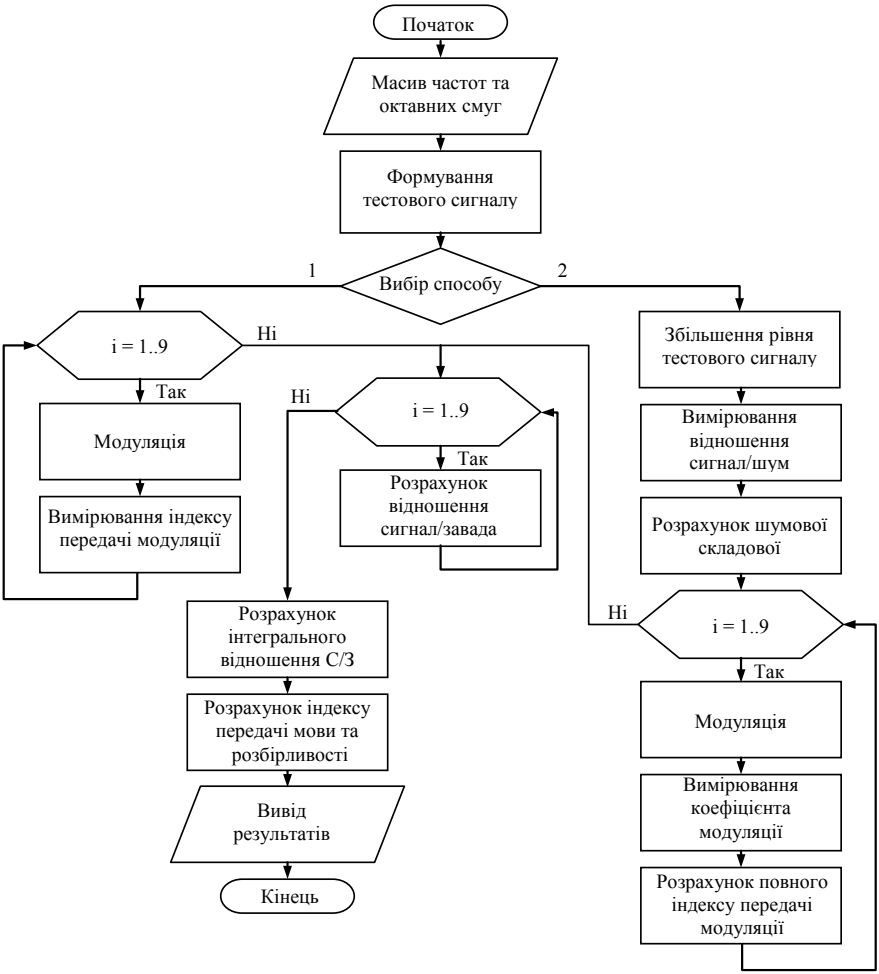


Рисунок 3 – Блок-схема алгоритму інструментально-розрахункових етапів

Перед виконанням програми вимірювань по осцилографу визначається достатність точності (можливість) визначення коефіцієнта модуляції, виходячи з найгіршого варіанту (враховуючи, що реверберація складова завади зростатиме з ростом частоти, це відповідатиме частоті модуляції 8 чи 11.2 Гц, залежно від частотної характеристики звукоізоляції огороджувальної конструкції).

Якщо точність достатня, то вимірювання проводяться за стандартною методикою RASTI. Якщо ж недостатня, то тестовий сигнал збільшується до рівня, при якому у контрольній точці рівень корисного сигналу перевищує рівень фонового шуму не менше чим на 15 дБ, і використовується підхід, описаний в [6].

Висновок: Розроблено методику оцінки захищеності мовної інформації від витоку прямим акустичним каналом за критерієм розбірливості мови з використанням модуляційного методу RASTI. В методиці враховано можливість низького рівня корисного сигналу по відношенню до завади в контрольних точках вимірювання. Використання даної методики дозволить враховувати вплив як шумової, так і реверберації завади.

Список літератури:

1. *Торокин А.А.* Инженерно-техническая защита информации / *А.А. Торокин*. – М.: Гелиос АРВ, 2005. – 960 с.

2. Технические средства и методы защиты информации / *А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др.* – М.: ООО "Издательство Машиностроение", 2009 – 508 с.

3. Методика контролю захищеності мовної інформації від витоку акустичним та віброакустичним каналами: НД ТЗІ 2.3-017-08. – К.: ДССЗЗІ України, 2008. – 18 с.

4. *Хорев А.А.* Методы защиты речевой информации и оценки их эффективности / *А.А.Хорев, Ю.К. Макаров* // Защита информации. Конфидент. – 2001. – № 4. – С. 22 – 33.

5. *Дворянкин С.В.* Обоснование критериев эффективности защиты речевой информации / *С.В. Дворянкин, Ю.К. Макаров, А.А. Хорев* // Защита информации. Инсайд. – М.: 2007. – №2. – С.39-45.

6. Акустическая экспертиза каналов речевой коммуникации. Монография / *Дидковский В.С., Дидковская М.В., Продеус А.Н.* – Киев: Имэкс-ЛТД, 2008. – 420 с.

7. *Продеус А.Н.* Формантный и формантно-модуляционный методы оценки разборчивости речи. Часть 1. Унификация алгоритмов / *А.Н. Продеус, Л.Б. Дронжевская, В.А. Климков, Д.А. Шагитова* // Электроника и связь. – 2010. – №6 (59), ч.2. – С. 117 – 124.

8. *Рашевский Я.И.* Обзор зарубежных методов определения разборчивости речи / *Я.И. Рашевский, В.Л. Каргашин* // Специальная техника. – 2002. – № 4 – 6, 2003. – №1.

УДК 004.056.5: 534.7/.8: 699.844

КРИТЕРІЙ РОЗБІРЛИВОСТІ МОВИ В ОЦІНЦІ ЗВУКОІЗОЛЯЦІЇ

Автори: *Ю.І. Касьянов, ст. викладач; А.Ю. Нохріна, студентка; А.І. Кривда, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Захист мовної інформації є однієї з найважливіших завдань у загальному комплексі заходів щодо забезпечення інформаційної безпеки об'єктів та установ. Це обумовлено тим, що мовна інформація має високе смислове навантаження і є основним засобом комунікації між людьми.

Оскільки мова є акустичним сигналом, то перш за все потрібно виключити витік мовної інформації прямим акустичним каналом. Одним з основних способів вирішення цієї задачі є забезпечення необхідного рівня звукоізоляції.

Існуючі методики оцінки звукоізоляції, в тому числі в області інформаційної безпеки, побудовані на співставленні рівня сигналу до і після огороджувальної конструкції [1, 2]. Визначається як інтегральний рівень звукоізоляції, так і залежність коефіцієнта звукоізоляції від частоти. Але дані методики орієнтовані на шумові сигнали і у якості тестового сигналу використовується сигнал білого шуму. Цього повністю достатньо для вирішення задач захисту від шуму тощо. В задачах же захисту мовної інформації потрібно враховувати властивості і особливості мовного сигналу.

Витік мовної інформації визначається зрозумілістю смислового змісту розмови, що залежатиме від розбірливості мови в точці прослу-

ховування. Тому для оцінки захищеності мовної інформації широкого впровадження на разі набуває критерій розбірливості мови.

Російськими вченими під керівництвом А.А.Хорева розроблено інструментально-розрахункову методику оцінки захищеності мовної інформації від витоку акустичним каналом [3, 4], що базується на формантному методі визначення розбірливості мови в інтерпретації Покровського [5] з апроксимацією окремих залежностей аналогічно методу АІ, що дає можливість автоматизації розрахунків. Ця методика рекомендована Гостехкомісією Росії до використання.

В Україні питанням розвитку методів визначення розбірливості мови та використання їх для задач інформаційної безпеки присвячено роботи В.С. Дідковського, А.М. Продеуса та ін. [6, 7]. В роботі [7] обґрунтовано необхідність встановлення зв'язку між звукоізоляцією та розбірливістю мови.

Метою даної роботи є отримання і порівняльний аналіз частотних залежностей октавних рівнів звукоізоляції та відносного зниження формантної розбірливості за рахунок звукоізоляції для типової огороджувальної конструкції (ОК).

Для дослідження було взято типову одношарову дверну конструкцію. Схема лабораторної установки показана на рис. 1. В якості генератора ГС використано генератор шуму з регульованим спектром [8]. Сигнал відтворювався активною акустичною системою Gemix TF-611 та вимірювався шумоміром ВШВ-003.

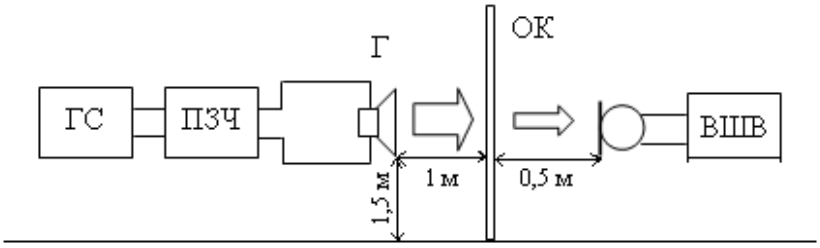


Рисунок 1 – Схема лабораторної установки

Вимірювання та розрахунок октавних рівнів звукоізоляції виконувались за стандартизованою методикою, детально описаною в [2]. При цьому генератором задавався тестовий сигнал "білого" шуму з

інтегральним рівнем 70 дБ (на відстані 0,5 м від гучномовця) та вимірювались його рівні L_{Ti} у семи октавних смугах з середньогеометричними частотами: 125, 250, 500, 1000, 2000, 4000, 8000 Гц. Потім в контрольній точці (на відстані 0,5 м за огороджувальною конструкцією) вимірювались октавні рівні шуму $L_{шi}$ (при відсутності тестового сигналу) та сумарного сигналу $L_{(с+ш)i}$. Октавні рівні корисного сигналу в контрольній точці розраховувались за співвідношенням

$$L_{сi} = \begin{cases} L_{(с+ш)i}, \text{ якщо } L_{(с+ш)i} - L_{шi} \geq 10 \\ L_{(с+ш)i} - \Delta, \text{ якщо } L_{(с+ш)i} - L_{шi} < 10 \end{cases}, \quad (1)$$

де Δ – поправка, взята з табл.1.

Таблиця 1 – Поправка рівня корисного сигналу

$L_{(с+ш)i} - L_{шi}$	≥ 10	6…10	4…6	3	2	1	0,5
Δ	0	1	2	3	4	7	10

Октавні рівні звукоізоляції Q_i розраховувались за формулою

$$Q_i = L_{Ti} - L_{сi}. \quad (2)$$

Отримана частотна характеристика звукоізоляції приведена на рис.2.

Аналогічні вимірювання і розрахунки були проведені для тестового сигналу зі спектром, що відповідає узагальненому спектру довготривалої мови. При інтегральному рівні сигналу 70 дБ його рівні в октавних смугах становили відповідно 63, 66, 66, 61, 56, 53, 49 дБ. Розрахунок октавних рівнів звукоізоляції підтвердив, що вони не залежать від рівня і спектру сигналу, відхилення знаходяться в межах похибки вимірювання (рис.2).

Для даного тестового сигналу було визначено відношення сигнал/шум в контрольній точці та розраховано розбірливість формант в октавних смугах A_i (спектральний індекс артикуляції) по інструментально-розрахунковій методиці. При цьому, враховуючи, що вимірювання проводились у семи октавних смугах, у формулі, що апроксимує залежність $A_m(f)$, потрібно було змінити частотний діапазон

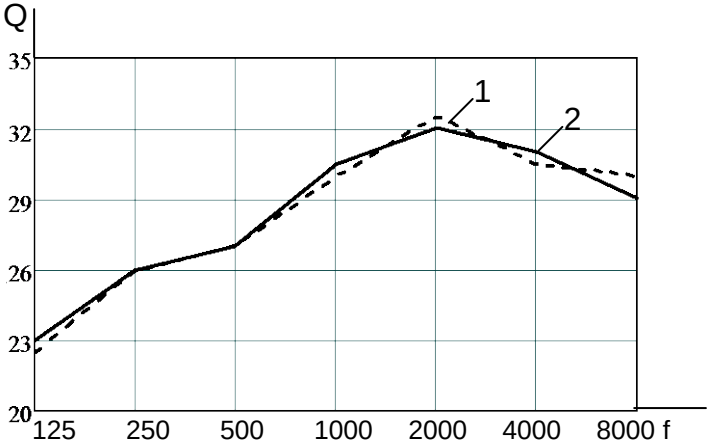


Рисунок 2 – Частотна характеристика звукоізоляції:
1 – при тестовому сигналі "білого" шуму;
2 – при тестовому сигналі зі спектром довготривалої мови

$$A_m(f) = \begin{cases} 2{,}57 \cdot 10^{-8} \cdot f^{2{,}4}, & \text{якщо } 90 \le f \le 400 \text{ Гц}; \\ 1 - 1{,}074 \exp(-10^{-4} \cdot f^{1{,}18}), & \text{якщо } 400 < f \le 11200 \text{ Гц}. \end{cases} \quad (3)$$

Графік залежності розбірливості формант в октавних смугах від частоти наведено на рис. 3. Там же приводяться залежності максимальної формантної розбірливості (ймовірності появи формант) A_{mi}, ймовірності сприйняття формант P_i , та абсолютних

$$\Delta A_i = A_{mi} - A_i \quad (4)$$

і відносних

$$\delta A_i = \frac{A_{mi} - A_i}{A_{mi}} = 1 - P_i \quad (5)$$

втрат формант у октавних смугах (зниження спектрального індексу артикуляції). Відносні втрати формант являють собою ймовірність втрати.

Як бачимо, що, хоч рівень звукоізоляції в октавній смузі з середньогеометричною частотою 2000 Гц має максимум, кількість сприй-

нятих формант в ній є досить високою. Також з частотної характеристики звукоізоляції не можна передбачити високу ймовірність сприйняття формант в октавних смугах з середньогеометричними частотами 500, 1000 та 8000 Гц.

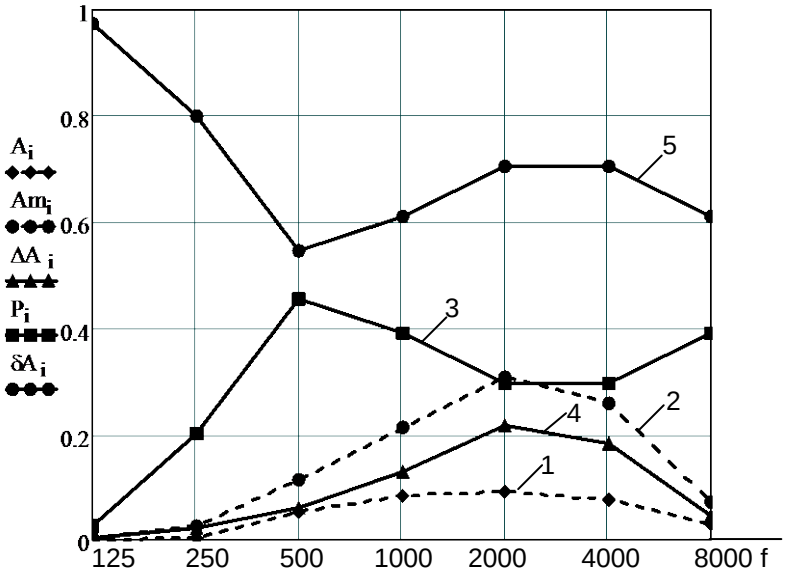


Рисунок 3 – Частотні залежності розбірливості формант (1), ймовірності появи формант (2), ймовірності сприйняття формант (3) та абсолютних (4) і відносних (5) втрат формант у октавних смугах

Важливо, однак, пам’ятати, що отримані характеристики будуть залежати від рівня та спектру корисного сигналу.

Висновок: Частотна характеристика звукоізоляції не дає можливості оцінити вплив звукоізоляційної конструкції на розбірливість мови. Використання частотних характеристик втрат формантної розбірливості, дозволить більш адекватно оцінювати можливості звукоізоляційних конструкцій та шумових завад щодо захисту мовної інформації.

Список літератури:

1. Конструкції будинків і споруд. Звукоізоляція огороджувальних конструкцій. Методи оцінювання: ДСТУ Б В.2.6-85:2009. – К. : Міжрегіонбуд, 2010. – (Національний стандарт України).

2. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. – М.: ООО "Издательство Машиностроение", 2009 – 508 с.

3. Хорев А.А. Методы защиты речевой информации и оценки их эффективности / А.А.Хорев, Ю.К. Макаров // Защита информации. Конфидент. – 2001. – № 4. – С. 22 – 33.

4. Дворянкин С.В. Обоснование критериев эффективности защиты речевой информации / С.В. Дворянкин, Ю.К. Макаров, А.А. Хорев // Защита информации. Инсайд. – М.: 2007. – №2. – С.39-45.

5. Покровский Н.Б. Расчет и измерение разборчивости речи / Н.Б. Покровский. – М.: Гос. изд-во литературы по вопросам связи и радио, 1962. – 392 с.

6. Акустическая экспертиза каналов речевой коммуникации. Монография / Дидковский В.С., Дидковская М.В., Продеус А.Н. – Киев: Имэкс-ЛТД, 2008. – 420 с.

7. Дідковський В.С. Зв'язок між розбірливістю мови та звукоізоляцією / В.С. Дідковський, В.П. Заєць, Д.П. Рудь, Н.О. Самійленко // Электроника и связь. – 2010. – № 3(56) – С. 131 – 143.

8. Касьянов Ю.І. Акустичний генератор шуму з регульованим спектром та фіксованими настройками / Ю.І. Касьянов // Захист інформації і безпека інформаційних систем: Матеріали 2-ої міжнародної науково-технічної конференції. – Львів: НУ "Львівська політехніка", 2013. – С. 136 – 137

УДК 004.056.5

СИСТЕМА ПРОТИДІЇ ДОСЛІДЖЕННЮ КОДУ АВТОРСЬКИХ ПРОГРАМНИХ ПРОДУКТІВ

Автор: *С.С. Козирєв, к.т.н., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Сучасні інформаційні системи та технології усе ширше використовуються в транспортній інфраструктурі для автоматизації процесів керування й контролю. Недооцінка питань інформаційної безпеки при впровадженні таких систем може привести до серйозних економічних та інших збитків. У зв'язку з цим зростає значення інформаційної безпеки на транспорті, особливо важливим є захист програмних продуктів, оскільки характеристики функціональності й надійності інформаційних систем визначаються якістю, надійністю та захищеністю програмних продуктів, що входять до їхнього складу. При цьому на перший план висувається безпека технологій створення програмних продуктів, що пов'язано з необхідністю внесення в програмні продукти захисних функцій на протязі всього життєвого циклу. Технології захисту програмних продуктів постійно розвиваються, оскільки тільки динамічний випереджаючий їх розвиток може забезпечити надійний тривалий захист.

Проблеми захисту програмних продуктів від злому і несанкціонованого доступу обумовлені швидким розвитком інформаційних технологій і зростаючою кількістю програм, сприяючих зворотній розробці, тобто дослідженню коду, а також відсутністю доступних та надійних методів розв'язання проблеми захисту коду, який міг би гідно протистояти як статичному, так і динамічному його аналізу.

Для злому сучасних програмних продуктів найчастіше використовують їхній динамічний аналіз для визначення місця перевірки ключа. Як правило, досить легко виявити місце звірення введеного ключа з заданим у програмі значенням і, модифікуючи код захищеної програми, домогтися її працездатності. Найбільш відомі методи захисту змінюють або блокують роботу налагоджувальних засобів [1].

В даній роботі для захисту від несанкціонованої модифікації програмних продуктів з метою впровадження програмних зловживань, а

також для захисту від незаконного використання алгоритмів, які є інтелектуальною власністю автора, при написанні аналогів програмного продукту (промислове шпигунство), пропонується використання алгоритмів обфускації (obfuscation – заплутування) для захисту програмних продуктів в процесі розробки.

Обфускація або заплутування коду – приведення вихідного тексту або виконуваного коду програми до виду, що зберігає її функціональність, але ускладнює аналіз, розуміння алгоритмів роботи та модифікацію при декомпіляції. «Заплутування» коду може здійснюватися на рівні алгоритму, на рівні вихідного коду програми, асемблерного тексту. Для створення заплутаного асемблерного тексту можуть використовуватися спеціалізовані компілятори, що використовують неочевидні або недокументовані можливості середовища виконання програми. Існують також спеціальні програми, що проводять обфускацію, так звані обфускатори.

Застосування обфускації дозволяє заплутати програмний код і усунути більшість логічних зв'язків у ньому шляхом побудови захисних фрагментів значної складності, що містять велику кількість перетворень, таких як розгалуження, шифрування й т.п. Тобто трансформувати код програми так, щоб він був дуже складним для аналізу й модифікації сторонніми особами.

З метою розробки ефективної системи програмного захисту проведено аналіз існуючих засобів технологічного захисту. Проаналізовано принципи роботи програм-обфускаторів, проведено огляд засобів та методів обфускації. На основі проведеного аналізу розроблено програмний метод захисту, оснований на спеціальних захисних алгоритмах лексичної обфускації та обфускації даних.

Висновки

В результаті проведених досліджень розроблена та реалізована система захисту програмних продуктів від дослідження, злому та несанкціонованого доступу, в основу якої покладено одночасне застосування сукупності захисних перетворень, що значно ускладнюють задачу злому та аналізу.

Отримали подальший розвиток узагальнені моделі лексичної обфускції та обфускації даних, які використано в розробленій системі захисту. Запропонований підхід до обфускації програм дозволяє підвищити складність зворотної трансляції і аналізу програми, оскільки заплутування програми являється багаторівневим і починається на

алгоритмічному рівні. Для реалізації методу опрацьовано методи розв'язання поетапних завдань на рівні даних як перенесення рядків з коду даних і видалення їх з динамічної пам'яті.

Створена система захисту із застосуванням методів на основі декількох різних видів заплутування коду може бути використана на різних операційних системах та комп'ютерах різної архітектури.

Список літератури:

1. Блінцов В.С. Захист програмних продуктів / В. С. Блінцов, С. С. Козирєв // Навч. Посібник. – Миколаїв: НУК, 2010. – 144 с.

УДК 004.056:534.6

НОВІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ ЗАХИЩЕНОСТІ АКУСТИЧНОЇ ІНФОРМАЦІЇ

Автор: *С.М. Нужний, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Актуальність. Розвиток інформаційного суспільства в Україні та широке застосування комп'ютерних (мережевих) технологій суттєво збільшив ризики витоку інформації по відповідним каналам. Однак, не зважаючи на такі зміни, канали витоку мовної інформації зостаються одними з найбільш вагомих джерел доступу до конфіденційної інформації. До найбільш задіяних з таких каналів відносяться перехоплення повідомлень в телекомунікаційних мережах (як дротові так і бездротові мережі) та використання беззахідних методик (спрямовані і лазерні мікрофони, віброакустичні стетоскопи та інші). Особливе значення витоку акустичної (мовної) інформації для України та світової спільноти показують останні події – перехоплення телефонних розмов та несанкціонований запис конфіденційних перемов видатних політичних діячів, в тому числі керівників держав, та військовослужбовців від МВС України, Генерального штабу ЗСУ, штабу АТО і до окремих бійців в зоні АТО.

Найбільш ефективним методом протидії витоку акустичної (мовної) інформації в наш час є використання активних методів зашумлення. Їх основою є генератори завади. До недавнішнього часу вони будувались на основі генераторів «білого шуму» та/чи його модифіка-

цій – так званих «кольорових шумів». Однак розвиток спеціалізованих напрямків аналізу складних сигналів та принципів формування мовних сигналів дозволили створити методики, які дозволяють проводити очищення фонограм сигналів від такого типу шумів.

Як заміну для генераторів «білого шуму», в наш час, передові виробники спеціалізованої апаратури запропонували генератори, які отримали додаткову функцію – «мовний хор» або як його називають в літературі «гомін (галас) натовпу». Головною перевагою таких генераторів є використання реальної людської мови [1]. Це призводить до появи зв'язаних частотних спектрів при формуванні мовних формант, які є основою при створенні гомону натовпу. Для збільшення рівня захищеності мовної інформації в деяких моделях VIP класу є можливість модифікувати (доповнювати) типовий мовний хор акустичною фонограмою дикторів, які знаходяться в контрольованій зоні.

Аналіз алгоритмів роботи генераторів «мовний хор» та пристроїв зашумлення на їх основі показує, що рівень захищеності мовної інформації від несанкціонованого доступу значно збільшується [1,2]. Однак і такі пристрої мають ряд системних недоліків. До основних з них відносяться: обмеженість довжини коду формування завади (тобто він є псевдо випадковим) та можливість проведення зловмисником фільтрації несанкціонованих фонограм методами виявлення нетипових фонем [3]. Безумовно, такий аналіз можливий тільки при наявності у зловмисника значного об'єму первинних записів, що суттєво обмежує його можливості.

Таким чином нагальною є **наукова проблема**, яка полягає в розробці нових підходів (теоретичних засад) пов'язаних із організацією, створенням методів та засобів забезпечення захисту акустичної (мовної) інформації в місцях її виникнення (контрольованих зонах) з використанням сучасних математичних методів, інформаційних технологій та технічних засобів.

Метою даної роботи є обґрунтування основних положень розробки нових технології й засоби захисту акустичної інформації від відпливу технічними каналами.

Для її досягнення необхідно вирішити наступні завдання:

1) Провести аналіз принципів побудови, технологічні рішення і напрямки розвитку активних систем протидії витоку акустичної (мовної) інформації за межі контрольованої зони з точки зору їх адекватності та можливого використання для вирішення поставленої проблеми.

2) Удосконалити математичну модель технічного каналу витоку комплексної акустичної (мовної) інформації за межі контрольованої зони з урахуванням впливу декількох джерел завади.

3) На основі методики професора М.Б. Покровського провести аналіз фонемної структури комплексного акустичного (мовного) сигналу з метою визначення основних вимог до системи активного зашумлення та допустимі кордони зміни параметрів фонемних змінних по критерію вірогідності виявлення небезпечного сигналу в комплексному акустичному (мовному) сигналу.

4) Розробити модель системи активної протидії витоку акустичної (мовної) інформації за межі контрольованої зони на основі генератора мовоподібного сигналу скремблерного типу (ГМПС СТ).

5) Розробити алгоритм та структурну схему ГМПС СТ.

6) Оцінити якість захищеності акустичної (мовної) інформації на межі контрольованої зони з урахуванням можливості використання зловмисником декількох точок несанкціонованого доступу до інформації.

Основний зміст.

В загальному випадку, акустичний (мовний) сигнал, який розповсюджується в контрольованій зоні створює складну просторову картинку розподілення інтенсивності звукової енергії. Вона складається з основної хвилі та безкінечного набору додаткових компонентів, створення яких обумовлене наявністю процесів відбиття (реверберації), розсіювання та дифракції. Наявність такої кількості хвиль може призводити до появи процесів інтерференції в окремих точках простору. Однак, вклад таких додаткових компонентів є незначним і ним можна знехтувати.

Існуючі методики проведення дослідження приміщень (контрольованих зон) на звукоізоляцію, в тому числі й затверджені в НД ТЗІ, основуються на представленні джерела акустичної енергії як точкового випромінювача. При цьому, для розрахунків, застосовується перехід від сферичної хвилі, яку створює точковий випромінювач, до рівномірної плоско-паралельно хвилі – тобто, додатковими компонентами знехтують.

Таким чином, в роботі при подальшому розгляді процесів формування віброакустичних коливань на поверхні конструкційних компонентів, які входять до складу периметру контрольованої зони, прийня-

то, що падаюча хвиля є плоско-паралельною та перпендикулярною до поверхні конструкційного елементу в будь-якій точці поверхні. Вказане припущення є справедливим, так як в моделях коливання пластин, які найшли широке використання в механіці коливань, розподілене по поверхні навантаження прикладується до умовної середньої, по товщині, лінії пластини. Наявність нерівностей (виступи, потовщення, впадини та інше) розглядається, при умові що їх розмір перевищує ¼ довжини хвилі, як додаткові ребра жорсткості та накладки, а врахування їх впливу на коливання пластини виконується шляхом застосування методу суперпозиції.

На основі вказаних теоретичних підходів, в роботі запропоновано удосконалену структурно-просторову модель (СПМ) акустичного каналу витоку мовної інформації (АКВМІ) в умовах використання пристроїв активного зашумлення (протидії) та використанням зловмисником декількох точок НСД на зовнішньому кордоні контрольованої зони. За основу при її створенні була використана СПМ АКВМІ, запропонована в [2]. Основним напрямком її вдосконалення стало введення додаткових елементів, які визначають вплив системи технічного захисту акустичної інформації, можливість використання зловмисником декількох комплексних АКВМІ, та рекомендації по розрахунку засобів акустичної розвідки, рекомендованих в [1].

Список літератури:

1. *Хорев А.А.* Оценка возможностей средств акустической (речевой) разведки // Специальная техника. – 2009. – № 4. – С. 49-63.

2. *Сагдеев К.М., Оленев А.А.* Математическая модель акустического канала утечки речевой информации // Фундаментальные исследования. – 2012. – № 6 (часть 3). – стр. 668-673.

3. *Бичковський О.М.; Нужний С.М.* Генератор мовоподібного шуму для систем просторового та лінійного зашумлення // Сучасні проблеми інформаційної безпеки на транспорті 2013: матеріали Всеукраїнської науково-технічної конференції з міжнародною участю: НУК, 2013.

КЛАССИФИКАЦИЯ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ РАДИОИЗЛУЧЕНИЙ

Автор: *В.В. Опарин, Научно-технический центр «Квант», г. Николаев*

При проектировании приборов поиска источников несанкционированных радиоизлучений необходимо учитывать все их многообразие, в противном случае эффективность создаваемой аппаратуры поиска будет недостаточной.

Передачу информации радиоизлучением представим в виде некоторого сообщения S

$$S=(f, t, \tau, w, \Delta f), \quad (1)$$

где: f – несущая частота; t – время начала передачи сообщения; τ – продолжительность передачи сообщения; w – мощность излучения передающего устройства; Δf – ширина спектра радиоизлучения.

Экспериментальные исследования показывают, что в соответствии с (1) радиоизлучения можно классифицировать следующим образом:

- радиоизлучения на фиксированной частоте с различными алгоритмами излучения во времени $t=\{t_i\}$;

- радиоизлучения со случайным изменением несущей частоты $f=\{f_i\}$ и различными алгоритмами излучения во времени $t=\{t_i\}$.

1. Радиоизлучения на фиксированной частоте можно представить следующим выражением:

$$s(t)=S(t)[\cos\omega_0 t+\Theta(t)], \quad (2)$$

где: амплитуда S(t) или фаза Θ(t) изменяются по закону передаваемого сообщения, модулированного аналоговым или цифровым сигналами $\omega_0=2\pi f_0$, где f_0 несущая частота.

1.1. Радиоизлучения с непрерывной передачей информации во времени ведутся при времени непрерывного излучения $\tau=T_{сут}$, где $T_{сут}=24$ часа. Примером такой передачи являются УКВ и FM-радиостанции, аналоговое и цифровое телевидение, базовые станции стандартов связи GSM 1800/900, CDMA, систем беспроводной связи Wi-Fi, ZigBee.

1.2. Кратковременное радиоизлучение имеет длительность передачи сообщения

$$\tau < T\text{сут}. \quad (3)$$

При этом время начала сообщения может быть случайным или априорно известным (например, перед началом важного совещания).

1.3. Сверхкороткая передача (СКП) производится со сжатием информации во времени. Начало передачи сообщения случайное. Длительность передачи информации зависит от ее объема С и емкости частотного канала $C_к$ и определяется

$$\tau = C/C_к. \quad (4)$$

Емкость частотного канала определяется по формуле Шеннона

$$C_к = \Delta f_к * \log_2(1+W/N). \quad (5)$$

где $C_к$ – емкость канала, бит/с; $\Delta f_к$ – полоса пропускання канала, Гц; W – полная мощность сигнала под. полосой пропускання, Вт или $В^2$; N – полная шумовая мощность, Вт или $В^2$.

1.4. Пакетная передача информации. Временная диаграмма пакетной передачи приведена на рис. 1.

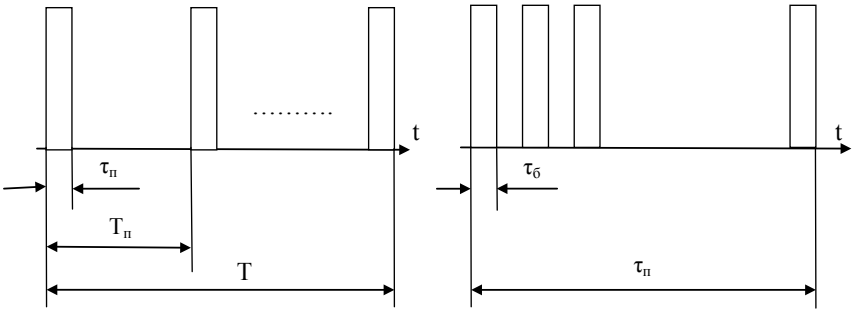


Рис. 1. Временная диаграмма пакетной передачи: $\tau_п$ – длительность пакетов; $T_п$ – период повторения пакетов; T – длительность передачи информации; $\tau_б$ – длительность бита информации

Математическую модель пакетной передачи можно представить следующим образом:

$$C = C\sum_{i=1}^{n} C_k \tau_{ni} \quad (6)$$

где $C_к$ – емкость частотного канала, определяется по формуле (5); $n=C/C_к$ – количество необходимых пакетов для передачи всей информации.

Длительность передачи сообщения:

$$T=n*T_{п}. \quad (7)$$

1.5. Шумоподобный сигнал (ШПС) применяется сокрытия факта передачи сообщения в объектовых шумах. Производится с применением широкополосного сигнала с мощностью излучения W_c на уровне или ниже уровня мощности объектовых шумов $W_ш$

$$W_c \leq W_ш . \quad (8)$$

Центральная частота априорно неизвестна.

1.6. Маскированный сигнал имеет назначение сокрытия факта передачи сообщения путем ее маскировки радиоизлучением одного из действующих радиосредств мощностью $W_{рс}$, приведенных в п.1.1.

$$W_c \leq W_{рс} . \quad (9)$$

2. Радиоизлучения с быстрой перестройкой рабочей частоты (БПРЧ).

2.1. Передача сообщения по частотным каналам мобильных телефонов стандарта GSM1800/900 в известных диапазонах частот Δf. Перестройка рабочей частоты по известным частотным каналам в известном диапазоне частот ΔF.

$$f=\{f_1, f_{2, \dots} f_n\}; n=\Delta F/\Delta f , \quad (10)$$

где n – количество каналов.

Начало сообщения с f_i частоты, где i – любой из n-каналов. Передача сообщения по m-любым каналам, m<n. Длительность сообщения определяется формулами (4) и (5).

Сонограмма такого сообщения в координатах время-частота приведена на рис. 2.

2.2. Псевдослучайная перестройка рабочей частоты (ППРЧ)

Перестройка рабочей частоты в априорно неизвестном диапазоне частот ΔF. Передача сообщения может начинаться в любое время суток. Длительность передачи зависит от объема передаваемой информации С и емкости частотного канала $C_к$ и определяется по формулам (4) и (5).

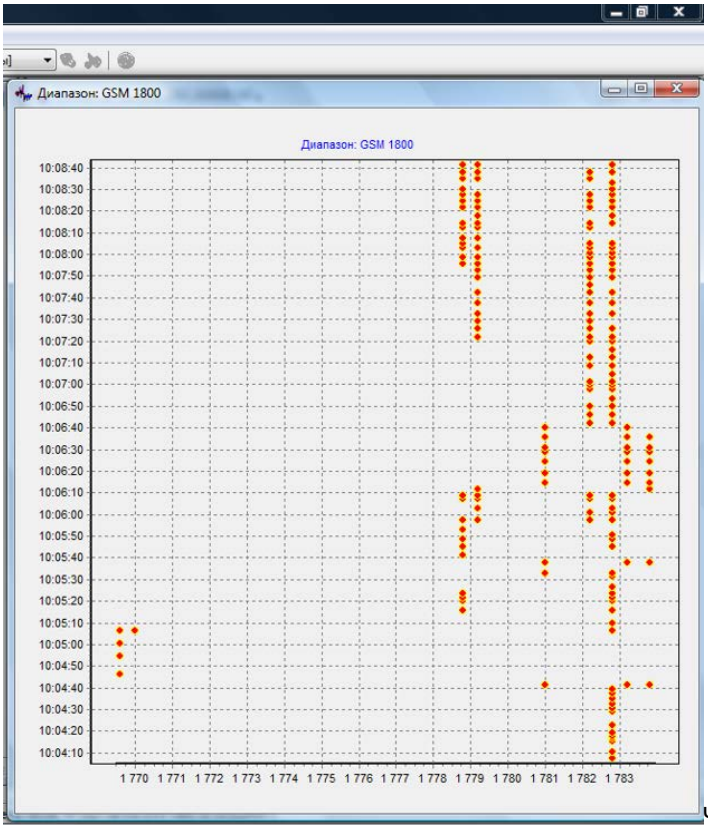


Рис.2. Типовая сонограмма радиоизлучений с БПРЧ мобильных телефонов стандарта GSM 1800, полученная автоматизированным комплексом радиомониторинга АКОР-3

Сонограмма такой передачи приведена на рис. 3.

Изложенная классификация радиоизлучений может быть использована как научно-методологическая основа при создании новых и модернизации существующих систем и устройств радиомониторинга.

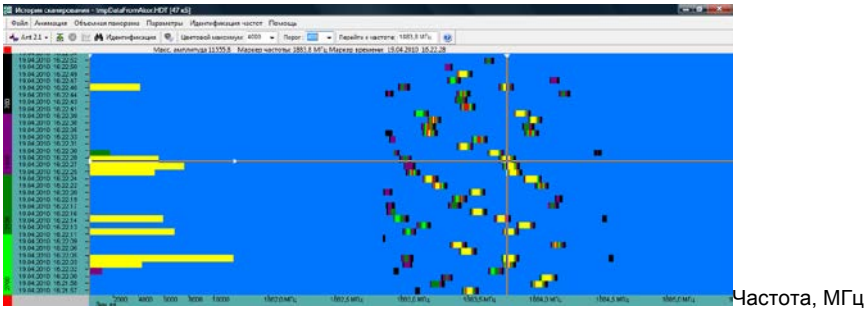


Рис.3. Типовая сонограмма радиоизлучений с ППРЧ на примере системы Dect, полученная автоматизированным комплексом радиомониторинга АКОР-3

УДК 681.3:519.62:519.711

ЗАХИСТ ІНФОРМАЦІЇ В ГРАФІЧНИХ ФАЙЛАХ ІЗ ВИКОРИСТАННЯМ МАТЕМАТИЧНОЇ МОДЕЛІ НЕЛІНІЙНОЇ СТОХАСТИЧНОЇ ДИФЕРЕНЦІЙНОЇ СИСТЕМИ

Автори: *С.Б. Приходько, д.т.н.; В.Г. Безрукавий, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Зараз, окрім використання добре відомих криптографічних алгоритмів, для захисту мультимедійної інформації втому числі для захисту інформації в графічних файлах спостерігається пошук нових рішень, до яких можна віднести застосування динамічних хаотичних систем та стохастичних диференціальних систем [1, 2]. У динамічних хаотичних систем є ряд негативних властивостей: існування непередбачено коротких довжин орбіт, чутливість до невеликих змін параметрів і початкових умов, що у криптографії неприпустимо. Стохастичні диференціальні системи (СДС) – такі системи, поведінка яких описується стохастичними диференціальними рівняннями (СДР) – у меншій степені чутливі до таких змін. Тому слушним є використати СДС для захисту мовних сигналів.

В [1] було запропоновано новий підхід до захисту мовних сигналів на основі нелінійних СДС. В [1, 2] були наведені можливі варіанти

реалізації цього підходу до захисту аудіо файлів на основі математичної моделі нелінійної СДС – це нелінійного СДР з кубічною нелінійністю у відновлюючий частині. Використання нелінійності більш високого порядку може покращити ступень захисту. Тому актуальним є удосконалення математичних моделей СДС – нелінійних СДР для захисту інформації в графічних файлах.

В роботі удосконалено математичну модель нелінійної СДС за рахунок використання в СДР нелінійностей 3-го та 5-го порядків, що дає змогу покращити ступень захисту інформації в графічних файлах. Наведено приклади захисту графічних даних в BMP файлах.

Список літератури:

1. Приходько С.Б. Використання нелінійних стохастичних диференціальних систем для захисту мовних сигналів / С. Б. Приходько // Системи обробки інформації. – 2010. – Вип. 3 (84). – С.75-76. – ISSN 1681-7710.

2. Prykhodko S. Application of nonlinear stochastic differential systems for data protection in audio files / S. Prykhodko, K. Basin // 11th International Conference Modern Problems of Radio Engineering, Telecommunications and Computer Science TCSET'2012 21-24 February 2012, Lviv-Slavske, Ukraine. – Lviv Polytechnic National University, 2012. – P.425. – ISBN: 978-1-4673-0283-8

УДК 681.3:519.62:519.711

ЗАХИСТ ІНФОРМАЦІЇ В АУДІО ФАЙЛАХ ІЗ ВИКОРИСТАННЯМ МАТЕМАТИЧНОЇ МОДЕЛІ НЕЛІНІЙНОЇ СТОХАСТИЧНОЇ ДИФЕРЕНЦІЙНОЇ СИСТЕМИ

Автори: *С.Б. Приходько, д.т.н.; М.Ю. Бойченко, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Зараз, окрім використання добре відомих криптографічних алгоритмів, для захисту інформації в аудіо файлах спостерігається пошук нових рішень, до яких можна віднести застосування динамічних хаотичних систем та стохастичних диференціальних систем [1, 2]. У динамічних хаотичних систем є ряд негативних властивостей: існування непередбачено коротких довжин орбіт, чутливість до невеликих змін параметрів і початкових умов, що у криптографії неприпустимо. Сто-

хастичні диференціальні системи (СДС) – такі системи, поведінка яких описується стохастичними диференціальними рівняннями (СДР) – у меншій степені чутливі до таких змін. Тому слушним є використати СДС для захисту мовних сигналів.

В [1] було запропоновано новий підхід до захисту мовних сигналів на основі нелінійних СДС. В [1, 2] були наведені можливі варіанти реалізації цього підходу до захисту мовних сигналів в аудіо файлах на основі математичної моделі нелінійної СДС – це нелінійного СДР з кубічною нелінійністю у відновлюючий частині. Використання нелінійності більш високого порядку може покращити ступень захисту. Тому актуальним є удосконалення математичних моделей СДС – нелінійних СДР для захисту інформації в аудіо файлах.

В роботі удосконалено математичну модель нелінійної СДС за рахунок використання в СДР нелінійностей 3-го та 5-го порядків, що дає змогу покращити ступень захисту інформації в аудіо файлах. Наведено приклади захисту аудіо даних в WAV файлах, а також їх сонограми до та після захисту.

Список літератури:

1. Приходько С.Б. Використання нелінійних стохастичних диференціальних систем для захисту мовних сигналів / С. Б. Приходько // Системи обробки інформації. – 2010. – Вип. 3 (84). – С.75-76. – ISSN 1681-7710.

2. Prykhodko S. Application of nonlinear stochastic differential systems for data protection in audio files / S. Prykhodko, K. Basin // 11th International Conference Modern Problems of Radio Engineering, Telecommunications and Computer Science TCSET'2012 21-24 February 2012, Lviv-Slavske, Ukraine. – Lviv Polytechnic National University, 2012. – P.425. – ISBN: 978-1-4673-0283-8

УДК 681.3:519.62:519.711

УДОСКОНАЛЕННЯ МАТЕМАТИЧНОЇ МОДЕЛІ ДЛЯ СТВОРЕННЯ ПОСЛІДОВНИХ ВИПАДКОВИХ ЧИСЕЛ З РІВНОМІРНИМ РОЗПОДІЛОМ

Автори: *С.Б. Приходько, д.т.н.; В.В. Решетняк, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

В галузі техніки захисту інформації існують засоби, в яких потрібно використовувати випадкові числа (ВЧ) з рівномірним законом розподілу. Зараз ВЧ отримують фізичним способом за допомогою відповідних апаратних датчиків (АД), наприклад, шумових діодів. Але використання АД супроводжується певними труднощами, які обумовлені сильною залежності статистичних властивостей послідовності ВЧ, що сгенерована, від зовнішніх факторів. Наприклад, для АД, які побудовані на основі теплових шумів пів провідникових приладів, суттєвими є таки фактори, як температура оточуючого середовища і напруга зовнішнього джерела живлення. Все це приводе до певних проблем при створенні ВЧ з рівномірним розподілом [1]. Помилки оцифровки є завжди, з іншого боку шум сильно залежить від фізичного пристрою аудіо карти [2], тому потрібно корегувати параметри. В роботи [1] пропонується підхід суть якого полягає у наступному. За АД отримують послідовність значень випадкової величини з довільним розподілом, за якою знаходять перетворення Джонсона певної сім'ї. Далі за знайденим перетворенням Джонсона значення випадкової величини з довільним розподілом перетворюють у значення гаусівської випадкової величини, за якими потім отримують ВЧ з рівномірним законом розподілу використовуючи зворотне перетворення Джонсона із сім'ї S_B [1]. Тому виникає необхідність в удосконалені математичної моделі, яка дозволить отримати послідовність ВЧ заданим розподілом, зокрема, рівномірним. Ціль даної роботи полягає у тому, щоб удосконалити запропоновану модель для формування ВЧ з рівномірним розподілом за значеннями випадкової величини з довільним розподілом для аудіо карти Realtek ALC269. В роботі була удосконалена математична модель, для звукової карти Realtek ALC269, показало працездатність даної математичної моделі.

Список літератури:

1. Приходько С.Б. Використання перетворення Джонсона для отримання випадкових чисел з рівномірним розподілом за значеннями випадкової величини з довільним розподілом [Текст] / С.Б. Приходько // Системи обробки інформації. – 2012. – Вип. 4 (102), Т.2. – С.128-130.
2. Випадкові числа з звукової карти [Електронний ресурс] / – Режим доступу: http://habrahabr.ru/post/62237/1

УДК 004: 519.2: 519:6

УДОСКОНАЛЕННЯ МАТЕМАТИЧНОЇ МОДЕЛІ ДЛЯ ГЕНЕРАЦІЇ ЗНАЧЕНЬ ГАУСІВСЬКОЇ ВИПАДКОВОЇ ВЕЛИЧИНИ НА БАЗІ ПЕРЕТВОРЕННЯ ДЖОНСОНА ІЗ СІМ'Ї S_U

Автори: *С.Б. Приходько, д.т.н.; Ю.О. Яблуновська, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

На сьогодні існує спосіб побудови криптографічних систем, що базується на використанні значень випадкової величини з нерівномірним розподілом, в тому числі, нормальним [1]. Але для ефективної роботи даної системи шифрування необхідно застосовувати високошвидкісний генератор випадкових чисел з розподілом відмінним від рівномірного, який має досить високу стійкість до криптографічних атак. Для реалізації такого генератора пропонується використати нормалізуюче перетворення Джонсона. В роботі [2] було застосоване перетворення Джонсона із сім'ї S_B. При його використанні, на відміну від інших перетворень, наприклад, Бокса-Мюллера, для створення одного значення гаусівської випадкової величини необхідне лише одне значення випадкової величини з рівномірним розподілом. Але при цьому значення випадкової величини можна моделювати лише на інтервалі $\pm 2\sigma_z$, де σ_z –середньоквадратичне відхилення випадкової величини z. З метою розширення даного інтервалу в роботі [3] було запропоновано використати нормалізуюче перетворення Джонсона із сім'ї S_U, що дозволяє отримати значення на інтервалі $\pm 3.1\sigma_z$. Щоб покращити результати моделювання на границях розподілу, необхідно удосконалити математичну модель для генерування значень випадкової величини на базі нормалізуючого перетворення Джон-

сона з сім'ї S_U. Це відповідно підвищить і якість криптографічної системи. В роботі була удосконалена математична модель, яка дозволяє покращити генерування значень на хвостах розподілу за рахунок розширення вищезазначеного інтервалу.

Список літератури:

1. **Михерский, Р.М.** Шифр на основеслучайных чисел с неравномерным распределением [Текст] / Р. М. Михерский // Проблеми програмування. – 2011. – №4. – С.90-94. – ISSN 1727-4907.

2. **Приходько, С.Б.** Моделювання гаусівських випадкових величин на основі перетворення Джонсона із сім'ї S_B [Текст] / С. Б. Приходько // Інформатика та математичні методи в моделюванні. – 2012. – т.2, №1. – С.64-69.

3. **Приходько, С.Б.** Генерування випадкових чисел з розподілом Гауса на основі перетворення Джонсона із сім'ї S_U [Електронний ресурс] / С. Б. Приходько – Електронне видання "Вісник Національного університету кораблебудування". – Миколаїв: НУК, 2013. – №4. – Режим доступу: http://evn.nuos.edu.ua/article/download/28205/25142

СИСТЕМА РАДІОЧАСТОТНОЇ ІДЕНТИФІКАЦІЇ ПО WI-FI

Автори: *Л.О. Ракутіна, студентка; С.Л. Трибулькевич, викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Постановка проблеми. Автентифікація персоналу та відстеження пересування працівників у межах підприємства є доволі важливим питанням для різноманітних об'єктів, так як оперативність та однозначність виконання цих завдань є запорукою спрощення та одночасно зміцнення системи контролю та управління доступом. Цілісність, конфіденційність та безпека циркулюючої всередині інформації може бути порушена при потраплянні зловмисника на територію підприємства, або, навіть, співробітника в заборонені для нього зони. Однією з найбільш популярних технологій, що реалізує задачу безконтактної ідентифікації об'єктів, автентифікації осіб, управління доступом, є радіочастотна ідентифікація *RFID* (*radio frequency identification*).

Актуальність роботи визначається популярністю використання бездротових технологій інформаційного обміну, зокрема *RFID*, у задачах кон-

тролю та управління доступом і широким використанням пристроїв на базі різних ОС мобільних пристроїв, за допомогою яких можлива біометрична автентифікація при наявності необхідного програмного забезпечення.

Метою дослідження є побудова RFID-системи дальнього радіусу дії біометричної автентифікації персоналу за допомогою пристроїв на базі різних ОС мобільних пристроїв.

Для досягнення поставленої мети висунуті наступні **задачі:**

– розглянути технологію *RFID*, зокрема в мікрохвильовому діапазоні;

– встановити технічні особливості та створити програмне забезпечення для компонентів *RFID*-системи;

– реалізувати біометричну ідентифікацію;

– забезпечити захищений алгоритм ідентифікації;

– виключити можливість підробки ідентифікуючого пристрою та проникнення зловмисника в контрольовану зону.

У якості ***об'єкту дослідження*** обрано систему контролю та управління доступом з використанням радіочастотної ідентифікації та біометричної автентифікації. ***Предметом дослідження*** виступає програмно-апаратна реалізація радіочастотної ідентифікації та біометричної автентифікації. ***Метод дослідження*** являє собою науковий експеримент.

Наукова новизна отриманих результатів полягає у об'єднанні радіочастотної ідентифікації та біометричної автентифікації.

Практичне значення отриманих результатів визначається використанням описаної системи в системах контролю та управління доступом.

Висновки: основною ідеєю даного наукового експерименту є об'єднання радіочастотної ідентифікації та біометричної автентифікації, програмно-апаратна реалізація цієї системи та її впровадження в систему контролю та управління доступом. Створення та використання такої системи дозволить значно підвищити рівень захищеності інформації, циркулюючої на об'єкті використання, зменшити ймовірність несанкціонованого проникнення зловмисника на об'єкт та контролювати переміщення працівників на робочому місці.

УДК 003.26.09 : 004.056.55

ВПЛИВ ТИПУ БРАУЗЕРА НА HTML КОД СТОРІНКИ

Автор: *Д.М. Самойленко, к.ф.-м.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв / Збройні Сили України*

З метою розвинення засобів перевірки цілісності клієнтського коду мережного інформаційного ресурсу (МІР) необхідно провести дослідження щодо потенційного спотворення HTML коду різними браузерами.

Усі браузери одержують однаковий текстовий документ з HTML кодом, оскільки він передається сервером від одного джерела. Однак, перевірка HTML коду на цілісність, очевидно, буде здійснюватись активними клієнтськими скриптами після завантаження сторінки та її оброблення браузером.

З метою перевірки впливу браузера на вихідні коди було проведено випробування для однакових HTML документів та різних, найбільш популярних браузерів. Зміст активної частини полягав у запиті внутрішнього коду для статичних об'єктів (innerHTML) або тіла об'єкту виклику (arguments.callee) – для функцій. Результати випробувань, що ілюструють відзначений вплив для різних браузерів, зведені у табл. 1. У першому стовпчику таблиці відзначено назви та версії браузерів, у другому – статистика їх використання українськими користувачами, у третьому – ASCII код (коди), які відповідали символу розриву рядка у початковому HTML документі. У четвертому стовпчику наведено результат відображення внутрішнього тегу розриву рядка (через innerHTML), який у вихідному документі задавався як
. Окремо слід відзначити, що браузер K-Meleon суттєво змінив форматування тіла функції, додавши пробіли та розриви рядків, відсутні у вихідному документі.

Як видно з табл. 1, відмінності у оброблені вихідного коду наявні і відрізняються для різних браузерів. Відповідно, контроль цілісності через аналіз HTML коду елементів документу вимагає урахування специфіки конкретного браузера, що значно ускладнює його програмну реалізацію.

Інша можливість контролю цілісності клієнтського коду може бути запропонована з огляду на принципи, закладені у об'єктно-орієнтовану модель документа (DOM – document object model). У відповідності до DOM, виконання HTML коду браузером супроводжу-

ється побудовою об'єктного «документа». Наявність стандартів для процесів створення документів, встановлених консорціумом W3C (World Wide Web Consortium), спонукає дослідити сталість сформованої для однакових HTML кодів DOM структури для різних браузерів та можливість її використання для контролю цілісності.

Для вирішення поставленої задачі було створено простий HTML документ, який складається з заголовку (HEAD) та тіла (BODY), а також містить функцію аналізу дочірніх елементів об'єкта головного елементу DOM як скриптову функцію:

```
var c=document.documentElement.childNodes,d,str="";
for(var i=0;i<c.length;i++)
{d=c[i]; str+="["+i+"]: "+d.tagName; str+=" "+d.nodeName;}
alert(str);
```

Результати виконання наведеного вище коду на різних браузерах включено до табл. 1.

Табл. 1 – Вплив різних браузерів на однаковий вихідний HTML код

Браузер та версія	Рейтинг, %	Розрив рядка	Тег 	DOM структура
Google Chrome 36.0.1985.125 m	30.90	#10	 	[0]: HEAD HEAD [1]: undefined #text [2]: BODY BODY
Opera 12.14	29.97	#10	 	
Mozila Firefox 20.0	27.17	#10	 	
Yandex 1.5.1106.241	0.93	#10	 	
Apple Safari 5.1.7	0.48	#32	 	
Maxthon 4.4.1.2000	0.24	#10	 	
CoolNovo 2.0.7.11	н/д	#10	 	
SeaMonkey 2.17	н/д	#10	 	
SRWare Iron 25.0.1400.0	н/д	#10	 	
IE 8.0.6001.18702	7.54	#13 #10	 	[0]: HEAD HEAD [1]: BODY BODY
K-Meleon 1.5.4	н/д	#32 *	 	

* з додаванням додаткових символів до тіла функції

Як видно з табл. 1, вплив браузера на початковий HTML код полягає у наступному: 1) Різні браузери по-різному сприймають символ

розриву (переведення) рядка. 2) Відбувається модифікація текстового вираження стандартних тегів. 3) В окремих випадках спостерігається зміна форматування. Аналіз структури DOM також не придатний для контролю цілісності клієнтської частини коду, оскільки кількість дочірніх елементів головного об'єкту різна у різних браузерах. Слід відзначити, що подібні відмінності у побудові об'єктної структури присутні не лише елементу document, а й більшості його нащадків.

Висвітлені відмінності вимагають додаткових досліджень для впровадження контролю цілісності клієнтського коду МІР.

Висновки. Досліджено особливості формування структури документа та внутрішніх HTML кодів елементів для різних браузерів, виявлено їх вплив на вихідні тексти. Показано недоцільність реалізовувати контроль цілісності за аналізом структури чи коду документа в цілому.

Список літератури:

1. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу. [Текст] / НД ТЗІ, затверджений наказом ДСТСЗІ СБ України від 02.04.2003 № 33.

2. Лучшие браузеры. рейтинг браузеров в Украине [Електронний ресурс]. – Режим доступу: www.rooom.com.ua/info-staty/39-raskrutka-seo-site/145-best-browsers-ukraina-statistika.html

3. Самойленко Д. М. Комплексна система захисту інформаційного ресурсу [Текст] / Самойленко Д. М. // Інформаційна безпека, 2013. – № 1 (9). с. 147-151 (ISSN 2224-9613)

УДК 004.056 : 004.031.4

РОЗПОДІЛ СЕКРЕТУ ПРИ ПЕРЕДАЧІ ІЗОД У МЕРЕЖНИХ РЕСУРСАХ

Автор: *Д.М. Самойленко, к.ф.-м.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв / Збройні Сили України*

При створенні та запуску мережного інформаційного ресурсу (МІР) часто виникає ситуація, коли власники сервера, як інформаційно-телекомунікаційної системи (ІТС) та МІР, як програмного продукту, розрізняються між собою. У такому разі природно можна очікува-

ти від них взаємного обмеження доступу до своєї матеріальної та інтелектуальної власності. Однак, інформаційна безпека МІР не дозволяє простого однозначного поділу: недостатня захищеність ІТС може погіршити функціонування МІР, так само, як і «дірки» у захисті МІР можуть надати зловмиснику можливість нелегального впливу на ІТС шляхом «зламу» захисної системи МІР.

Розділення відповідальності за захист інформації, очевидно, має віддзеркалювати поділ власності. З іншого боку, намагання відмовитись від сподівань на ідеальний захист ІТС (фільтрацію пакетів, стабільність файлової системи та серверу бази даних, тощо) має спонукати розробника МІР вживати заходів з покращення показників безпеки.

Потенційна вразливість файлової системи ІТС та системи управління базами даних (СУБД) має посилити вимогу заборони на використання незашифрованої ІзОД при міжсистемному обміні до повної відмови від її існування у МІР чи ІТС у відкритому вигляді.

У відповідності до правил побудови криптографічного захисту, відомих також як правила Керкгофса, його головна надійність має забезпечуватись паролем. Оскільки пароль має бути відомим лише легальному користувачу, необхідне забезпечення умов, за яких актуалізація ІзОД можлива лише за його безпосередньої участі.

У архітектурі серверної частини пропонується виділяти три шари. Така кількість вбачається мінімально достатньою для логічного відокремлення задач узгодження сеансових ключів, перевірки автентифікаційних даних користувача та отримання доступу до БД, що зберігає ІзОД.

Сеансові ключі змінюються при кожному обміні між користувачем і МІР та забезпечують через шифрування непередбачувану трансформацію даних, що передаються. Задача узгодження сеансових ключів покладається на окремий архітектурний шар.

Перевірка автентифікаційних даних також вимагає відокремлення окремого шару, оскільки має оперувати з власною базою даних, доступ до якої з інших шарів має бути заборонений.

З схожих міркувань задача забезпечення доступу до ІзОД має вирішуватись окремим шаром з власною БД, недоступною для інших архітектурних елементів.

Як один з заходів покращення контролю цілісності можна запропонувати розподіл загального секрету (пароля) на декілька частин, що зберігаються у різних складових елементах (вузлах) МІР. При цьому доступ до ІзОД має додатково обмежуватись контролем відновлення повного секрету.

Висновки.

Запропоновано реалізовувати заходи з розподілу загального секрету доступу до ІзОД на окремі частини. У архітектурі серверної частини пропонується виділяти щонайменше три шари.

Список літератури:

1. Про захист інформації в інформаційно-телекомунікаційних системах: закон України від 05.07.1994 № 80/94-вр [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

2. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB – сторінки від несанкціонованого доступу. [Текст] / НД ТЗІ, затверджений наказом ДСТСЗІ СБ України від 02.04.2003 № 33.

3. Singapore: Institute for Mathematical Sciences. – 2001. – 36 p. Режим доступу: www2.ims.nus.edu.sg/Programs/coding/files/dypei.ps

4. Самойленко Д. М. Комплексна система захисту інформаційного ресурсу Інформаційна безпека, 2013. – № 1 (9). с. 147-151 (ISSN 2224-9613)

5. ISO/IEC 7498-2:1989(E) Information technology – Open Systems Interconnection – Basic Reference Model: Security Architecture. [Text] / International Organization for Standardization, 1989. First edition. / Switzerland: ISO/IEC Copyright Office. – 34 p.

ЗЧИТУВАЧ RFID СТАНДАРТА MIFARE 13,56 МГЦ З ETHERNET ІНТЕРФЕЙСОМ ДЛЯ СИСТЕМ БЕЗКОНТАКТНОЇ ІДЕНТИФІКАЦІЇ

Автори: *С.Л. Трибулькевич, викладач; В.О. Мигиль, студент; А.М. Куса, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Актуальність. Актуальність роботи обумовлена популярністю безконтактної ідентифікації стандарту Mifare 13,56 МГц та мережевої технології Ethernet і протоколів TCP/IP.

Метою даної роботи є розробка і виготовлення зчитувача RFID стандарту Mifare 13,56 МГц з Ethernet інтерфейсом для систем безконтактної ідентифікації..

Викладення основного матеріалу.

Радіочастотна ідентифікація (*radio frequency identification*, *RFID*) – спосіб автоматичної ідентифікації об'єктів, в якому за допомогою радіосигналів зчитуються або записуються дані, що зберігаються на *RFID*-мітках. Система *RFID* влаштована просто і складається з трьох складових:

– мітки (*tag*) *RFID* – пристрої, здатні зберігати і передавати дані.

– зчитувачі (*reader*) – прилади, які зчитують інформацію з міток і записують у них дані.

– облікова система – ПЗ, яке накопичує й аналізує отриману з міток інформацію і пов'язує всі елементи в єдину систему.

Актуальність використання технології RFID визначена її перевагими перед попередниками:

– не потрібен контакт або пряма видимість;

– мітки читаються швидко і точно через бруд, воду, пластмасу, деревину;

– пасивні мітки мають фактично необмежений термін експлуатації;

– мітки несуть велику кількість інформації і можуть бути інтелектуальні;

– мітки практично неможливо підробити.

У радіочастотної ідентифікації є і недоліки:

– працездатність мітки втрачається при частковому механічному пошкодженні;

– схильність до перешкод у вигляді електромагнітних полів;

– недовіра користувачів, можливості використання її для збору інформації про людей.

Mifare – це найпоширеніше, сімейство *RFID*-пристроїв з робочою частотою 13,56 МГц. Дальність зчитування: до 10 см. Криптозахищені.

Можливі застосування даного типу закладок:

– електронний контроль доступу;

– системи електронних платежів.

Структурна схема розроблюваного модуля представлена на рис.1.

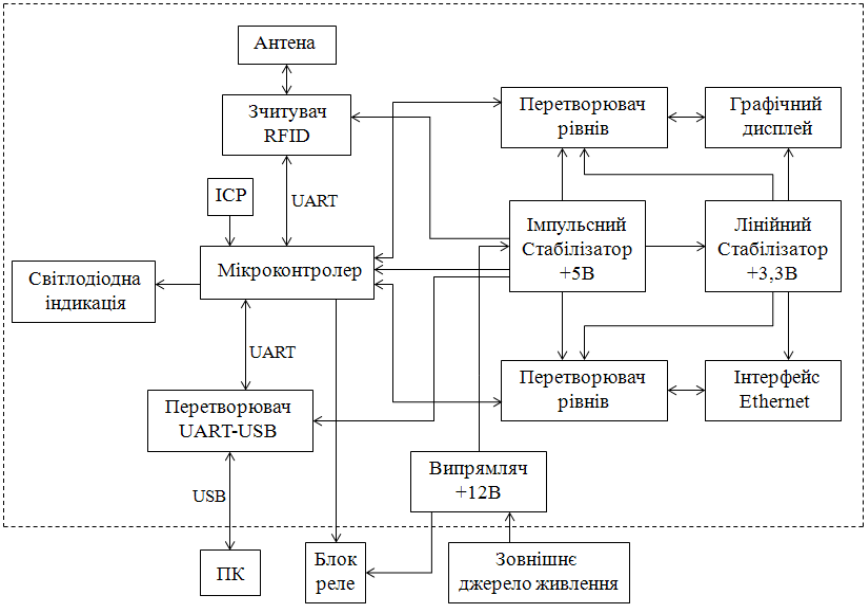


Рисунок 1 – Структурна схема модуля

Для обміну даними з ПК використовується перетворювач UART-USB.

Всі складові частини підключаються до мікроконтролера. Його призначення – керування схемою. інтерфейс Ethernet дозволяє передавати та отримувати дані через комп'ютерну мережу. Графічний дисплей та інтерфейс Ethernet підключаються через перетворювач рівнів, бо в них використовуються рівні напруги, що відрізняються від контролерних. Блок живлення складається з випрямляча напруги та імпульсного і лінійного стабілізаторів. Блок реле виконує механічну складову системи контролю доступу. ICP призначений для внутрисхемного програмування мікроконтролера.

На рисунках 2 – 4 зображені принципові схеми модуля.

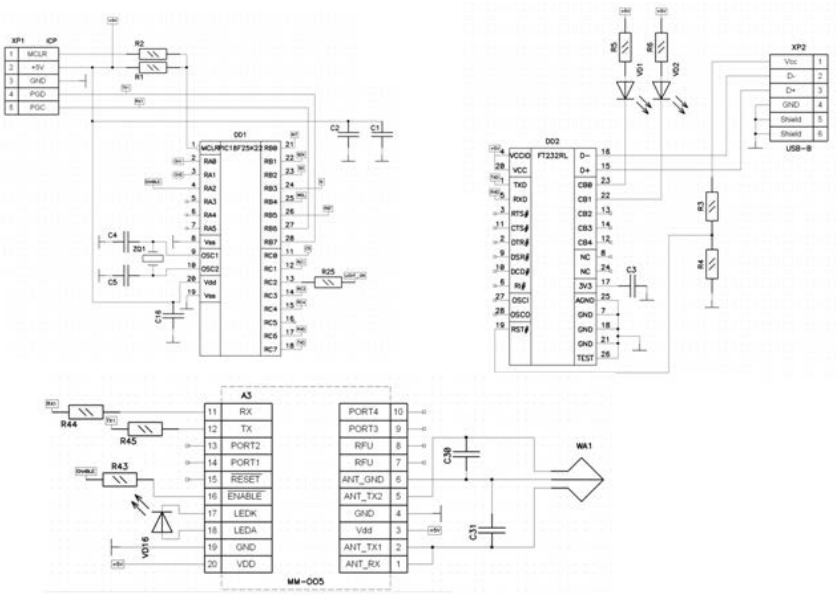


Рисунок 2 – Принципова схема мікроконтролерного блоку, перетворювача UART-USB та блоку зчитувача з антеною

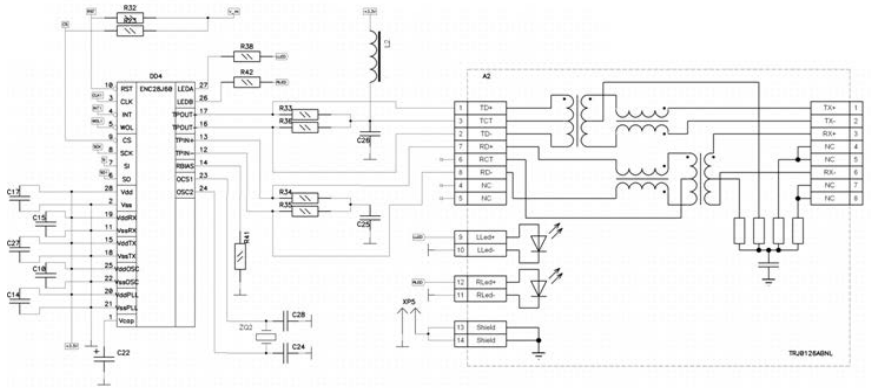


Рисунок 3 – Принципова схема інтерфейсу Ethernet

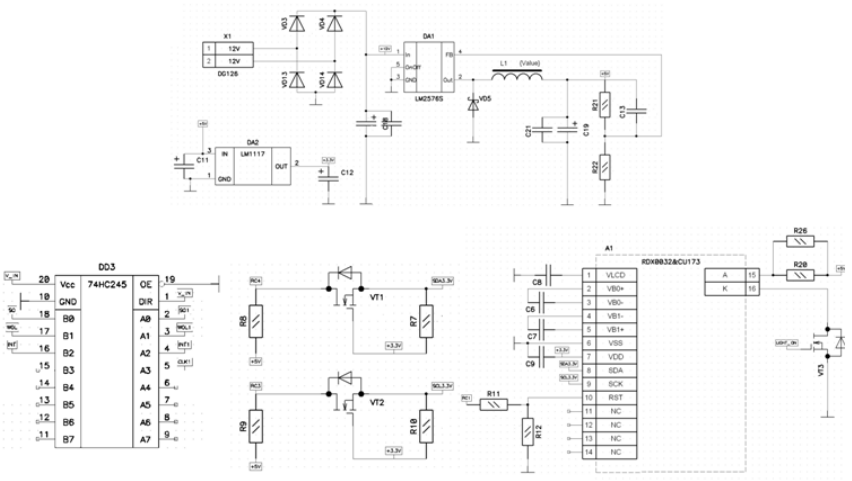


Рисунок 4 – Принципова схема джерела живлення, графічного дисплею та перетворювачів рівнів

Розроблені печатні плати зображені на рисунках 5,6.

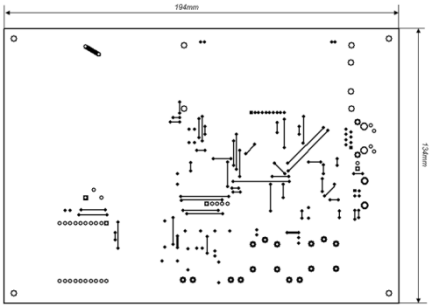


Рисунок 5 – Печатна плата (вид згори)

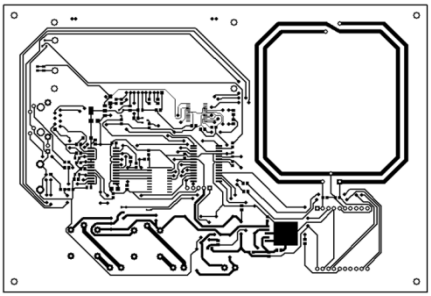


Рисунок 6 – Печатна плата (вид знизу)

Зовнішній вигляд вид згори (рис. 7) та знизу (рис.8).

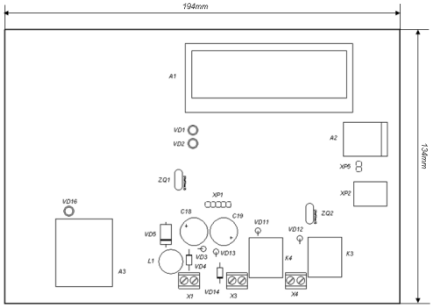


Рисунок 7 – Зовнішній вигляд (вид зверху)

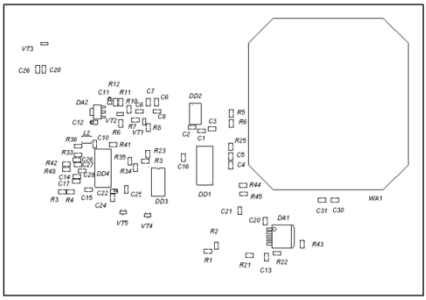


Рисунок 8 – Зовнішній вигляд (вид знизу)

Для підтвердження працездатності блоку зчитувача було розроблено і виготовлено макетну плату рис. 9.

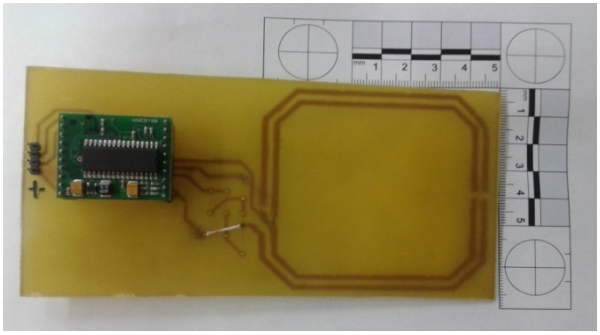


Рисунок 9 – Макетна плата

Було перевірено працездатність розробленого блоку у програмі netronix framer. При піднесенні мітки дані, отримані зчитувачем, передаються на ПК. Результати дослідів зображені на рисунку 10.

Було виготовлено печатну плату та під'єднано компоненти розроблюваного модуля. Зовнішній вигляд отриманого продукту зображено на рис.11.

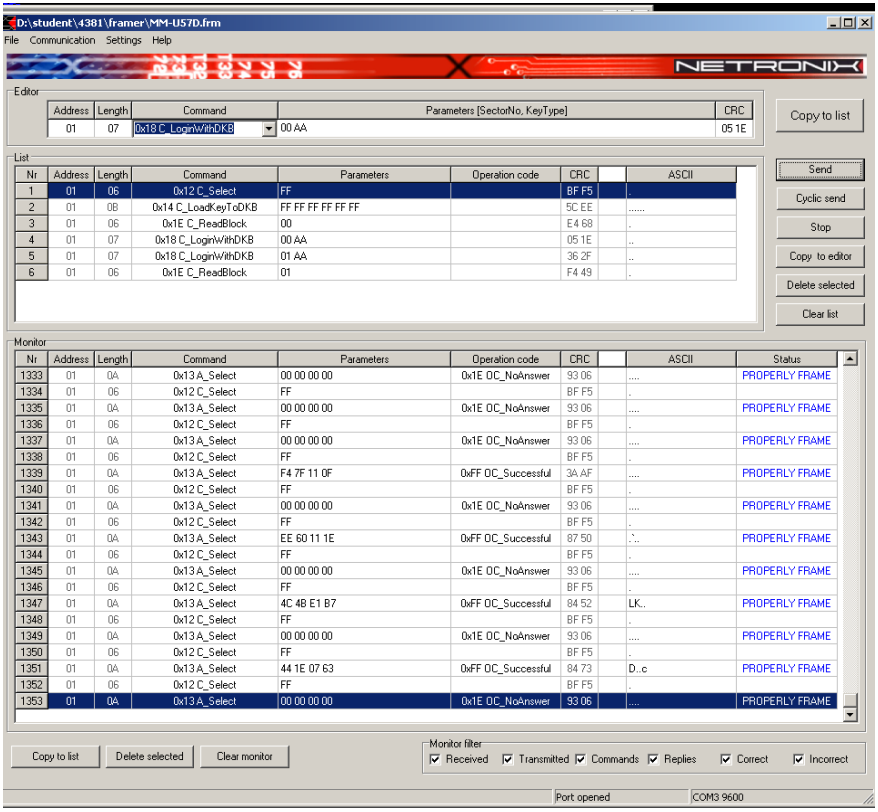


Рисунок 10 – Робота блоку зчитувача

Висновок: Виконано розробку та виготовлення модуля зчитувача RFID стандарту Mifare 13,56 МГц з інтерфейсом Ethernet.

Розроблено структурну та принципову схеми модуля зчитувача з графічним дисплеєм, світлодіодною індикацією, двома інтерфейсами: USB та Ethernet. Розроблено друковану плату та виготовлено сам модуль зчитувача.

Основне застосування розробленого пристрою – системи контролю доступу та термінали оплати.

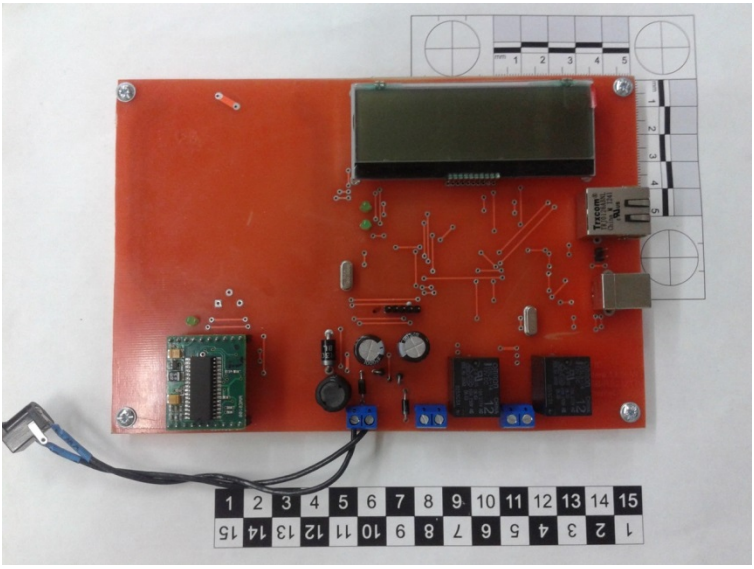


Рисунок 11 – Розроблений модуль зчитувача RFID

СЕКЦІЯ 3. ПРАВОВІ АСПЕКТИ ДІЯЛЬНОСТІ В ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

УДК 343.983

КРИМІНАЛІСТИЧНЕ ДОСЛІДЖЕННЯ НОВИХ ЗРАЗКІВ МИСЛИВСЬКОЇ НАРІЗНОЇ ЗБРОЇ ІНОЗЕМНОГО ВИРОБНИЦТВА

Автор: *С.А. Матвієнко, начальник сектору балістичної експертизи відділу криміналістичних експертиз, Науково-дослідний експертно-криміналістичний центр при Управління Міністерства внутрішніх справ України в Миколаївській області*

Розглянуто перелік фірм-виробників мисливської нарізної зброї та виокремлено конструктивні особливості рушниць та карабінів, що виготовляються. Розмежовано криміналістичний інтерес відносно рушниць та карабінів. Наведено стислий класифікаційний опис конструкції та ідентифікаційні особливості найпоширеніших мисливських нарізних карабінів.

Ключові слова: нарізна мисливська зброя; проблемні питання ідентифікації зброї; карабіни; сліди від деталей зброї; конструктивні особливості рушниць.

Окремі аспекти криміналістичного ідентифікаційного дослідження нарізної мисливської вогнепальної зброї знайшли своє відображення у роботах відомих криміналістів: Закутського Д.М., Філіппова В.В., Устінова О.І., Белкіна Р.С., Біленчука П.Д., Гусарова В.П., Горбачева І.В., Ермоленка Б.Н., Кофанова А.В. та ін. Проте роботи даних вчених стосувались екземплярів зброї вітчизняного виробництва, водночас, залишаючи питання дослідження нарізної мисливської вогнепальної зброї іноземних виробників відкритим.

Ми пропонуємо розглянути проблемні питання криміналістичного дослідження саме нарізної мисливської вогнепальної зброї іноземних виробників. Актуальність криміналістичного дослідження саме даного виду зброї зумовлена:

– великим розповсюдженням даного типу зброї, через надійність, якість, ергономічність та зовнішнє оздоблення, що приваблює власників;

– великою відстанню з якої можливо проводити прицільні постріли (до 1000 метрів і більше) через потужність патронів таких калібрів, як «.30-06 Spr» , «.300 WinMag», «.338 Winchester», «.416 Remington Magnum»;

– можливість використання збільшуваних оптичних приладів, що значно підвищує ефективність стрільби, і на великій відстані також;

– відсутністю достатньої кількості довідкової інформації, що могла б стати у нагоді при проведенні ідентифікаційних балістичних досліджень при розслідуванні кримінальних справ пов'язаних із застосуванням даного виду зброї.

Новітні технології та новаторські рішення, що використовуються під час конструювання та подальшого виготовлення сучасних зразків нарізної мисливської вогнепальної зброї іноземних виробників, які досі залишаються невідомими загальному колу експертів-практиків можуть призвести до численних помилок при проведенні діагностичних досліджень, використанні регіональних кулегільзотек НДЕКЦ УМВС, а подекуди і до помилкових висновків при проведенні ідентифікаційних досліджень.

Наприклад, снайперська гвинтівка «Blaser Tactical 2», виробництва Blaser Jagdwaffen GmbH, що перебуває на озброєнні військових формувань підрозділів поліції Німеччини, має свій аналог у вигляді мисливської гвинтівки «Blaser R 93 LR S». Калібр використовуваних патронів варіюється виробником: «.223 rem», «6 mm Norma BR», «6,5x55», «.308 win», «.300 WinMag», «.338 LM».

Рис. 1. Військова снайперська гвинтівка «Blaser Tactical 2»

Рис. 2. Мисливська гвинтівка «Blaser R 93 LR S»

Мисливська версія зброї відрізняється від бойового зразка лише відсутністю полум'ягасника та бази для кронштейнів кріплення оптичних прицілів [2].

Модель «Tikka T 3» однойменного виробника з Фінляндії містить у чашці затвору круглий виступ сигнального штифта, що сповіщає про наявність/відсутність патрону у патроннику ствола зброї. Внаслідок проведення пострілу та подальшої екстракції стріляної гільзи, даний виступ одночасно виконує функцію відбивача, та залишає свої сліди на денці гільзи, які можуть бути помилково сприйняті за слідову інформацію від інших зразків зброї (рис. 3).

Рис. 3. Денце гільзи із позначенням сліду від виступу сигнального штифта

Проведення повноцінного криміналістичного дослідження сучасних зразків нарізної мисливської вогнепальної зброї іноземних виробників, не можливе без вивчення характеристик відповідних зразків боєприпасів, що використовуються для проведення пострілів з них.

До числа найпоширеніших патронів до мисливської нарізної зброї нових зразків належать набої наступних калібрів: «.22 lr»; «.22 wmr»; «.223 Remington»; «.30-06 Springfield»; «7,62х39 мм»; «.308 Winchester»; «8х57 JS»; «.338 Winchester».

Патрони сучасних видів споряджаються експансивними кулями, новітніми зразками метального заряду – кордітного та піроксилінового пороху. У таких випадках за рахунок збільшеної теплоти горіння можуть бути використані менші за об'ємом та кількістю заряди [3, 27].

З метою забезпечення повноцінного та ефективного функціонування регіональних кулегільзотек нарізної зброї, що перебуває у власності громадян та на об'єктах дозвільної системи (ОДС) МВС; діяльність яких регламентована вимогами Інструкції з організації функціонування криміналістичних обліків експертної служби МВС, затвердженої наказом МВС від 10.09.2009 № 390, та зареєстрованим в Міністерстві юстиції України 15.10.2009 за № 963/16979, існує необхідність створення окремих довідників-класифікаторів, що диференціювали б зброю, за точною назвою від виробника та відповідно до калібру.

Знов таки, відповідно до вимог п. 4.14 СОУ 78 – 41 – 002 – 97. Зброя спортивна та мисливська. Вимоги безпеки. Методи випробувань на безпеку: «…Зброя, яка виготовлена шляхом перероблення зі зброї військового призначення, повинна залишати на стріляних із неї кулях та гільзах сліди, придатні для визначення її моделі та виробника (криміналістичні мітки)» [4, 6].

Для успішного проходження сертифікації зброї вказаного типу, що виготовляється на теренах України, безумовно це є обов'язковим для виконання, проте на сконструйованій без попереднього використання ідей аналогів бойової зброї іноземних виробників, що коштує подекуди від декількох тисяч у.о., таких міток не знайти, що безумовно також ускладнює можливість проведення ідентифікаційних досліджень стріляних з них гільз та вистріляних куль.

Повне та узагальнююче наукове дослідження та висвітлення ідентифікаційних деталей у галузі криміналістичного дослідження сучасних зразків нарізної мисливської вогнепальної зброї іноземних виробників має на меті створити інформаційно-довідкову базу для подальшого використання у практичній діяльності органами Експертної служби МВС з метою забезпечення повноцінного функціонування балістичних обліків та при проведенні ідентифікаційних чи ситуаційних експертних досліджень.

Список літератури:

1. Біленчук П.Д., Кофанов А.В., Сулява О.Ф. Балістика: криміналістчине вогнестрільне зброєзнавство. Підручник / За редакцією проф.. П.Д. Біленчука. – К.: Міжнародна агенція «BeeZone», 2003. – 384 с.
2. Blaser R 92 [Електронний ресурс]. – Режим доступу: https://www.blaser.de
3. Бабак Ф.К. Индивидуальное стрелковое оружие / Бабак Ф.К. – Москва, Издательство «ПОЛИГОН», 2004 р. – 195 с.
4. Стандарт МВС України «СОУ 78 – 41 – 002 – 97». Зброя спортивна та мисливська. Вимоги безпеки. Методи випробувань на безпеку. – Київ: ДНДЕКЦ, 1997.
5. Гусаров В.П. Основные особенности криминалистической экспертизы охотничьих нарезных ружей / Гусаров В.П. – Москва: ВНИИСЭ, 1976. – с. 50.

ПРАВОВІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА МОРСЬКОМУ ТОРГОВЕЛЬНОМУ ТРАНСПОРТІ

Автор: *І.В. Підпала, юрисконсульт 1 категорії, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Безпека на морському торговельному транспорті є запорукою захищеності (збереження) людського здоров'я і життя, довкілля та майна на морі. Система управління безпекою судноплавства охоплює: захист людини – захист її життя, права щодо використання територіального моря, внутрішніх вод та інших водоймів загального користування для праці, відпочинку, спорту, використання водних ресурсів, у тому числі і для судноплавства; захист засобів інформаційних систем на судні, захист довкілля від негативного впливу судноплавства; судна – їх стан, умови плавання та перебування на них людини; водні шляхи – їх придатність до використання, умови плавання; берегові об'єкти – їх відповідність стандартам безпеки судноплавства, готовність і надійність. Нормативно-правова база забезпечення безпеки мореплавства в Україні взагалі регламентується Положенням про систему управління безпекою судноплавства на морському і річковому транспорті. Система безпеки являє собою – сукупність організаційної структури, діяльності та відповідних ресурсів і методів для формування, здійснення, аналізу і актуалізації державної політики в галузі безпеки на морсько-

му торговельному транспорті. Управління безпеки являє систему планомірних і цілеспрямованих заходів, у тому числі підготовку, прийняття та реалізацію на морському торговельному транспорті управлінських рішень, спрямованих на забезпечення безпеки судноплавства. Управління повинно забезпечувати виявлення інформації та оцінку факторів, що впливають на рівень безпеки, включаючи фактори ризику, підготовку, прийняття та реалізацію управлінських рішень, спрямованих на забезпечення належного рівня безпеки. На судні управління безпекою здійснює безпосередньо капітан судна (судноводій), який володіє найбільшою інформаційною базою, в порту капітан порту.

Згідно зі ст. 75 КТМ для забезпечення безпеки мореплавства на морські порти покладається здійснення таких функцій: 1) забезпечення безпечного руху в портових водах, безпечної стоянки та обробки суден; 2) утримання у справному стані гідротехнічних споруд, засобів зв'язку та електрорадіонавігації, що перебувають у володінні порту та забезпечення дотримання інформаційних засобів і систем для уникнення ризиків; 3) утримання у справному стані засобів навігаційного устаткування на підхідних каналах і акваторії порту; 4) контроль і підтримання оголошених глибин; 5) визначення районів обов'язкового використання буксирів; 6) забезпечення виконання вимог чинного законодавства України щодо охорони навколишнього природного середовища; 7) подання допомоги потерпілим; 8) вжиття ефективних заходів для прийняття з суден забруднених і стічних вод.

Згідно Положення про систему управління безпекою судноплавства на морському і річковому транспорті визначено вимоги безпеки судноплавства до людського життя, інформаційного захисту, матеріальних цінностей, вантажу та ін. Ці вимоги, встановлені чинним законодавством України (включаючи міжнародні договори), виконання яких на морському торговельному транспорті дозволяє йому функціонувати без надмірного ризику для життя і здоров'я людей, довкілля і схоронності майна. Всі перелічені функції мають спільну мету та залежно від об'єкта спрямування розподіляються на групи. Спільною метою функцій є забезпечення виконання вимог чинного законодавства України щодо безпеки на морському торговельному транспорті.

Для забезпечення правових процесів можна зазначити групи функцій: 1) технічно-технологічні функції – це функції, пов'язані з дотриманням законодавства щодо інформаційних та техніко-технологічних процесів під час організації та здійснення морської діяльності: а) забезпечення безпечного руху у водяних просторах; б) забезпечення безпечної стоянки та обробки суден; в) утримання у справному стані гідротехнічних споруд, інформаційних систем, засобів зв'язку і електрорадіонавігації; г) утримання у справному стані засобів навігаційного устаткування на підхідних каналах і акваторій; д) контроль і підтримання оголошених глибин; є) визначення районів обов'язкового використання буксирів; 2) функції щодо захисту людського життя і здоров'я – це функції, спрямовані на запобігання ризику життя і здоров'я людей: а) надання допомоги потерпілим; б) вжиття ефективних заходів для прийняття з суден забруднених і стічних вод; 3) функції щодо захисту довкілля – функції спрямовані на забезпечення охорони навколишнього природного середовища.

Головною метою системи управління безпекою судноплавства на морському торговельному транспорті є забезпечення безпечного функціонування морського транспорту і попередження аварійних подій. Для цього існують контрольно-наглядові органи на морському і річковому транспорті до, яких належать: Головна державна інспекція України з безпеки судноплавства (Держфлотінспекція України); Державне підприємство «Класифікаційне товариство Регістр судноплавства України», Державне підприємство «Агентство морської безпеки», Інспекції державного портового нагляду; Інспекція з питань підготовки та дипломування моряків та ін., які створенні для здійснення нагляду за безпекою. Основними завданнями цих установ є: – здійснення нагляду за безпекою судноплавства у морських і річкових портах, територіальному морі, внутрішніх водах, на внутрішніх водних шляхах, а також на суднах, що плавають під Державним Прапором України, інформаційних систем морських транспортних засобів; – контролювання додержання законодавства і міжнародних договорів України з безпеки судноплавства та здійснення заходів щодо запобігання забрудненню довкілля із суден; – здійснення заходів щодо імплементації міжнародних договорів України з питань безпеки судноплавства та запобігання забрудненню довкілля із суден.

Таким чином, забезпечення безпеки мореплавства визначається Кодексом торговельного мореплавства України, законами України, постановами КМУ, конвенціями, стандартами резолюціями та ін. нормативними актами. Усі ці законодавчі акти сприяють забезпеченню загальної безпеки на морському торговельному транспорті, а акти локальної дії регламентують безпосередньо специфіку виду безпеки: за життя людей на судні, водних шляхів, інформаційних систем та ін. і надають можливість спрогнозувати ситуації та передбачити ризики і уникнути перешкод. Тому захист інформаційної безпеки є найнеобхіднішим на морському торговельному транспорті, так як є запорукою безпеки людського життя на морі, водних шляхах та і від нападу піратів.

УДОСКОНАЛЕННЯ ПРОЦЕДУРИ ЗБОРУ ДОКАЗОВОЇ БАЗИ РОЗСЛІДУВАННЯ ЕКОЛОГІЧНИХ ЗЛОЧИНІВ ПРИ ЗАБРУДНЕННІ МОРСЬКОГО СЕРЕДОВИЩА ШКІДЛИВИМИ РЕЧОВИНАМИ

Автор: *О.В. Тимченко, експерт, Науково-дослідний експертно-криміналістичний центр при Управління Міністерства внутрішніх справ України в Миколаївській області*

Анотація: досліджено проблему формування доказової бази при розслідуванні екологічних злочинів пов'язаних з забрудненням морського середовища шкідливими речовинами в рамках проведення досудового розслідування. Визначено пошагову оптимальну процедуру (модель) дій, яку рекомендується використовувати слідчому, спеціалісту при проведенні огляду місця події, проваджені слідчих дій та призначенні судових експертиз.

Ключові слова: екологічних злочин, пошагова процедура, доказова база, модель дій.

Актуальність питання. Навколишнє природне середовище є умовою існування людини, джерелом економічного збагачення держави та духовного розвитку нації. Екологічна безпека в Україні закріплена на найвищому державному рівні – Ст. 16 Конституції України («Забезпечення екологічної безпеки і підтримання екологічної рівноваги на території України, подавання наслідків Чорнобильської катастрофи – катастрофи пленарного масштабу, збереження генофонду Українського народу є обов'язком дер-

жави») [1, с. 3]. Конвенція ООН з морського права, яка була ратифікована Україною в 1999 році, регламентує положення згідно з яких держави зобов'язані приймати закони і правила для запобігання забруднень, їх скорочення, а також збереження морського середовища від шкідливих речовин [2] (ст. 192). Так, під шкідливою розуміється будь-яка рідка речовина, яка потрапляючи у море здатна створити екологічну небезпеку морському середовищу [3]. Найбільш шкідливими речовинами є нафта та нафтопродукти. Так, значні розливи нафти порушують екологічну рівновагу морських систем на багато років, масово знищують популяцію риб, зменшують прибутки від курортного бізнесу, та насамперед, створюють загрозу для збереження морського середовища у майбутньому. Україна є морською державою, яка омивається Чорним та Азовським морем, через українські морські порти проходять судна, які перевозять різноманітні вантажі, у тому числі і шкідливі речовини. В цьому контексті виникає необхідність розроблення пошагової процедури збору доказової бази при розслідуванні екологічних злочинів в даній сфері з метою об'єктивного, повного, всебічного розгляду справи, притягнення винних до відповідальності та відшкодування збитків. Треба зазначити, що з прийняттям нового кримінального кодексу України з'явилось поняття екологічного злочину [4, с. 108-116]. Кожний рік в Україні здійснюється багата кількість злочинів та правопорушень проти довкілля, але співвідношення притягнених до відповідальності порушників приблизно дорівнює один к сотні. Це пов'язано передусім з величезною корупцією в екологічної сфері, підприємства-порушники «відкупаються» від відповідальності, або на їх діяльність «закривають очі». За даними Державної служби статистики України питома вага злочинів проти довкілля у загальній структурі злочинності в Україні за період 2006–2010 років становить 0,56 % [5, с. 4]. Злочинам в сфері забруднення морського середовища шкідливим речовинами притаманний високий ступень латентності (73%) [5, с. 4], а їх наслідки можуть бути катастрофічні, тому вони повинні бути розслідуванні самим ретельним чином.

Аналіз останніх досліджень.

Розслідування екологічних злочинів були присвячені праці багатьох вітчизняних та закордонних авторів: Карагодіна В.І., Іванової Л.А., Книженка С.О., Одерія О.В., Лаврищєва В.В., Ринкової О.В., Стасюка Л.Л., Лаврищенка В.В., Руденка М.В., Сибірної Р.І., Сибірного А.В., Рузметова С.А., Чугаєва В.А., Туровца Ю.М., Мельника О.В., Архіпова

О.М. та інших. Аналіз даних робіт вказує на те що вітчизняні та закордоні вчені досліджували питання методики розслідування екологічних злочинів як в загалі та і в конкретних випадках (забруднення атмосферного повітря, забруднення при проведенні робіт та ін.), криміналістичної характеристики екологічних злочинів, першочергового етапу розслідування екологічних злочинів та інші аспекти, але питання вдосконалення процедури розслідування екологічних злочинів, пов'язаних саме з забрудненням моря нафтою на даний час є не достатньо розробленим.

Мета статті є побудова пошагової міжгалузевої процедури досудового розслідування екологічних злочинів, пов'язаних з забрудненням морського середовища нафтою та іншими шкідливими речовинами, у межах акваторії морських портів.

Виклад основного матеріалу.

З метою повного, об'єктивного та всебічного збору доказової бази та розслідування екологічного злочину пропонується наступний алгоритм дій:

1. Фіксація місця події (фотографування, відеозйомка, складання план-схем місця події).
2. Моделювання (створення моделі місця події з вказівкою розташування об'єктів, факторів, які впливають на оцінку ситуації та встановлення винних).
3. Виявлення та вилучення слідів та речових доказів.
4. Упакування речових доказів та складання протоколу огляду місця події.
5. Проведення досудових слідчий дій (обшук, слідчий експеримент, виїмка та ін.).
6. Призначення судових експертиз.
7. Формування та аналіз єдиної системи зібраних доказів.

Першочерговою та невідкладною дією в формуванні доказової бази та розслідування кожного екологічного злочину є огляд місця події. Дана слідча дія потребує чіткого механізму та процедури дій всіх учасників огляду, лише їх чітка налагоджена співпраця дозволить виявити важливі обставини справи та докази. Доцільно, щоб учасники огляду місця події керувалися у своїй роботі визначеною схемою,

виконання якої забезпечувало б відповідну якість збору доказової бази. До кожної схеми повинен додаватися алгоритм дій по виявленню, фіксації та вилучення слідів та речових доказів, виходячи з конкретних випадків вчинення екологічних злочинів (наприклад, план дій при розливу нафти у в межах ВЕЗ при невідомому джерелі забруднення, виявлення забруднення нафтою в межах морського порту при відомому порушнику тощо). Дані алгоритми повині бути наукового обгрунтованими та постійно вдосконалюватися, з метою побудови ефективної пошагової моделі дій, яку в подальшому можливо було запроваджувати у всіх сферах діяльності в процесі розслідування екологічних злочинів. Перед початком огляду місця події слідчий повинен прийняти міри для надання допомоги потерпілим, виявленню причини та умови забруднення, а також попередити його поширення [6, с. 228]. Перед виїздом на огляд місця події слідчий проводить інструктаж між учасниками, розподіляючи обов'язки. Спеціаліст повинен звертати увагу слідчого на істотні обставини, які можуть виникнути при огляді місця (наприклад, як треба діяти, щоб не знищити сліди, яку ділянку місцевості доцільно оглянути в першу чергу та ін.).

Початком огляду місця події є чітка фіксація та орієнтування на місці події. Основним завданням фіксації є використання технічних засобів та прийомів фіксування обставин події та матеріальних об'єктів у тому стані, у якому вони залишилися, з метою ілюстрації та їх всебічного, повного та об'єктивного дослідження в процесі судового розгляду. В науковій літературі виділяють наступні засоби фіксації: графічний – плани, схеми, креслення, рисунки; предметний – вилучення предмета чи сліду, виготовлення зліпків і відбитків, наочно-образний – фотографування, відеозапис [7, с. 7]. Також, пропонується використання наступних видів фотозйомки: орієнтуюча, оглядова, вузлова, детальна, а також методів фотозйомки: панорамна, стереоскопічна, вимірювальна (масштабна, метрична), макроскопічна [7, с. 21]. При застосуванні орієнтуючої та обзорної фотозйомки рекомендується займати високі позиції (дахи будівель, вершина портового крана, з гелікоптера), щоб повністю охопити місця події та проілюструвати масштаб злочину; а також звертати увагу на фотографування назви, номерів, індивідуальних ознак судна тощо. При вузлової фотозйомки

потрібно охопити весь комплекс слідів, з їх взаємозв'язком. При детальної фотозйомки обов'язковим є використання при фотографуванні масштабної лінійки, з метою можливості вимірювання об'єкта по фотознімкам. Використання відеозйомки дозволяє в суді довести, що саме цей речовий доказ знаходився на місці події, наглядно прослідкувати напрямок та динаміку руху плями шкідливої речовин в морському середовищі (наприклад, при зйомки з гелікоптеру); подальшим переглядом відзнятого матеріалу можна виявити докази, які не були вилучені при огляді місця події. Коли виникають сумніви в правильності вилучення слідів, в якості проведеного огляду, відеозйомка дозволяє наглядно проаналізувати процес збору слідової інформації [8, с. 184]. Складання план-схем, як спосіб фіксацій місця події, дозволяє додатково (поряд з фотографуванням) відобразити обстановку події, матеріальні об'єкти, з зазначенням відстані до них, їх розмірів та співвідношення між ними. План-схеми можуть бути орієнтуючими, оглядовими, вузловими та детальними [8, с. 181].

Для всебічного аналізу ситуації й визначення ймовірного винуватця аварії необхідним є визначення динаміки зміни параметрів розливу шкідливих рідин на водній поверхні. Запропонована процедура збору доказової бази містить алгоритм моделювання та прогнозування [9]. Алгоритм, що використовується базується на імітаційній моделі динаміки забруднюючих речовин у водному середовищі за умови незначного впливу вітрових збурень та експертній системі визначення характеру розділу нафтового поля на окремі елементи (плями) і включає визначення концентрацій забруднюючих речовин в різні моменти часу, та координати. При цьому з деякою похибкою розрахунків можливим є визначення початкового місця розливу. Дані отриманні при моделюванні ситуації заносяться в відповідну базу даних. Для здійснення процесу моделювання необхідно залучати спеціалістів – екологів, його необхідно починати з оглядом місця події (якщо дозволяють обставин без шкоди для ефективності збору доказової бази). На рис. 1 наведено діалогове вікно програми моделювання та прогнозування параметрів розливів нафти для деяких сценаріїв розвитку ситуації:

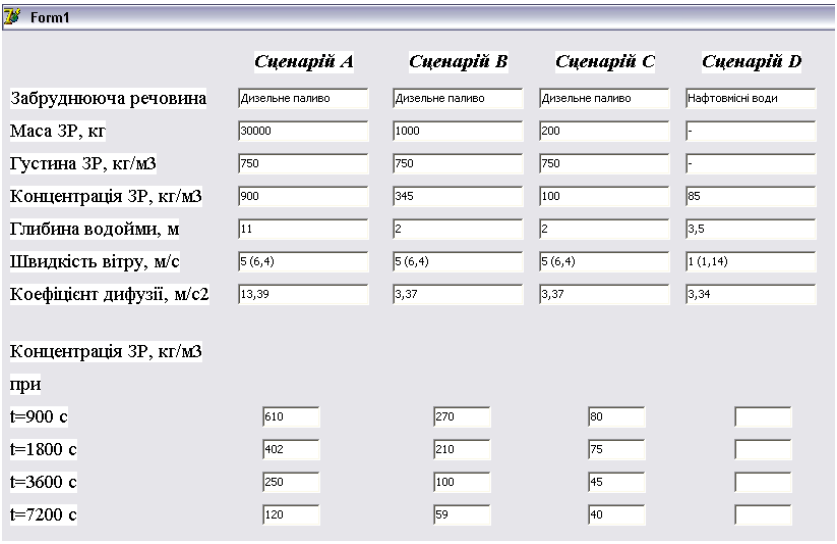


Рис. 1. Діалогове вікно даних моделювання

Доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому законодавством порядку, на підставі яких суд встановлює наявність чи відсутність фактів та обставин, що мають значення для судового провадження та підлягають доказуванню. [10, с. 50.]. Огляд в залежності від обставин та місця скоєння злочину доцільно проводити наступними способами: ексцентричний, концентричний, фронтальний [8, с. 176]. Важливе значення при здійсненні якісного збору доказів є планування даного процесу [8, с. 177]. Доцільним в даному випадку є створення плану дій для окремих випадків вчинення злочину. Цей план формується на основі алгоритм дій слідчого, спеціаліста, інших осіб задіяних в огляді місця події, починаючи з отримання сигналу та проведення огляду місця події, закінчуючи призначенням експертиз та підготовкою справи до суду. Будь-яка подія (аварія, вилив нафти, тощо) виникає, розвивається і закінчується в матеріальному середовищі. Як наслідок утворюються «сліди» цієї події, які в подальшому можливо використовувати для формування доказової інформації [7, с. 16]. Цінність слідів полягає в тому, що за ними встановлюється зв'язок об’єктів із подією, що розслідується [7, с. 17]. Сліди дозволяють вирішувати як ідентифікаційні так і діагностичні завдання, а саме: встановити індивідуальну тотожність об’єкта; групову належність об’єктів;

механізм та умови їх утворення; окремі обставини події, вміст шкідливих речовин та ін. При проведені огляду важливим моментом є те, що результативність огляду місця події знижуються прямо пропорційно моменту здійснення забруднення (тобто, з часом сліди втрачають свою інформативну значимості). Кожен пошук слідів та речових доказів – це процес моделювання дій порушників, вивчення обставин місця події, змін та завданої шкоди; на даній стадії ставляться відповідні пріоритети щодо попереднього дослідження об'єктів та виявлення слідів. В кожному конкретному випадку необхідно використовувати окремий підхід для виявлення та вилучення речових доказів. Так, наприклад, якщо події відбувались в межах порту необхідно вести пошук слідів взуття, об'єктів зі слідами рук чи ДНК, транспортних засобів, мікрочастинок, паливно-мастильних матеріалів, та інших слідоносіїв, з метою ідентифікації слідоутворюючих об'єктів (осіб-порушників, транспортного засобу тощо). Якщо подія відбулася у відкритому морі, особливу увагу приділяють вилученню проб з води, де можлива наявність шкідливої речовини, огляду судна на предмет залишків шкідливої речовини та ін. Так, в останньому випадку необхідно більш ретельно оглянути корпус судна, при цьому фіксуються нашарування та залишки шкідливих речовин, із зазначенням їх розташування (так, при фотографуванні детальним та вузловим знімком фіксуються розташування залишків речовини, колір та її розмір). Доцільним є графічна ілюстрація розміщення залишків речовини на план-схемах. Після фіксування залишки речовин вилучаються наступними способами: зі слідоносієм, на якому вони знаходяться (цей спосіб найбільш ефективний, адже він не вносить змін до об'єкту та збережує топографію розташування речовини на об'єкті), безпосереднє вилучення речовини з об'єкту [8, с. 154]. Завдяки новітнім досягненням на сьогоднішній день з'явилась можливість встановлення генетичних ознак епітеліальних клітин (ДНК-профілю) людини, що можуть знаходитись у потожирових слідах рук, які залишаються при безпосередньому контакті поверхні руки особи з об'єктом. Велике значення при якісному зборі доказової інформації відіграє виявлення та вилучення мікрооб'єктів. Так, мікрооб'єкти дозволяють отримати дані про одягу осіб-порушників, рід їх професійної діяльності, тощо. [11, с. 493-509]. В процесі пошуку слідів злочину пріоритетне значення необхідно приділяти тим слідам, які до-

казують причетність особи до злочину та встановлюють завдану шкоду (чи імовірну шкоду, яку вдалось попередити).

Заключною стадією в процесі виявлення та вилучення доказів при огляді місця події є пакування речових доказів та складання протоколу даної слідчої дії. Правильне упакування забезпечує збереження властивостей об'єктів, щоб вони могли бути джерелом доказу в подальшому. Всі об'єкти вилучаються з місця події у тому виді, у якому вони виявлені. Мокрі об'єкти просушуються. Дрібні предмети (наприклад недопалки) можливо упакувати в різні пенали, сірникові коробки тощо. Об'єкти необхідно упакувати таким чином, щоб по-перше унеможливити їх пошкодження або знищення, по-друге, щоб вони не втратили своїх властивостей, по-третє, щоб на об'єктах збереглися сліди злочину. При завершенні огляду складається протокол, у якому письмово фіксується обстановка місця події: вказується місце знаходження, вид об'єкта, який оглядається, і його індивідуалізуючі ознаки, а також записуються виявлені речові докази та сліди. Протокол огляду місця події підписується всіма учасниками, які беруть участь у огляді.

Наведений у даній статті перелік слідів, які можуть залишатись на місці події, не є вичерпним, він залежить від кожного окремого випадку. Крім того, для повного формування доказової інформації необхідно користуватися іншими джерелами доказів: поясненнями свідків, які дозволяють вирішити суперечності в показах сторін, перегляд камерспостережень, огляд документації судна та ін.

Проведення слідчих дій, які є доцільними у конкретних випадках (виїмка та огляд документів, допроси, обшуку та ін.), дозволяє встановити істотні обставини справи, доповнити доказовою базою розслідувану справу. Доцільним є розроблення планів, схем, моделей проведення окремих слідчий дій в конкретних випадках екологічних злочинів, з метою використання їх слідчими природоохраної прокуратури, спеціалістами тощо.

Після проведення відповідних судових експертиз (трасологічних, хімічних, біологічних, екологічних тощо) з вилучених в процесі огляду слідів формується доказова база з метою її використання в подальшому у суді. Судові експертизи дозволяють встановити місце, час, тривалість, інтенсивність та безпосередні причини забруднення, встановити причини гибелі риб, забруднення акваторій, склад шкідливої речовини, її концент-

рація, ототожнити особу порушника (дактилоскопічна та ДНК експертиза), ототожнити транспортний засіб (трасологічна експертиза), встановити фальсифікацію документів (експертиза почерку та технічне експертиза документів) та інші завдання. В кожному конкретному випадку необхідно призначати лише ті види експертиз, які доцільні та мають доказове значення, а не ті, які можуть «загромаджувати» справу «зайвими» експертизами, що лише затримують слідство, а їх проведення тягне додаткові матеріальні затрати. Якщо проведення одного виду експертизи виключає проведення іншого, то необхідно проводити ту експертизу, висновок якої містить більшу доказову значимість. Доцільно розробити рекомендації для слідчих природоохоронної прокуратури щодо питань, які експертизи в першу чергу необхідно призначати виходячи з конкретних випадків вчинення екологічних злочинів.

Проблемою в галузі правовідносин пов'язаних з забрудненням навколишнього середовища шкідливими речовинами вважається відсутність в експертних установах та наукових інститутах осіб, які спеціалізувались на проведенні оглядів місць події та збору доказової бази саме у цій сфері. В екологічних злочинах необхідна чітка співпраця між слідчим, який проводить огляд та розслідує даний злочин, та спеціалістом який допомагає йому в цьому. Для досягнення високих показників у цій сфері доцільно проводити спільні навчання даних працівників, проводити семінари, курси підвищення класифікації, наукові конференції, обмін досвідом з міжнародними колегами. Також, вважається за необхідно не тільки встановити суворіші санкції за скоєння екологічних злочинів, а й створити умови, щоб вони були невідворотними.

Висновки. Досягнення мети якісного збору доказів передусім пов'язано з їх науковим вивченням та дослідженням, впровадженням алгоритмів, інструкцій щодо дій осіб, які розслідують екологічні злочини, впровадження міжнародної практики, а також міжнародної співпраці в даній галузі. Саме якісний процес виявлення та вилучення доказів дозволить удосконалити вирішення спорів пов'язаних з забрудненням нафтою та іншими шкідливими речовинами. Пропонується використання наступного пошагового алгоритму дій: фіксація (фото та відеозйомка), моделювання, виявлення та вилучення слідів, упакування речових доказів, оформлення

протоколу огляду місця події, провадження слідчих дій, призначення судових експертиз, формування та аналіз єдиної системи зібраних доказів. Саме вдосконалення цих процедур для слідчих та спеціалістів, складання рекомендації та моделей щодо них, дозволить ефективно провести досудове розслідування та довести вину злочинців у судовому розгляді справи.

Список літератури:

1. Конституція України: станом на 28.06.1996 р. / Верховна Рада України. — Офіц. вид. – К.: Відомості верховної ради України від 23.07.2006/№30/1996. – 43, с.

2. Конвенція ООН з морського права від 1982 р/ [Електронний ресурс]\ – Режим доступу : URL : http://zakon4.rada.gov.ua/laws/show/995_057.

3. Міжнародна конвенція з запобігання забруднення з суден 1973 р. [Електронний ресурс]. – Режим доступу : http://www.conventions.coe.int

4. Кримінальний кодекс України: станом на 05.04.2001 / Верховна Рада України. — Офіц. вид. – Голос України від 19.06.2001 №107 – 203, с.

5. Туровець Ю.М. Початковий етап розслідування злочинів проти довкілля [текст] автореферат дис. канд. юрид. наук. : 12.00.9 / Туровець Ю.М.: Нац. акд. внутр. справ. – Київ., 2012. – С. 203.

6. Ипатова И.А. Криминалистика: Учебно-методический комплекс – . М.: ИЗД. центр ЕАОИ, 2008, – с. 558

7. Шевцов С.О. Науково-технічні засоби в експертній практиці : коцептуальні засади : Метод. Посіб. / М-во внутр. справ України; Держ. Наук.-дослід. Експерт-криміналіст. Центр. / Шевцов С.О., Перлін С.І. – Харьків : ФО-П Чальцев О.В., 2009. – 152, с.

8. Разумов Є.А. Практическое руководство по криминалистике : учеб.практ. пособ. / М-во внутр. справ України; Держ. Наук.-дослід. Експерт-криміналіст. Центр. / Разумов Є.А. – Київ : ТОВ «Еліт Прінт», 2009. – 465, с.

9. Ryzhkov, S.S.,Tymchenko I.V., Girzheva O.L. Simulation modeling of the dynamics of pollutant spreading in the sea of estuary channel // NUS Journal. – Mykolayiv, 2012. – №4. p.372-380.

10. Кримінальний процесуальний кодекс України: станом 19.05.2012 / Верховна Рада України. — Офіц. вид. – Голос України від 19.05.2012 №90 – 324, с.

11. Разумов Є.А. Осмотр места происшествия/ Є.А. Разумов, Н.П. Молибога. – К., 1994 –672, с.

ИНФОРМАЦИОННЫЙ АНАЛИЗ ПРАВОВОГО МЕХАНИЗМА СОЗДАНИЯ И ВОЗМОЖНОСТИ ФУНКЦИОНИРОВАНИЯ КОММУНАЛЬНОГО ПАРОХОДСТВА В УКРАИНЕ

Авторы: *Э.Б. Хачатуров, к.т.н., с.н.с; Н.В. Мишутин, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев*

Коммунальное предприятие – в экономической науке – предприятие, обеспечивающее население водой, электроэнергией, газам и другими товарами и услугами первой необходимости.

Коммунальные предприятия являются естественными монополистами и их деятельность регулируется правительством во избежание злоупотреблений монопольной властью.

С точки зрения юридической следует рассматривать факт не «коммунального» пароходства, а «государственного коммунального предприятия».

Понятие государственного унитарного предприятия:

государственное унитарное предприятие создается компетентным органом государственной власти в распорядительном порядке на базе отделенной части государственной собственности, как правило, без деления ее на частицы, и входит в сферу его управления;

орган государственной власти, в сферу управления которого входит предприятие, есть представителем собственника и выполняет его функции в границах, определенных этим Кодексом и другими законодательными актами;

имущество государственного унитарного предприятия находится в государственной собственности и закрепляется за таким предприятием на праве хозяйственного ведения или праве оперативного управления;

наименование государственного унитарного предприятия должно содержать слова "государственное предприятие";

государственное унитарное предприятие не несет ответственности за обязательствами собственника и органа власти, в сфере управления которого оно входит;

органом управления государственного унитарного предприятия есть руководитель предприятия, который назначается органом, в сфе-

ру управления которого входит предприятие, и есть подотчетным этому органу;

законом могут быть определены особенности статуса руководителя государственного унитарного предприятия, в том числе установлена повышенная ответственность руководителя за результаты работы предприятия;

государственные унитарные предприятия действуют как государственные коммерческие предприятия или казенные предприятия.

Одна из самых острых проблем для судоходных компаний страны –проблема обновления и строительства флота. Если раньше вопрос постройки новых судов решался централизованно, в масштабах другого государственного строя, то сейчас судоходным компаниям приходится действовать самостоятельно. К сожалению, экономика Украины не позволяет строить и обновлять флот быстро и качественно, поэтому он в основном состоит из старых, технически изношенных судов, и поддержание их в хорошем состоянии требует от судовладельцев значительных материальных затрат. А для Украины, как независимой страны, очень важно иметь свой современный флот, который укреплял бы ее имидж морской державы.

В мировой практике основными источниками финансирования строительства нового тоннажа являются собственные средства предприятия, а также различные займы в виде банковских кредитов и государственная поддержка в форме субсидий и предоставления различного вида льгот. К сожалению, действующее в Украине налоговое законодательство, одно из самых жестких среди постсоветских стран, не позволяет национальным судоходным компаниям накапливать значительные собственные средства для постройки нового флота. Поэтому единственный источник финансирования обновления тоннажа – кредиты банков.

Реальный путь возрождения флота (естественно, при наличии желания у государства) такой. На основе одной из ныне существующих компаний создается национальная судоходная компания, куда собирают остатки действующего флота. Там формируется нормальный работоспособный коллектив.

Компания сертифицируется в соответствии со всеми международными стандартами. В бюджете выделяется сумма для строительства судов. Прежде всего – на наших судоверфях. Определяются рынки, где они

будут работать. Таких рынков сегодня немного. Но они есть. Например, несколько миллионов тонн глинозема, импортируемого Украиной. Миллионы тонн экспортируемого металла, производимого нашими Криворожским, Днепропетровским и другими металлургическими комбинатами. Сейчас этот металл продается на условиях, когда украинская сторона почти не участвует в его перевозках. Но производители говорят нам, что уже устали от частных лавочек, от посредников, не обеспечивающих той стабильности и надежности в работе, которые могли бы обеспечить государство и национальная судоходная компания.

Статус национального перевозчика должен предоставляться судоходным компаниям на конкурсных началах решением специальной межправительственной комиссии, созданной при Министерстве транспорта Украины. Учитывая неопределенный статус понятия «госзаказ» для морских перевозок, нужно, чтобы Кабинет Министров утвердил номенклатурный перечень грузов (металл, химгрузы, удобрения, зерно и т.д.), на которые право «первой руки» или определенной квоты имел бы национальный перевозчик.

Для реализации права получения грузов национальным перевозчиком необходимо создание в Украине, в виде государственной (стопроцентно) акционерной компании, Украинской фрахтовой биржи, и через нее в обязательном порядке должна проходить регистрация всех запродажных контрактов на отправку экспортной продукции по утвержденной номенклатуре, а также всех чартеров или договоров на морские перевозки грузов указанной номенклатуры (по аналогии с тем, как отчуждение госимущества обязательно проводится через аукцион по действующим инструкциям Фонда госимущества). Об этом же речь идет и в многочисленных обращениях Ассоциации украинских судовладельцев.

Данные регистрации должны поступать в компьютерную сеть Государственной таможенной службы, она и будет осуществлять окончательный контроль за соблюдением прав национального перевозчика в портах Украины.

Безусловно, введение в действие такого механизма потребует изменений и дополнений в существующей законодательной базе Украины, поэтому уровень постановления Кабинета Министров для этого

недостаточен. Необходим закон о национальном морском перевозчике, где предусматривалось бы поручение Минтрансу подготовить проекты законодательных актов о внесении изменений и дополнений в другие законодательные акты Украины, вытекающие из принятия данного закона, а также поручение Кабинету Министров, министерствам и ведомствам создания подзаконных актов, нормативных и ведомственных документов, обеспечивающих работу института национального перевозчика и реализацию его прав.

Существующая сегодня в Украине система дифференцированного режима портовых сборов – «наибольшего благоприятствования» и «обычного», с точки зрения международного права, воспринимается мировым сообществом как практика дискредитации отдельных флагов.

В то же время дифференциация и распределение приоритетов в системе налогообложения является внутренним делом каждого государства. Для поддержки национального судовладельца, по моему мнению, государству необходимо выделить следующие приоритеты:

льготное налогообложение прибыли при перевозке грузов под украинским флагом в/из портов Украины;

снятие таможенных сборов с импорта судов, предназначенных для осуществления перевозок в режиме национального перевозчика, с немедленной реализацией этих сборов при смене флага либо при переходе к перевозкам грузов между иностранными портами;

освобождение от НДС импорта товаров, услуг и основных фондов для собственных нужд предприятий морского транспорта Украины, обусловленных необходимостью осуществления экспортных и транзитных перевозок;

освобождение от таможенных пошлин и налогов импорта комплектующих механизмов и машин, входящих в спецификацию судов, построенных на национальных верфях.

На основании вышеизложенного можно сделать заключение, что механизм функционирования «коммунального» или «коммунального унитарного» предприятия – пароходства, в основном зависит от следующих факторов:

– влияние и осуществление руководства предприятием местными органами власти или вновь организованными структурами при исполнительной власти на местном уровне;

– создание инфраструктуры предприятия – объединение в состав коммунального предприятия, помимо основного флота (пассажирского, грузового), вспомогательного флота (буксиры, заправщики, дноуглубительная техника, плавкраны…), ремонтных баз (доки, мастерские, плавмастерские…), мест базирования (причалы, акватории, водные и сухопутные подходы, складские помещения…);

– экономический и политический интерес государства в развитии судоходства.

Сегодня объем морских перевозок украинских экспортно-импортных грузов – значительный и имеет тенденцию к ежегодному увеличению. Сохранилась и мощная судоремонтно-судостроительная база в стране, есть квалифицированные морские кадры, которые ежегодно пополняются выпускниками солидных учебных заведений. Все это создает благоприятные условия для возрождения украинского торгового флота.

СЕКЦІЯ 4. ПІДГОТОВКА КАДРІВ У ГАЛУЗІ ЗНАНЬ «ІНФОРМАЦІЙНА БЕЗПЕКА»

ДЕЯКІ ПИТАННЯ ВДОСКОНАЛЕННЯ ВИКЛАДАННЯ НОРМАТИВНО-ПРАВОВОЇ БАЗИ ЗАХИСТУ ІНФОРМАЦІЇ

Автор: *О.А. Баронова, ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Питання забезпечення інформаційної безпеки сьогодні для України стоять на одному рівні із захистом суверенітету і територіальної цілісності, забезпеченням її економічної безпеки. В Україні, як сучасній державі, наявна постійно зростаюча потреба у спеціалістах з інформаційної безпеки(ІБ) інформаційних і комунікаційних систем, що мають стратегічне значення в сучасній інфраструктурі держави, спеціалістах з технічного захисту інформації і з управління інформаційною безпекою.

Національний університет кораблебудування імені адмірала Макарова(НУК) бере участь в підготовці кадрів в галузі захисту інформації з 1996 року.

Враховуючи, що легітимність і дієвість використання будь-яких організаційних і технічних засобів захисту інформації визначається їх відповідністю вимогам нормативно-правової бази, яка склалася у державі, в програми підготовки фахівців із захисту інформації необхідно включити вивчення відповідних законів, підзаконних актів, нормативних документів.

Однією з головних проблем в підвищенні якості підготовки фахівців на основі сьогоденних вимог є відсутність єдиного підходу до правової підготовки.

Аналіз вимог державних стандартів з підготовки фахівців в галузі знань «Інформаційна безпека» та досвіду підготовки фахівців з інформаційної безпеки в НУК показав, що основними проблемами в правовій підготовці фахівців є наступні

- постійно зростаючий об’єм нормативної та законодавчої документації;
- відсутність єдиної правової дисципліни в ОПП;
- велика кількість змін в законах та нормативних документах з ІБ;
- поширення використання міжнародних стандартів в галузі ІБ.

Достатній рівень підготовки спеціалістів може бути досягнутий з врахуванням необхідності засвоєння ними базових знань галузі правового регулювання інформаційної діяльності

Для вирішення проблем розподіляємо вивчення базових тем правових основ захисту інформації між дисциплінами, які входять в схему бакалаврату. Загальну характеристику інформації та принципів правового регулювання захисту інформації, інформаційного законодавства України вивчаємо в рамках дисциплін "Вступ до спеціальності" та "Управління інформаційною безпекою", а питання законодавчої та нормативної бази захисту інформації в автоматизованих системах вивчаємо в рамках дисципліни "Безпека інформаційних та комунікаційних систем".

УДК 378

ВПРОВАДЖЕННЯ ЗАКОНУ УКРАЇНИ «ПРО ВИЩУ ОСВІТУ»: ЗАВДАННЯ, ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ

Автори: *О.В. Дашковська, к.х.н., доц.; В.П. Погребняк, к.т.н., проф., Інститут інноваційних технологій і змісту освіти МОН, м. Київ*

Закон України «Про вищу освіту» від 01.07.2014 № 1556-VII визначив стратегічні напрями реформування вищої освіти, завдання органів управління освітою та вищих навчальних закладів щодо його імплементації.

Передбачається осучаснення вітчизняної вищої освіти, яка по своїй структурі, рівнях та ступенях освіти, розширенню автономії вищих навчальних закладів і обмеженню монополії держави у сфері освіти та спрощенню процедур має наблизити вищу школу України до рівня європейської.

Законом установлено, що підготовка фахівців з вищою освітою здійснюється за спеціальностями та згідно з положеннями Національної рамки кваліфікацій – за відповідними освітньо-професійними, освітньо-науковими, науковими програмами на таких рівнях вищої освіти:

початковий рівень (короткий цикл) вищої освіти;
перший (бакалаврський) рівень;
другий (магістерський) рівень;
третій (освітньо-науковий) рівень;
науковий рівень.

Їм відповідають наступні ступені вищої освіти:

1) молодший бакалавр;
2) бакалавр;

3) магістр;

4) доктор філософії;

5) доктор наук.

Акцент зроблено на підвищення якості освіти. Принципово новим є положення статті 10 щодо створення Національного агентства із забезпечення якості вищої освіти, на яке покладається формування вимог до системи забезпечення якості вищої освіти та аналіз діяльності вищих навчальних закладів через процедури ліцензування, акредитації, погодження стандартів освітньої діяльності та стандартів вищої освіти.

У зв'язку з новою концепцією системи стандартів для вищої школи, у складі стандарту освітньої діяльності та стандартів вищої освіти, першочерговим завданням для Міністерства є розроблення методології та відповідних методичних рекомендацій щодо їх створення.

Інститутом розробляються проекти цих документів. Зокрема, методологія розроблення стандарту освітньої діяльності встановляє, що він має визначати сукупність мінімальних вимог до кадрового, навчально-методичного, матеріально-технічного та інформаційного забезпечення освітнього процесу вищого навчального закладу і наукової установи і включати:

1) концепцію діяльності за заявленою освітньою послугою, яка ґрунтується на результатах моніторингу регіонального ринку праці та освітніх послуг;

2) копії затверджених в установленому порядку навчальних планів;

3) відомості про кількісні показники кадрового, матеріально-технічного, науково-методичного, інформаційного забезпечення освітньої діяльності, наявність бібліотеки та обсяг її фондів;

4) копії документів, що засвідчують право власності, оперативного управління чи користування основними засобами для здійснення навчально-виховного процесу на строк, необхідний для завершення надання послуги;

5) документи про відповідність приміщень закладу та його матеріально-технічної бази санітарним нормам, вимогам правил пожежної безпеки, а також нормам з охорони праці (для навчання за напрямами підготовки (спеціальностями) з підвищеною небезпекою);

6) відомості про систему внутрішнього забезпечення якості освітньої діяльності;

7) копії документів, що засвідчують рівень освіти, кваліфікації та громадянство керівника закладу.

Стандарти освітньої діяльності розробляються для кожного рівня вищої освіти в межах кожної спеціальності з урахуванням необхідності створення умов для осіб з особливими освітніми потребами та є обов'язковими до виконання всіма вищими навчальними закладами незалежно від форми власності та підпорядкування, а також науковими установами, що забезпечують підготовку докторів філософії та докторів наук.

Розробляються та затверджуються стандарти освітньої діяльності центральним органом виконавчої влади у сфері освіти і науки за погодженням з Національним агентством із забезпечення якості вищої освіти.

Проекти стандартів освітньої діяльності розробляють науково-методичні комісії НМР з питань освіти, погоджують з Національним агентством із забезпечення якості вищої освіти та подають на затвердження центральному органу виконавчої влади у сфері освіти і науки.

Документи, які подає вищий навчальний заклад Національному агентству із забезпечення якості вищої освіти на отримання ліцензії для проведення освітньої діяльності, мають підтверджувати його відповідність стандарту освітньої діяльності за заявленою спеціальністю.

Методологія розроблення стандартів вищої освіти базується на тому, що вони визначають сукупність вимог до змісту та результатів освітньої діяльності вищих навчальних закладів і наукових установ за кожним рівнем вищої освіти в межах кожної спеціальності.

Стандарти вищої освіти розробляються для кожного рівня вищої освіти в межах кожної спеціальності і встановлюють такі вимоги до освітньої програми:

1) обсяг кредитів ЄКТС, необхідний для здобуття відповідного ступеня вищої освіти;

2) перелік компетентностей випускника;

3) нормативний зміст підготовки здобувачів вищої освіти, сформульований у термінах результатів навчання;

4) форми атестації здобувачів вищої освіти;

5) вимоги до наявності системи внутрішнього забезпечення якості вищої освіти;

6) вимоги професійних стандартів (у разі їх наявності).

Стандарти вищої освіти за кожною спеціальністю розробляє центральний орган виконавчої влади у сфері освіти і науки з урахуванням пропозицій галузевих державних органів, до сфери управління яких належать вищі навчальні заклади, і галузевих об'єднань організацій роботодавців та затверджує їх за погодженням з Національним агентством із забезпечення якості вищої освіти.

Проекти стандартів вищої освіти розробляють науково-методичні комісії НМР з питань освіти, погоджують з Національним агентством із забезпечення якості вищої освіти та подають на затвердження центральному органу виконавчої влади у сфері освіти і науки.

Слід зазначити, якщо роботу над методологіями, рекомендаціями і деякими іншими документами уже розпочато інститутом, то розробленню стандартів має передувати прийняття актів Уряду щодо переліків галузей знань і спеціальностей, за якими буде здійснюватись підготовка фахівців з вищою освітою, створення Національного агентством із забезпечення якості вищої освіти. Крім того, Міністерству потрібно сформувати нову Науково-методичну раду з питань освіти та науково-методичні комісії. До речі, виписані у Законі умови створення останніх (відсутність у складі представників керівництва вищих навчальних закладів, не більше одного представника від навчального закладу тощо) значно ускладнять виконання, покладеної на науково-методичні комісії функції: розроблення стандартів освітньої діяльності та стандартів вищої освіти. Спростити цю проблему могли б внесені вищими навчальними закладами пропозиції щодо надання відповідних прав НМК, у тому числі створення робочих груп, визначення базових навчальних закладів, заохочення розробників стандартів.

В контексті розширення автономії вищих навчальних закладів актуальним є відміна «грифування» Міністерством навчальної літератури для вищої школи. Одночасно йдеться про підвищення відповідальності вчених рад і керівників вищих навчальних закладів за якість підручників і навчальних посібників.

Остаточне рішення зафіксоване в Порядку висунення Міністерством освіти і науки підручників для здобуття Державної премії України в галузі освіти і науки, схваленим колегією від 26.06.2014 року, протокол № 4/6-19.

Порядком (абзац 2 преамбули) визначено поняття «підручник» як «будь-яке видання в друкованому або електронному вигляді, в т.ч.

електронні підручники, яке використовується у навчальному процесі для вивчення певного навчального предмету або дисципліни». Підпунктом 1.2 пункту 1 «Критерії прийняття підручників для розгляду» визначено, що Міністерство розглядає підручники, які «затверджені як підручники для використання у навчальному процесі Міністерством освіти і науки України – стосовно підручників для середньої та професійно-технічної освіти, а також стосовно підручників для вищої освіти – до 2014 року, або рекомендованих як підручники вченими радами вищих навчальних закладів, починаючи з 2014 року».

Підводячи підсумок, зазначимо, що попереду важка і довготривала робота з імплементації положень Закону в освітню практику. Її успіх залежить від спільної і системної діяльності органів управління освітою, вищих навчальних закладів, активної участі освітянської громадськості і стане запорукою інноваційного розвитку вітчизняної вищої школи, її успішної інтеграції в міжнародний освітній простір.

УДК 004.056

РОЗРОБКА АЛГОРИТМУ ВИЯВЛЕННЯ МОДИФІКАЦІЇ ЦИФРОВОГО АУДІОЗАПИСУ МЕТОДОМ ФРАКТАЛЬНИХ ПЕРЕТВОРЕНЬ

Автор: *С.М. Нужний, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Вступ. Прискорений розвиток цифрових та мобільних пристроїв зв'язку призвід до суттєвого зменшення сфери використання стаціонарних телефонних апаратів. Однак є напрямки, в яких така відмова неможлива. Одним з них є система телекомунікації для контрольованої зони, так як при застосуванні системи радіочастотного зашумлення («РІАС», «ІЗ-2000», «Крона», «Пелена» та інші) використання засобів радіозв'язку не можливе.

Одночасно з цим, використання стаціонарних ліній зв'язку пов'язане з наявністю широкого спектру засобів НСД, які можуть бути використані зловмисниками, для перехоплення ІзОД. Це твердження є головним аргументом, який підтверджує актуальність створення лабо-

раторних комплексів для вивчення студентами принципів побудови систем моніторингу електропровідних телекомунікаційних мереж для запобігання витоку інформації і локалізації технічних засобів розвідки та набуття навичок по експлуатації відповідного обладнання. Комплекс може бути застосованим і для проведення тестування нових методик та засобів протидії витоку інформації по телекомунікаційним лініям.

Метою роботи є впровадження в учбовий процес першого етапу лабораторного комплексу «Основи технічного захисту інформації в ВТКМ»

Основна частина. Створення сучасних телекомунікаційних систем неможливе без комплексного використання різнотипних мереж. Їх різноманітність останнім часом збільшується кожні декілька років. Особливо швидкими темпами йде створення аналогових систем передачі великої кількості інформації на понад високих частотах та розвиток цифрових технологій з передачею інформації з псевдошумовою модуляцією. Одночасно з цим йде й подальший розвиток електропровідних та оптиковолоконних технологій передачі інформації.

Така різноманітність сприяє зловмисникам, даючи можливість використання як класичних каналів для доступу до ІзОД, так і створювати нові.

На рис. 1 наведено структурна схема лабораторного комплексу для дослідження методів протидії несанкціонованому доступу до інформації, яка передається по ВТКМ. Схема складається з трьох базових блоків:

– блок 1 «Дослідження принципів протидії НСД до ІзОД, яка передається по провідним ВТКМ»;

– блок 2 «Моделювання перехоплення інформації (СМПІн), що передається по дротяних і радіочастотним ВТКМ»;

– блок 3 «Дослідження принципів протидії НСД до конфіденційної інформації, яка передається по дротяних і радіочастотним ВТКМ (зв'язок через Інтернет)».

Блок "Дослідження принципів протидії НСД "Телефон"" складається з телефонного апарату, засобу контролю фізичних параметрів лінії і захисту інформації від НСД. Призначений – для моделювання обміну інформацією між абонентами по дротяній ВТКМ, контролю фізичних параметрів дротяної ВТКМ і захисту інформації, яка передається по лініям в мережі, від НСД інженерно-технічними і криптографічними методами [7]. До складу блоку входить два модуля «Дослідження принципів протидії НСД «Телефон»».

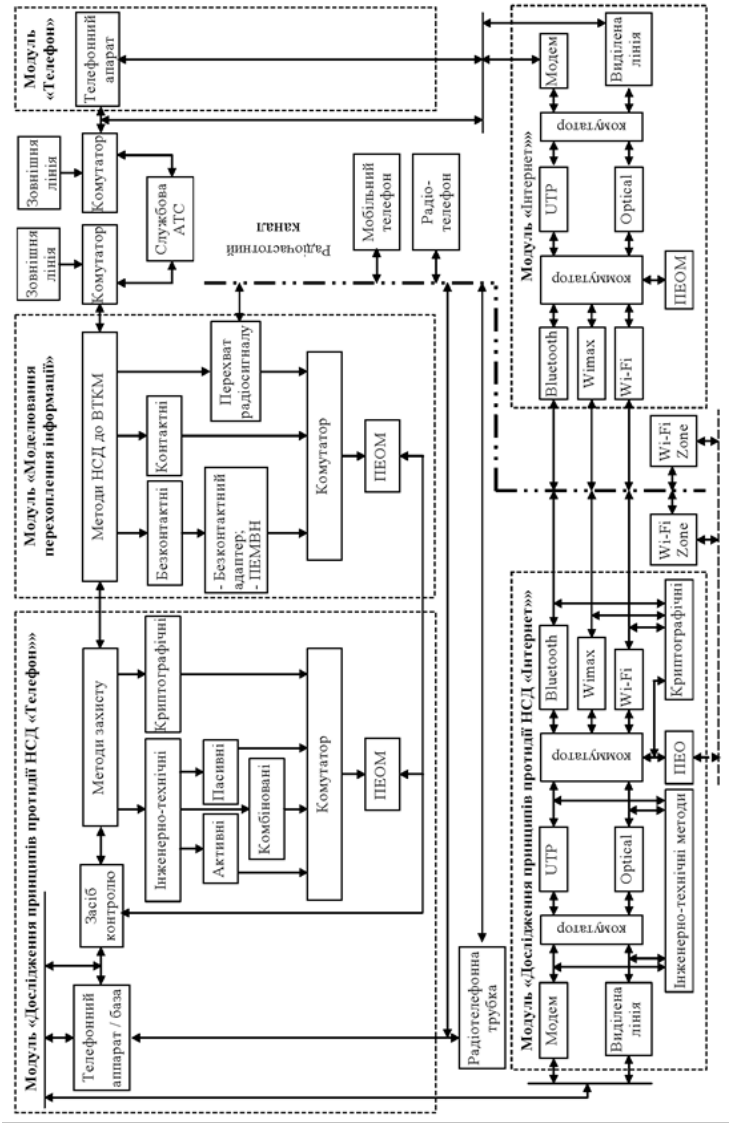


Рис. 1. Структурна схема лабораторії по дослідженню методів протидії НСД до ІзОД, яка передається по ВТКМ

Блок "Дослідження принципів протидії НСД "Інтернет"" складається з ПЕОМ і пристроїв підключення Інтернет-ресурсів. Призначений – для моделювання обміну інформацією між абонентами (АС2), у тому числі, з виходом в Інтернет (АС3), контролю фізичних параметрів радіочастот і захисту інформації, яка передається в мережі, від НСД інженерно-технічними і криптографічними методами.

Блок "Моделювання перехоплення інформації" складається з моделей пристроїв НСД до ВТКМ та призначений для моделювання пристроїв знімання інформації з дротяних і радіочастотних ВТКМ, а також впливу фізичних параметрів середовища на канал передачі інформації.

На першому етапі планується реалізувати розробку лабораторного стенду на базі міні-АТС Simens OfficeCom, субблоків з модулів «Дослідження принципів протидії НСД «Телефон» (блок «Засіб контролю» та субблок «Інженерно-технічні засоби» блоку «Методи захисту», пристроїв «Граніт-7» та «Граніт-8») та «Моделювання перехоплення інформації» (блок «Контактні»).

Висновки

Лабораторний комплекс «Основи технічного захисту інформації в ВТКМ» планується до використання в учбовому процесі при підготовці фахівців за напрямком «Інформаційна безпека» по спеціальностях 170101, а також для проведення перепідготовки фахівців відділів «ТЗІ» та проведення науково-дослідних робіт і експертиз обладнання.

Список літератури:

1. Нужний С.М. Лабораторний навчально-дослідний комплекс „Дослідження методів виявлення та протидії несанкціонованому доступу до конфіденційної інформації з використанням радіопередавачів та електропровідних ліній” / Вісник Східноукраїнського національного університету ім. В.Даля. Науковий журнал. – Луганськ, 2010. – №9 (150)

2. Блінцов В.С., Нужний С.М., Баша Д.А. Концепція створення лабораторного комплексу «Основи технічного захисту інформації в ВТКМ» / Матеріали X Міжнародної науково-технічної конференції «Авіа-2011». – Т.1.– К.: НАУ, 2011. – С.2.48-2.51

ЛАБОРАТОРНИЙ КОМПЛЕКС ПО СИСТЕМАМ РАДІОЧАСТОТНОЇ ІДЕНТИФІКАЦІЇ

Автор: *С.Л. Трибулькевич, викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

За останні роки системи контролю доступу (СКД) на базі технології радіочастотної ідентифікації (RFID) отримали широке поширення, оскільки при мінімальних витратах дозволяють практично повністю автоматизувати контроль доступу співробітників на територію підприємства.

У найпростіших випадках, де не потрібен високий рівень безпеки, а виділений на організацію системи бюджет невеликий, для побудови СКД використовується стандарт EM Marine. Всі карти і зчитувачі цього стандарту працюють на частоті 125 кГц, і саме вони встановлені на більшості дрібних і середніх підприємств. Крім низької вартості такі системи привабливі для користувача ще й різноманітністю пропонованих рішень. Як мінімум, вони дозволяють організувати контроль доступу через одну-дві двері, а як максимум – створити сучасні мережеві IP-рішення з можливістю масштабування.

У порівнянні з бюджетним EM Marine більш цікавим стандартом в області радіочастотної ідентифікації є Mifare. Карти та зчитувачі Mifare працюють на частоті 13,56 МГц. До основних переваг Mifare відноситься, по-перше, шифрування даних при обміні між картою і зчитувачем і, по-друге, наявність у карти вбудованої пам'яті, куди можна записувати різні додатки.

Представляється досить зручним на одній апаратній базі з СКД організувати також і систему обліку робочого часу (СОРЧ). Використовуючи дані, зібрані RFID-зчитувачами і контролерами СКД, програма може формувати різні види звітів.

Схема взаємодії програмно-апаратного забезпечення стенду наведена на рис. 1. Програмне забезпечення приймає дані від зчитувачів RFID стандартів EmMarine 125 кГц та Mifare 13,56 МГц для системи контролю доступу передбачено підтримку баз даних на базі серверу MS SQL 2008.

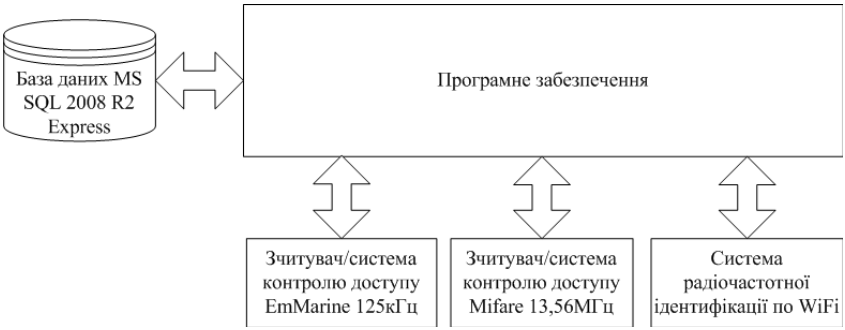


Рисунок 1 – Схема взаємодії програмно апаратного забезпесення

Структуру бази даних наведено на рис. 2. База у даній реалізації складається з трьох таблиць. Таблиця "Cards" зберігає ключі міток, у відповідність кожному ключу ставиться ідентифікатор власника, який зв'язаний з таблицею "CardsOwners". Таблиця "CardsOwners" зберігає персональні дані власників карток. Таблиця "Func" зберігає перелік посад персоналу, для зв'язку таблиці посад з таблицею власників передбачено спеціальний ідентифікатор FuncID у таблиці "CardsOwners".

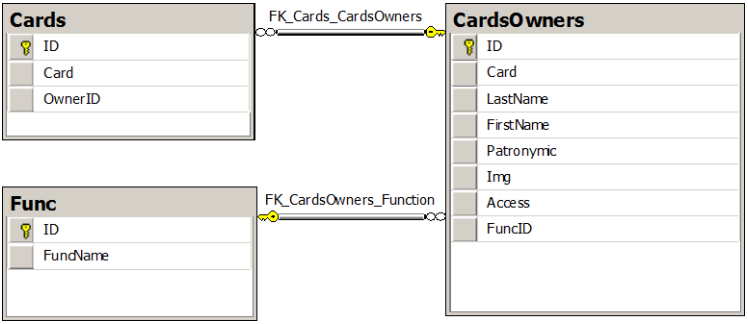


Рисунок 2 – Структура таблиць бази даних

Модулі програми викликаються з головного вікна, яке являє собою прототип системи контролю доступу. Редагування записів у базі даних передбачено у меню редактора (рис. 3).

Після запуску з'являється головне вікно програми (рис. 4). Головне вікно програми складається зі строки меню, полів персональних даних особи, що було ідентифіковано та поля керування виконавчими механізмами.

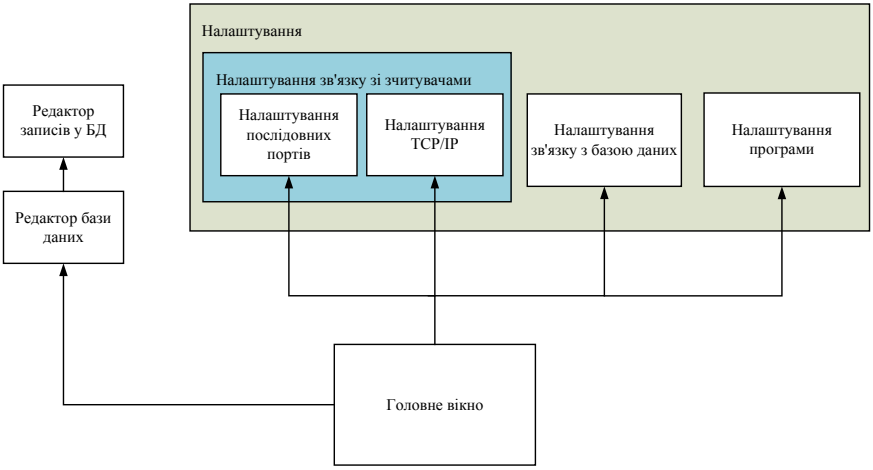


Рисунок 3 – Структура модулів програмног забезпечення

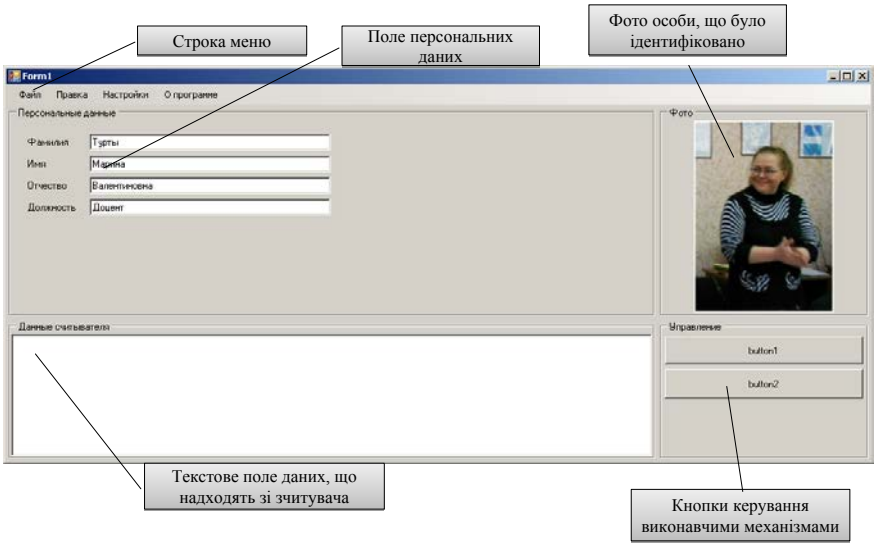


Рисунок 4 – Головне вікно програми

Для роботи з базою даних передбачено відповідний редактор. При завантаженні редактора проводиться вибірка даних з усіх таблиць бази. Є можливість як редагування існуючих записів так і додавання нових.

Апаратна частина являє собою систему контролю доступу на базі зчитувача RFID EmMarine 125 кГц (рис. 5). Зчитувач відправляє дані до ПЕОМ через послідовний порт, комп'ютер обробляє прийняті дані та відправляє відповідь до зчитувача, яка складається з прізвища та першої букви імені працівника, а також спеціального символу керування виконавчими механізмами, Якщо була піднесена картка з невідомим ідентифікатором до зчитувача відправляється текст "Неизвестно". Зчитувач приймає дані від ПЕОМ, включає відповідні механізми та виводить інформацію на дисплей.

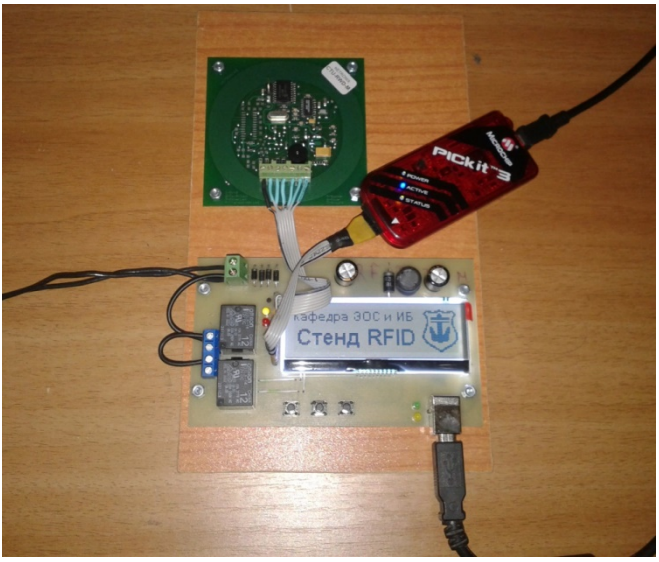


Рисунок 5 – Апаратна частина стенду

Висновки: виконано розробку програмного забезпечення для стенду по дослідженню RFID технологій. Програмне забезпечення має функції по дослідженню технології RFID та реалізує прототип системи контролю доступу з використанням сучасних мережевих технологій.

УДК 004.056:378.14

ФОРМАЛІЗАЦІЯ ЗАДАЧІ РОЗРОБКИ МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ ПІДГОТОВКИ КАДРІВ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Автор: *М.В. Турти, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Вступ. При розробці методичного забезпечення підготовці кадрів виникають задачі створення стандартів освіти, робочих програм нормативних і варіативних дисциплін, методичних вказівок до практичних занять, курсового проектування і поза аудиторної роботи. При цьому важливим є здобуття студентами комплексних знань і вмінь для прийняття рішень у фаховій діяльності. Оскільки темпи генерації нових знань в інформаційному суспільстві є надзвичайно високими, то для забезпечення відповідності змісту навчального процесу і стану розвитку предметної галузі необхідно регулярно оновлювати методичне забезпечення із збереженням його відповідності поточним нормативним документам. Особливо відчутною при розробці методичного забезпечення є динаміка інформаційної моделі навчального процесу і динаміка розвитку відповідних предметних галузей в разі підготовки фахівців з інформаційних технологій, які відрізняються найвищими темпами розвитку, зокрема, підготовки фахівців з інформаційної безпеки [1, 2]. Розробка і оновлення методичного забезпечення для таких галузей знань вимагають моніторингу предметної галузі і відстежування динамічних взаємозв'язків між дисциплінами, тобто вимагають великих витрат часу і припускають наявність помилок, пов'язаних із відповідністю методичного забезпечення різних дисциплін і відповідності вимогам стандартів освіти. Типовим засобом рішення таких проблем є використання автоматизованих систем. Процедури розробки методичного забезпечення на даний час можна вважати частково автоматизованими [3], але формалізація задачі в загальному вигляді відсутня.

Метою даної роботи є розробка теоретичних положень формалізації задачі розробки методичного забезпечення підготовки кадрів у галузі інформаційної безпеки.

Для формалізації задачі розробки методичного забезпечення навчального процесу пропонується наступний алгоритм:

1. Визначення зі стандартів освіти множини Z фахових задач діяльності z_i: $Z = \{z_1, z_2, \ldots, z_i, \ldots, z_n\}$, де $i = \overline{1,n}$ – номер фахової задачі діяльності, n - загальна кількість фахових задач діяльності.

2. Визначення зі стандартів освіти множини D дисциплін d_j: $D = \{d_1, d_2, \ldots, d_j, \ldots, d_m\}$, де $j = \overline{1,m}$ – номер дисципліни, m - загальна кількість дисциплін.

3. Визначення зі стандартів освіти множин ZM_j змістових модулів zm_{lj_j} дисциплін d_j: $ZM_j = \{zm_{1j}, zm_{2j}, \ldots, zm_{lj}, \ldots, zm_{L_j j}\}$, де $l = \overline{1,L_j}$ – номер змістового модуля дисципліни d_j, L_j – загальна кількість змістових модулів дисципліни d_j.

4. Визначення із інформаційної моделі навчального процесу системи зв'язків між змістовими модулями дисциплін d_j і d_k у вигляді матриць ZV_{jk} розмірності $L_j \times L_k$: $ZV_{jk} = \{zv_{jk_{lq}}\}$, $q = \overline{1,L_k}$ за правилами:

- $zv_{jk_{lq}} = 0$ – зв'язок відсутній;
- $zv_{jk_{lq}} = v_{kq}$, $v_{kq} \in \left\{\frac{1}{9}, \frac{1}{8}, \ldots, \frac{1}{2}, 1, 2, \ldots, 9\right\}$ – зв'язок наявний.

$0 < v_{kq} < 1$ – дисципліна d_j містить інформацію, необхідну для засвоєння дисципліни d_k. $1 < v_{kq} < 9$ – дисципліна d_k містить інформацію, необхідну для засвоєння дисципліни d_j.

5. Визначення за методикою аналогічною [4] векторів пріоритетів змістових модулів $PM = \{pm_h\}$, $h = \overline{1,H}$, довжиною $H = \sum_{j=1}^{m} L_j$, вважаючи всі дисципліни рівнозначними.

6. Визначення в результаті моніторингу стану предметної галузі експертним шляхом критеріїв оцінювання поточної важливості фахо-

вих задач діяльності $KZ = \{kz_1, kz_2, \ldots, kz_g, \ldots, kz_{K1}\}$, де $g = \overline{1, K1}$ – номер критерію, $K1$ - загальна кількість дисциплін критеріїв оцінювання поточної важливості фахових задач діяльності.

7. Визначення в результаті моніторингу стану предметної галузі експертних оцінок поточної важливості фахових задач діяльності vz_i: $VZ = \{vz_1, vz_2, \ldots, vz_i, \ldots, vz_n\}$ за сукупністю критеріїв п.6.

8. Визначення аналогічно [4] ступенів важливості змістових модулів з точки зору виконання сукупності фахових задач діяльності vm_i: $VM = \{vm_1, vm_2, \ldots, vm_i, \ldots, vm_h\}$.

9. Визначення аналогічно [4] глобальних пріоритетів змістових модулів $VMG = \{vmg_1, vmg_2, \ldots, vmg_i, \ldots, vmg_h\}$ з точки зору виконання сукупності фахових задач діяльності і організації навчального процесу з врахуванням важливості фахових задач діяльності.

Такий підхід дозволяє автоматизувати процеси динамічної перебудови інформаційних моделей навчального процесу (п.2-4) і врахувати динамічні зміни пріоритетів фахових задач діяльності.

Висновки. Визначено теоретичні положення формалізації задачі розробки методичного забезпечення підготовки кадрів у галузі інформаційної безпеки, які дозволяють оптимізувати навчальний процес, є відкритими для подальшої модернізації і можуть бути поширені на інші динамічні галузі знань.

Список літератури:

1. Турти М.В., Овсянніков В.М. Інформаційні технології і процес підготовки спеціалістів з електромеханіки // Матеріали Всеукраїнської науково-технічної конференції з міжнародною участю «Проблеми електрообладнання і автоматики транспортних засобів» (ПАЕТЗ-2009).- Миколаїв: НУК, 2013. – С.34-36.

2. Турти М.В. Підготовка кадрів у галузі інформаційної безпеки у вузі наукового типу // Матеріали Всеукраїнської науково-технічної конференції з міжнародною участю «Проблеми електрообладнання і автоматики транспортних засобів» (ПАЕТЗ-2013). – Миколаїв: НУК, 2013.

3. Турти М.В., Балакін І.А. Захищена автоматизована система генерації стандартів освіти вузу // Вісник Східноукраїнського національного університету ім.В.Даля. Луганськ: Вид-во СНУ ім.В.Даля, 2012. – №8(179). – Ч.1.- С.251-259.

4. Баронова О.А., Турти М.В. Методика визначення комплексу методів системного аналізу для оцінювання об'єктів і процесів ТЗІ //Тези доповідей Третьої Міжнародної науково-практичної конференції «Інформаційні технології та коп'ютерна інженерія» м. Вінниця, 29-31 травня 2012 року. – Вінниця: ВНТУ, 2012. – С.180-181.

УДК 004.056

ПРОГРАМНИЙ МОДУЛЬ ПОРІВНЯННЯ НЕЧІТКИХ ЕТАЛОНІВ ЗА ВЛАСТИВОСТЯМИ

Автори: *М.В. Турти, к.т.н., доц.; О.С. Дібрівний, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Вступ. Для ідентифікації загроз і уразливостей в інформаційних системах існують певні програмні засоби, однак вони мають закритий код і базуються на нечітких еталонах (НЕ), однак програмні засоби порівняння НЕ на даний момент на ринку відсутні. Тому необхідно розробити гнучкий програмний засіб з відкритим кодом, який дозволяв би формувати і обробляти НЕ і виводити результати у зручному для користувача вигляді. Автоматизація процедур обробки нечітких даних особливо важлива при роботі в реальному часі, тобто в режимі, в якому працюють всі системи моніторингу інформаційної безпеки і системи контролю доступу [1]. В системах розпізнавання об'єктів та ситуацій базовою процедурою є порівняння даних об'єкта і образа. В автоматизованій системі формування і обробки нечітких еталонів (АСФОНЕ) [2] для пари нечітких множин (нечіткого еталону та нечіткого числа, що відповідає досліджуваному об'єкту) можуть застосовуватися для порівняння операції впорядкування та порівняння за формою функцій належності (ФН). Остання процедура може бути реалізована як порівняння за властивостями ФН.

Метою даної роботи є розробка програмного засобу визначення властивостей нечітких еталонів в інформаційній безпеці.

Основна частина. Для досягнення поставленої мети необхідно розв'язати наступні задачі: провести аналіз властивостей нечітких множин (НМ) і визначити ті з них, що підлягають автоматичному визначенню, і ті, що можуть бути визначені лише в діалоговому режимі з користувачем; визначити особливості процедур визначення властивостей НЕ методами класичної теорії (КТ) і методами однозначної нечіткої логіки (ОНЛ) [3]; проаналізувати форми представлення вхідної і вихідної інформації блоку визначення властивостей нечітких еталонів у складі АСФОНЕ; розробити алгоритми визначення властивостей функцій належності нечітких чисел (НЧ) для АСФОНЕ і розробити відповідний програмний модуль а також модулі загального інтерфейсу системи, вводу даних і графічного представлення ФН окремих НЧ, термів лінгвістичних змінних та двох НМ; сформулювати практичні рекомендацій щодо використання розробленого програмного засобу.

Операції з окремими НМ можуть бути розділені на операції перетворення ФН, до яких відносяться операції нормалізації, концентрування, розтягування і операція розбиття НМ на α-рівневі підмножини, операції визначення властивостей ФН та операції визначення параметрів ФН, до яких відносяться вісі інші операції.

На основі проведеного аналізу властивостей НЕ, визначено, що автоматичному визначенню підлягають всі властивості, окрім дискретності і параметричності, які можуть бути визначені лише в діалоговому режимі з користувачем, а також, що процедури визначення властивостей ФН, які відповідають ОНЛ, є спрощеними, оскільки властивості унімодальності, нормальності та параметричності для таких ФН є наперед визначеними.

Оскільки формування ФН може здійснюватися різними методами [1], кожен з яких здатен забезпечити певні властивості ФН, і порівняння шляхом впорядкування може здійснюватися лише за методами, які мають певні властивості, то в розробленому програмному блоці передбачена перевірка відповідності властивостей введених НМ і властивостей, що є припустимими для кожного методу. При цьому використовується алгоритм порівняння векторів властивостей ФН, при однакових вагових коефіцієнтах властивостей. Розроблені алгоритми

визначення враховують наявність протирічних властивостей, наприклад, «нормальність» – «субнормальність» та ін.

Висновки. В роботі визначені структура блоку визначення властивостей НМ і структура його зв'язків з іншими блоками АСФОНЕ (рис.1), визначені форми представлення вхідної і вихідної інформації, розроблені алгоритми визначення властивостей ФН нечітких чисел і відповідний програмний модуль, а також модулі загального інтерфейсу системи, вводу даних і графічного представлення ФН (рис.2), сформульовані практичні рекомендацій щодо використання розробленого програмного засобу.

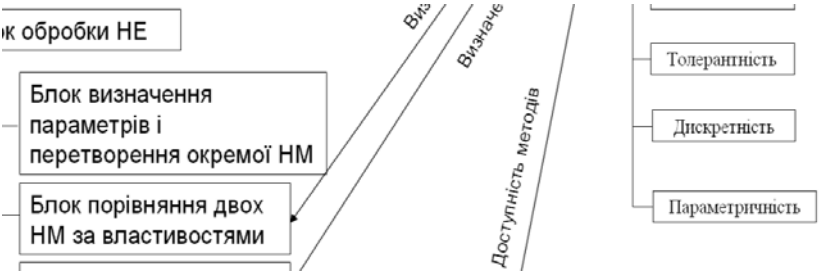


Рисунок 1 – Взаємодія блоків АСФОНЕ
з блоком визначення властивостей

Робота має практичне значення, оскільки на даний час діючі аналоги не дозволяють автоматично визначати властивості нечітких чисел, і створювати в залежності від отриманих результатів множини доступних методів для побудови і обробки НЕ.

Розроблений програмний блок може використовуватися як окремий модуль, або вбудовуватися в АСФОНЕ чи в системи ідентифікації, навігації, управління, системи виявлення уразливостей в початкових кодах, системи оцінювання ефективності захисту інформації.

Розробка може використовуватися також в навчальному процесі підготовки фахівців галузі знань 1701 «Інформаційна безпека».

Список літератури:

1. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: "МК-Пресс", 2006. – 320 с.

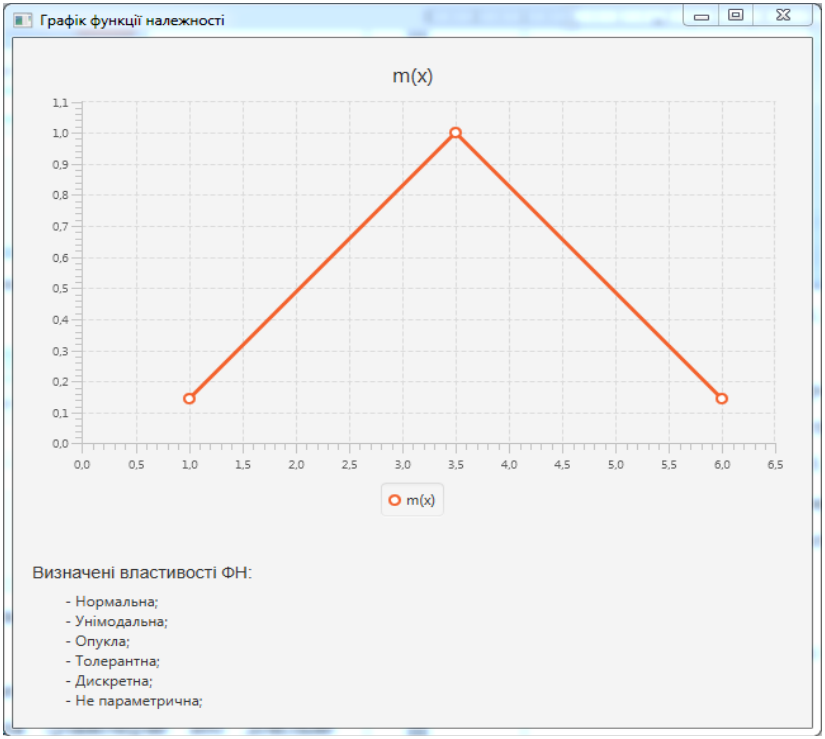


Рисунок 2 –Виведення результатів

2. Мігунов В.О. Програма обробки нечітких еталонів //Матеріали Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».-Миколаїв: НУК, 2011. – С.97-101.

3. Турти М.В. Теорія однозначних нечітких систем та нейронні мережі: Монографія. Частина 1. – Миколаїв: Вид-во Європейський університет, Миколаївська філія, 2007. –140 с.

УДК 004.056.55

ОПЫТ ИСПОЛЬЗОВАНИЯ ДИПЛОМНОГО ПРОЕКТИРОВАНИЯ ПРИ СОЗДАНИИ ПРОГРАММНОГО КОМПЛЕКСА ПО ЦИФРОВОЙ ОБРАБОТКЕ СИГНАЛОВ

Автор: *О.А. Щелконогов, ст. преподаватель, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев*

На кафедре электрооборудования судов и информационной безопасности Национального университета кораблестроения им. адм. Макарова разработан программный комплекс для лабораторного практикума по предмету «Цифровая обработка сигналов» (ЦОС) специальности 6.17010201 „Системы технической защиты информации, автоматизация ее обработки”. Существует несколько подходов к порядку выполнения лабораторных работ по ЦОС [1-6]. Они отличаются между собой тем, используются ли программы математического моделирования (Mathcad, Matlab) или нет, пишут ли студенты собственные программы или нет, используются ли готовые программы расчетов или нет. На наш взгляд, одним из самых удачных вариантов является комбинированное использование специализированных программ, реализующих алгоритмы ЦОС и универсальных программ математического моделирования. Именно такой подход реализован при проведении лабораторных работ по ЦОС с использованием описываемого комплекса. Использование специального программного комплекса должно решать проблему экспериментального получения результата. Все другое время занятия студенты могут уделить «аналитической» части: в среде Mathcad или Matlab составить свой проект под наблюдением преподавателя, а потом сравнить полученные результаты.

Исходя из требований учебного процесса, структура лабораторного комплекса состоит из трех частей (рис. 1):

– программа, которая реализует последовательность операций лабораторных работ (далее просто программный комплекс);

– тестовая система, которая осуществляет предварительное тестирование готовности и финальное тестирование для защиты;

– методические указания, которые вызываются в виде справочной системы.

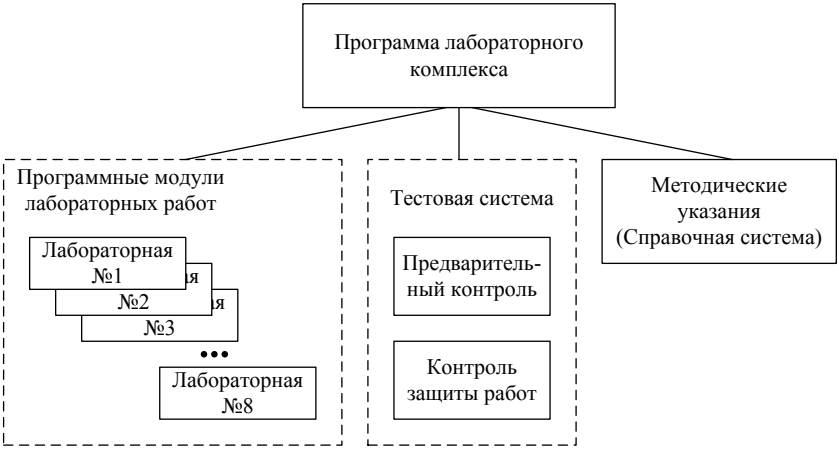


Рисунок 1 – Структура лабораторного комплекса

Каждая лабораторная работа реализована в виде одного программного модуля. Такое построение удобно с точки зрения программной реализации, использования и последующей модернизации. Каждый модуль относительно независим, общими являются некоторые функции (например, быстрое преобразование Фурье используется во многих лабораторных работах или функции сохранения результатов работы).

Все модули совместимы с MathCad по файлам данных с расширением prn, т.е. результат работы программы может быть загружена в MathCad и наоборот. Кроме того, имеется совместимость и по стандартным типам файлов (bmp, jpeg, wav).

Модули программного комплекса написаны на языке C++ и имеют близкую логику построения. Интерфейс достаточно простой и интуитивно понятный. Пример работы одного из модулей показан на рис. 2.

Порядок следования, темы лабораторных работ и их сложность определяются рабочей программной по дисциплине «Цифровая обработка сигналов» и выбраны по возможности в порядке следования лекционного материала. Само содержимое работ построено таким образом, чтобы студенты изучали именно алгоритмы обработки сигналов, а не возможности программ для этих целей (хотя попутно решается и эта задача).

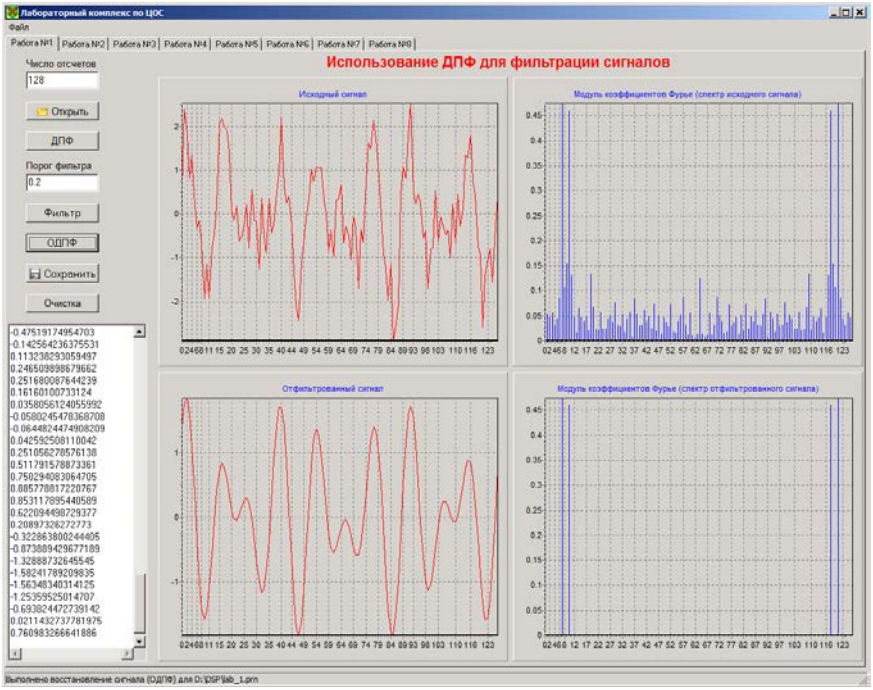


Рисунок 2 – Вид окна модуля лабораторной работы № 1

Все модули лабораторного комплекса создавались в рамках дипломного проектирования студентами – дипломниками. Основной сложностью такого принципа разработки является некоторая протяженность по времени (комплекс создавался на протяжении нескольких лет), разный уровень подготовки студентов по данному направлению и квалификации в области программирования. Это требует повышенной нагрузки на руководителя дипломного проекта.

Проект «Программный комплекс по ЦОС» находится в постоянном развитии. Вносятся изменения и дополнения в программные модули и в методическое обеспечение.

Выводы

В работе описан программный комплекс для лабораторного практикума по цифровой обработке сигналов: идеология создания, назначение, состав, методология применения. Использование лабораторно-

го комплекса на занятиях производится совместно с программным пакетом MathCad. Это позволяет, с одной стороны, упростить процесс программирования и облегчить визуализацию результатов, а с другой стороны, не снижает нагрузку на студентов по изучению алгоритмов и методов обработки сигналов. Создание комплекса происходило силами студентов-дипломников, что имеет большой учебно-методический и образовательный эффект.

Список литературы:

1. Задания на лабораторную работу. – Режим доступа: http://athena.vvsu.ru/carina/dsp.

2. Обработка информации в цифровых системах связи: учебное пособие по лабораторному практикуму / С.К. Абрамов, Д.В. Февралев, А.А. Роенко и др. – Х.: Нац. аэрокосм. ун-т «Харьк. авиац. ин-т», 2011. – 38 с. – Режим доступа: http://k504.xai.edu.ua/html/library/Lukin/OICSS-LR.pdf/.

3. Курячий М.И. Цифровая обработка сигналов: Лабораторный практикум. – Томск: Томский межвузовский центр дистанционного образования. 2012. – 79 с.

4. Лекции и бесплатные компьютерные программы: цифровая обработка сигналов, экспертные системы.– Режим доступа: http://aprodeus.narod.ru/teaching.htm.

5. Учебный комплекс: Проектирование систем цифровой обработки сигналов на устройствах программируемой логики. – Режим доступа: http://wl.unn.ru/study/courses/Edu_comlex/.

6. Глинченко А.С. Цифровая обработка сигналов. Лабораторный практикум. Красноярск: ИПК СФУ, 2008. – 135 с.

СЕКЦІЯ 5. ШКОЛА МОЛОДИХ НАУКОВЦІВ

УДК 004.05(081)

ПРОГРАМНИЙ ЗАСІБ ФОРМУВАННЯ НЕЧІТКИХ ЕТАЛОНІВ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ МЕТОДОМ РІВНЕВИХ МНОЖИН

Автор: *С.С. Бак, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *М.В. Турти, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Вступ. Розробка засобів моделювання об'єктів і процесів в інформаційній безпеці є актуальною задачею, розв'язку якої присвячені праці багатьох вітчизняних і зарубіжних науковців [1, 2], однак процедури автоматизації формування нечітких еталонів для деяких з них, зокрема для методу рівневих множин, відсутні.

Метою даної роботи є розробка програмного модуля формування нечітких еталонів методом рівневих множин для автоматизованої системи формування і обробки нечітких еталонів (АСФОНЕ).

Основна частина. Для досягнення поставленої мети необхідно розв'язати наступні задачі: проаналізувати сфери використання нечітких еталонів в інформаційній безпеці; визначити особливості формування НЕ методами однозначної нечіткої логіки (ОНЛ) [2]; проаналізувати форми представлення вхідної і вихідної інформації блоку формування НЕ методом рівневих множин за класичною теорією та ОНЛ у складі АСФОНЕ; розробити алгоритми визначення функцій належності (ФН) за методом рівневих множин за класичною теорією та ОНЛ в інформаційній безпеці та відповідний програмний модуль і сформулювати практичні рекомендацій щодо його використання в інформаційній безпеці.

Метод рівневих множин (МРМ) дозволяє визначити ступінь належності елементів нечіткій підмножині $\tilde{A}$ з урахуванням відомих ймовірностей вибірки X елементів множини для фіксованих α - рівнів:

$$\mu_{\tilde{A}}(x_1) = nP(x_1);$$

$$\mu_{\tilde{A}}(x_2) = (n-1)P(x_2) + P(x_1)$$

$$\mu_{\tilde{A}}(x_3) = (n-2)P(x_3) + P(x_2) + P(x_1);...$$

$$\mu_{\tilde{A}}(x_k) = (n-k+1)P(x_k) + \sum_{i=1}^{k-1} P(x_i);...$$

$$\mu_{\tilde{A}}(x_{n-1}) = 2P(x_{n-1}) + \sum_{i=1}^{k-2} P(x_i);$$

$$\mu_{\tilde{A}}(x_n) = \sum_{i=1}^{n} P(x_i),$$

де n – кількість елементів в X; $\mu_{\tilde{A}}(x_i)$ – ступінь належності x нечіткій підмножині $\tilde{A}$; $P(x_i)$ – імовірність того, що в цьому експерименті буде вибрано елемент x_i.

Якщо $i \geq j$ то передбачається, що $\mu_{\tilde{A}}(x_i) \geq \mu_{\tilde{A}}(x_j)$, і тому $P(x_i) \geq P(x_j)$. Навпаки, якщо, $P(x_i) \geq P(x_j)$ то $\mu_{\tilde{A}}(x_i) \geq \mu_{\tilde{A}}(x_j)$. Причому $\mu_{\tilde{A}}(x_n) = 1$ тоді і тільки тоді, коли ймовірність отримання порожньої множини дорівнює нулю.

Розроблений програмний модуль забезпечує: діалоговий режим роботи з експертами; можливість задавати кількість експертів, які беруть участь у формуванні нечіткого еталону; можливість повідомляти експертам про обраний метод формування нечіткого еталона і цілі опитування; можливість визначати вагові коефіцієнти експертів; можливість визначати межі носія функції належності із захистом від помилок введення; можливість задавати кількість оцінюваних точок в області визначення із захистом від помилок введення; можливість задавати обсяг вибірки в межах від 2 до 100 із захистом від помилок введення; можливість випадковим чином задавати α-рівень і формувати на основі зважених експертних оцінок відповідні α-рівневі множини з оцінюваних точок із захистом від помилок введення; автоматично визначати кількість елементів в кожній α-рівневій множині (рис.1), ймовірності вибірки елементів з множини X оцінюваних

точок для визначеного α-рівня; автоматично здійснювати ранжування отриманих ймовірностей і розраховувати за ними значення функції належності в оцінюваних точках $x \in X$; виводити отриманий НЕ у вигляді НМ (рис.2). Додатково за цим методом визначаються α-рівневі множини, які можуть використовуватися в блоках обробки нечітких еталонів АСФОНЕ.

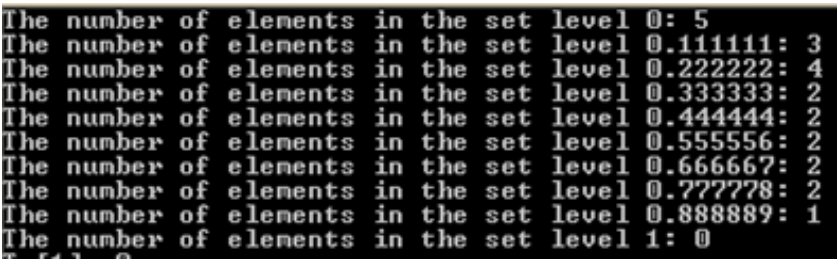


Рисунок 1 – Результати автоматичного визначення кількості елементів в α-рівневих множинах

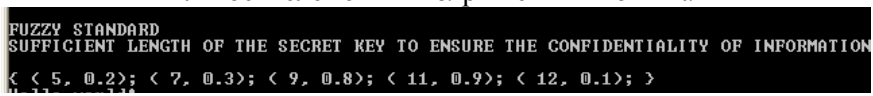


Рисунок 2 – Виведення НЕ, сформованого методом рівневих множин

Оскільки програмний модуль працює в діалоговому режимі, то для забезпечення цілісності даних передбачено захист від помилок введення (рис.3), тобто виведення повідомлень про допущені помилки введення і рекомендацій щодо їх усунення при: відмінності від шкали Сааті даних, що вводяться експертами при визначенні вагових коефіцієнтів експертів; відмінності від шкали Сааті даних, що вводяться експертами при завданні кількості оцінюваних точок носія НМ; відмінності від шкали Сааті даних, що вводяться експертами при формуванні α-рівневих множин; виходу за припустимі межі значень обсягу вибірки при експертному оцінюванні; недотриманні відносин порядку для меж носія НМ.

ФН, створені цим методом можуть бути нормальними і субнормальними, опуклими і не опуклими, унімодальними чи полімодальними, толерантними, але вони є дискретними і непараметричними в загальному випадку. Параметризація ФН можлива за окремою процедурою, яка

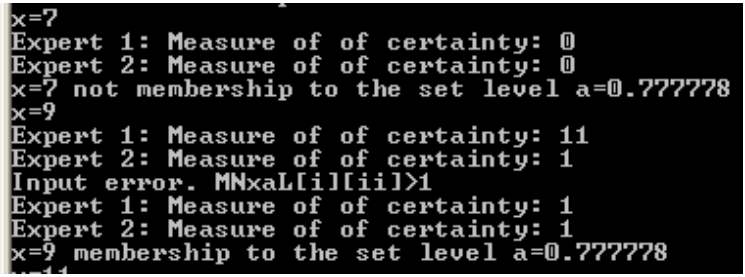


Рисунок 3 – Захист від помилок вводу при визначенні складу α–рівневих множин

передбачає підбір і оцінювання якості кривої вирівнювання. Однак, це вносить додаткову похибку в суб'єктивно визначені $\mu_{\tilde{A}}(x_n)$.

З властивостей ФН, які можна отримати за методом рівневих множин випливає, що такі ФН не відповідають вимогам ОНЛ, а для подальшої обробки таких ФН придатні методи узагальненої відстані Хеммінга, α-рівневої відстані і впорядкування на базі відношень. Якщо сформовані ФН виявляються нормальними, опуклими та унімодальними, то для подальшої обробки може бути застосований також метод впорядкування нечітких чисел.

Проведено успішну верифікацію розробленого програмного модуля на тестовому прикладі [1] формування НЕ "ДОСТАТНЯ ДОВЖИНА СЕКРЕТНОГО КЛЮЧА" при заданій множині $X = \{5, 7, 8, 10\}$, яка визначає кількість символів довжини секретного ключа, обсязі вибірки $M = 20$ і визначених в [1] результатах експертного опитування щодо складу α-рівневих множин.

Висновки. ФН, створені МРМ можуть бути нормальними і субнормаль ними, опуклими і не опуклими, унімодальними чи полімодальними, толерантними, але вони є дискретними і непараметричними в загальному випадку. Параметризація ФН можлива за окремою процедурою. Розроблено і веріфіковано програмний блок.

Список літератури:

1. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: "МК-Пресс", 2006. – 320 с.
2. Турти М.В. Теорія однозначних нечітких систем та нейронні мережі: Монографія. Частина 1. – Миколаїв: Вид-во Європейський університет, Миколаївська філія, 2007. –140 с.

УДК 004.056.5: 534: 621.391.88

ТЕОРЕТИКО–ІНФОРМАЦІЙНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ РОЗБІРЛИВОСТІ МОВИ В ОЦІНЦІ ЗАХИЩЕННОСТІ МОВНОЇ ІНФОРМАЦІЇ

Автор: *М.І. Батенко, студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *Ю.І. Касьянов, ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Захист мовної інформації – одне з найважливіших завдань у загальному комплексі заходів щодо забезпечення інформаційної безпеки об'єкта або установи.

Для технічного захисту акустичної (мовної) інформації використовуються пасивні й активні способи й засоби.

До пасивних засобів належать:

- звукоізоляція;
- установка спеціальних вставок і прокладок в трубопроводи;
- екранування виділених приміщень;
- фільтрація;
- обмеження електричних сигналів в лінії ДТЗС з мікрофонним ефектом;
- відключення перетворювачів (джерел) небезпечних сигналів.

До активних засобів належать:

- віброакустичне зашумлення;
- лінійне електромагнітне зашумлення;
- просторове електромагнітне зашумлення.

Метою роботи є аналіз теоретико–інформаційного підходу до визначення розбірливості мови та його можливостей в задачах оцінки захищеності мовної інформації від витоку прямим акустичним каналом.

Існування зв'язку між теорією розбірливості і теорією інформації відзначалось ще давно. Цей зв'язок відмічено в роботі Ю.С. Бикова [1], досліджувався він і в роботах М.А. Сапожкова [2]. Спробу використати апарат теорії інформації для визначення розбірливості мови зроблено в роботі Ю.К. Калінцева [3].

Спільним для теорії інформації і теорії розбірливості є висновок про можливість покращення якості передачі сигналу шляхом збільшення відношення сигнал – шум (при незмінному часі передачі і смуги частот сигналу). Сильною стороною теорії інформації є абстрактність її підходу до поняття сигналу, який може мати не лише мовну природу. Разом з тим, в теорії інформації відсутні рекомендації щодо вибору раціональних засобів завадостійкості передачі мовних сигналів.

Відповідно до теорії інформації, для неспотвореної передачі необхідно, щоб об'єм сигналу (V) був менше ємності каналу або рівний їй.

$$V = TFD \le V_к = TF_кD_к \qquad (1)$$

де T – час повного розуміння переданої інформації; F, $F_к$ – частотний діапазон сигналу та каналу; D, $D_к$ – динамічний діапазон сигналу та каналу.

Виходячи з того, що формантна розбірливість A може характеризувати пропускну здатність каналу мовної комунікації, що включає як засоби передачі, так і слухову систему людини, Ю.К. Калінцев запропонував оцінювати відносну кількість інформації в мовному повідомленні за допомогою співвідношення, аналогічного до

$$A = \sum_{i=1}^{n} \Delta A_i = \sum_{i=1}^{n} P_i \cdot \Delta A_{mi} \ , \qquad (2)$$

використовуваного в формантному методі [4].

Відмінність в тому, що тепер замість закону розподілу формант по частоті $A_m(f)$ оперують законом $C_0(f)$ розподілу інформації по частоті, а замість коефіцієнта сприйняття $P(E')$ використовують закон $C_{отн}(\Delta B_р)$ розподілу відносної кількості інформації за рівнем:

$$C_{отн}(\Delta B_р) = \frac{10}{D} \lg \left[\frac{1+10^{0,1 \cdot \Delta B_р}}{1+10^{0,1 \cdot (\Delta B_р - D)}} \right], \qquad (3)$$

де $\Delta B_р = B_р - B_ш$ – відношення сигнал/шум; $D = B_{pmax} - B_{pmin}$ – динамічний діапазон мовного сигналу.

Було розраховано залежність розподілу мовної інформації по частоті $C_0(f)$ та проведено її порівняння із законом розподілу формант по частоті $A_m(f)$, взятим з [4].

Алгоритм розрахунку наступний:

1. для скорочення обсягу обчислень частотний діапазон розділяємо на розрахункові смуги Δf_{pi} (в діапазоні 60…1000 Гц $\Delta f_p = 10$ Гц; в діапазоні 1…16 кГц $\Delta f_p = 100$ Гц);
2. на середніх частотах f_i кожної смуги Δf_{pi} по рис. 1 визначається $\Delta B_p(f_i)$;

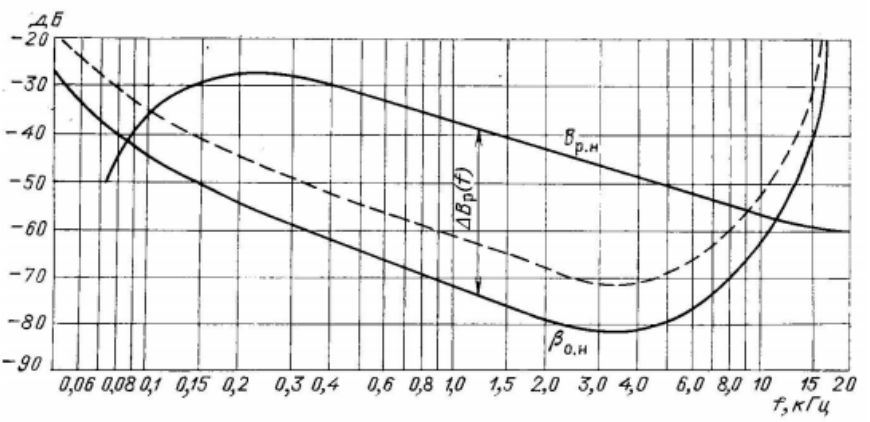


Рисунок 1 – Нормовані спектри мови і власних шумів слуху

3. по кривій 3 на рис. 2 визначаємо $C_{відн}(f_i)$;
4. визначаємо відносну кількість інформації в смугах шириною 1 Гц з урахуванням ширини критичних смуг слуху $C(f_i) = C_{відн}(f_i)/\Delta f_{эі}$;
5. за $\Delta C_0(f) = \dfrac{C(f)}{C_{\max}}$ визначається відносна кількість інформації $\Delta C_0(f)$, при цьому замість інтегрування використовувалось додавання: $C_{\max} = \sum_i C_i(f)\Delta f_p$;

6. за допомогою $C_0(f_i) := i\Delta f_{pi} \sum_1^i \Delta C(f_i)$ при $f_н = 0$, побудовано залежність $C_0(f)$ (рис. 3).

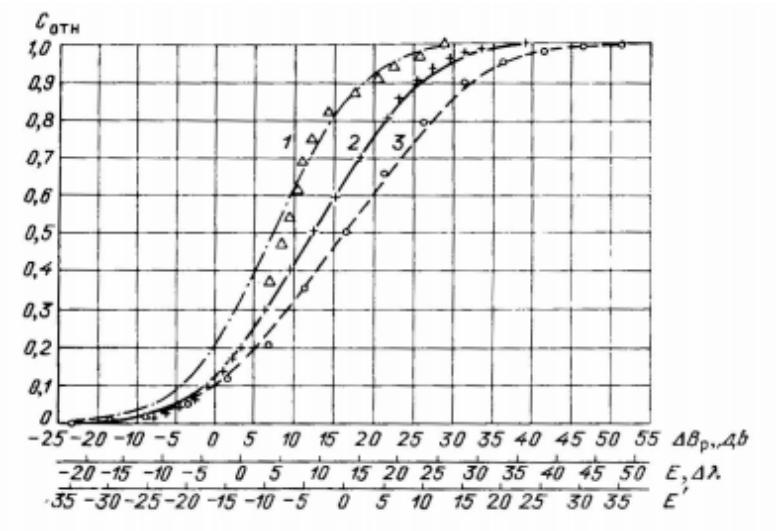


Рисунок 2 – Залежність відносної кількості інформації від перевищення рівня мови над шумами

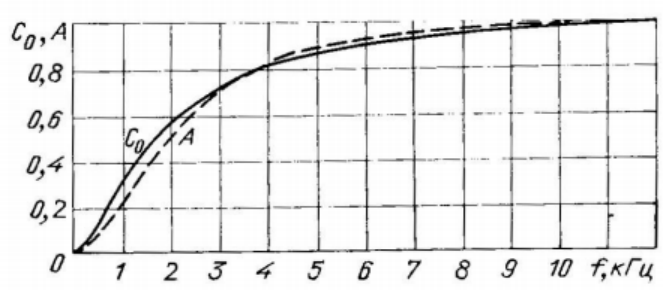


Рисунок 3 – Розподіл інформації по частотному діапазону C0(f) і розподіл формант Am(f)

При використанні кривої 2, замість кривої 3 (рис. 2) результат отримаємо практично такий самий (відхилення не перевищує 5%).

Штриховою лінією (рис. 3) показаний формантний розподіл *A(f)*. Видно, що криві дещо відрізняються одна від одної. Крива *A(f)* при частотах f<2.5 кГц зміщена відносно кривої $C_0(f)$ приблизно на 200…300 Гц і охоплює діапазон лише до 10 кГц. Перебудова кривої $C_0(f)$ для діапазону частот від $f_н$ = 300 Гц до $f_в$ = 10 кГц показало, що в цьому випадку вона практично співпадає з кривою *A(f)*.

В [5] вказується на ряд похибок, які допустив Ю.К. Калінцев.

Наприклад, він некоректно визначає зміст змінної $\Delta B_р = B_р - B_ш$, в той час, як в оригіналі ця змінна виводиться іншим чином, в результаті чого отримано відношення $\Delta B_р = B_р - B_ш + П_р$.

Друга помилка Калінцева полягає в тому, що розглядаючи коефіцієнт розбірливості М.А.Сапожкова $\omega(E)$, він прийняв $E = B_{р\ пик} - B_{ш\ пик.}$

Між іншим, насправді в працях М.А. Сапожкова прийнято $E = B_р - B_ш$.

В результаті отриманних двох помилок Ю.К.Калінцев приходить до висновку, що $\Delta B_р = B_р - B_ш = B_{р\ пик} - B_{ш\ пик.} - П_р - П_ш = E - 4{,}5$.

Вірне співвідношення повинно було мати вигляд

$$\Delta B_р = E + П_р = E+12 \qquad (4)$$

Отже, цей метод ще потребує детального розгляду та виправлення помилок для адаптації його для оцінки розбірливості мови.

Висновки. Закон розподілу інформації по частоті практично співпадає з законом розподілу формант, тому, опираючись на практику успішного використання формантного методу визначення розбірливості мови в задачах оцінки захищеності мовної інформації, можна стверджувати про можливість використання для цієї задачі і теоретико-інформаційного підходу після виправлення вказаних вище помилок та експериментальної перевірки.

Список літератури:

1. *Биков Ю.С.* Теория разборчивости речи и повышение эффективности радиотелефонной связи / *Ю.С.Быков*. – М.-Л.: Госэнергоиздат, 1959. – 350 с.

2. *Сапожков М.А.* Речевой сигнал в кибернетике и связи / *М.А. Сапожков.* – М.: Связьиздат, 1963. – 452 с.

3. *Калинцев Ю.К.* Разборчивость речи в цифровых вокодерах / *Ю.К. Калинцев.* – М.: Радио и связь, 1991. – 219 с.

4. *Покровский Н.Б.* Расчет и измерение разборчивости речи / *Н.Б. Покровский*. – М.: Связьиздат, 1962.–392 с.

5. Акустическая экспертиза каналов речевой коммуникации. Монография / *Дидковский В.С., Дидковская М.В., Продеус А.Н.* – Киев: Имэкс-ЛТД, 2008. – 420 с.

УДК 003.26

УДОСКОНАЛЕННЯ ЛАБОРАТОРНОГО СТЕНДУ З ВИВЧЕННЯ КВАНТОВИХ ПРОТОКОЛІВ

Автор: *М.С.Божко, студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *Д.М. Самойленко, к.ф.-м..н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв / Збройні Сили України*

Головну особливість квантово-криптографічних протоколів становить схема реалізації взаємодії між відправником та отримувачем інформації. У вільному доступі існує декілька схем, описаних дуже оглядово, з відзначенням лише фізичних принципів функціонування. Подібні схеми потребують значного перетворення як логічних принципів, так і елементної бази для практичної реалізації. У рамках виконання першої задачі наводяться пропозиції щодо модифікованої схеми, адаптованої для технічної реалізації.

Класичними вважаються наступні схеми. Схема на комірках Покеля(рис. 1), у рамках якої інформація передається по одній лінії зв'язку, а модуляція здійснюється електрооптичними комірками, наприклад, комірками Покеля.

Та інтерферометричні схеми (рис. 2).

Інтерферометричні схеми ґрунтуються на принципах внесення фазової різниці у плечі інтерферометрів. Схеми поділяються на одноволоконні (рис. 2а) та багатоволоконні (рис. 2б)

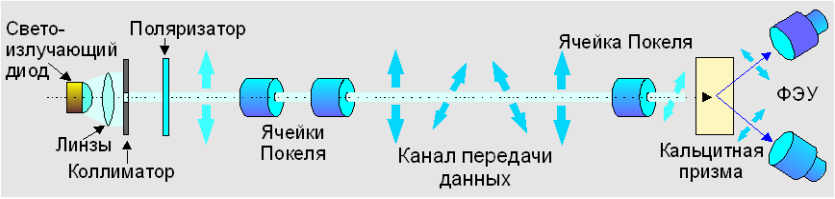
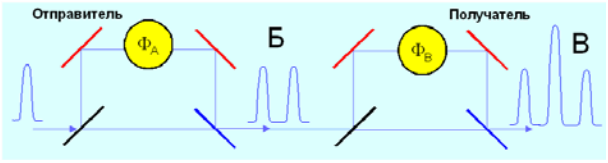
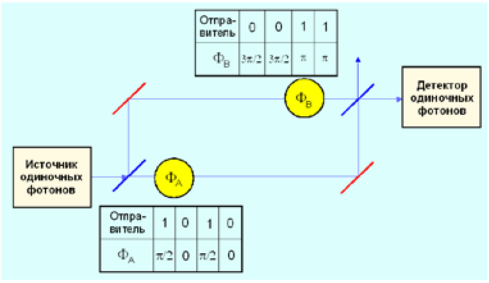


Рис.1 – Схема реалізації односпрямованого каналу з квантовим шифруванням на комірках Покеля



а



б

Рис.2 Схема на інтерферометрі з одним транспортним волокном (а), схема на інтерферометрі Маха-Цендера з двома волокнами (алгоритмВ92) (б)

Як можна помітити з рисунків, на схемах навіть не зазначається місце введення інформативного сигналу, відсутні помітки щодо електричного керування. Відтак, головним недоліком наведених схем є відсутність технічних деталей, які необхідно врахувати при конструюванні.Пропонується використання наступної схеми.

Схема основана на магнітооптичному модуляторі поляризації надхідного світла, наприклад, комірка Фарадея. Зазначений модулятор може бути виготовлений з довільної речовини, підверненої ефекту Фарадея, та соленоїду. Демодуляція сигналу відбувається за допомогою поляризаційної подільної призми, на зразок призми Волластона.

Рис. 3 Модифікована схема

Приймачами світла можуть бути фотоелектричні помножувачі або лавинні фотодіоди. На етапі налагодження можуть використовуватись звичайні фотодіоди і лазер у імпульсному режимі.

На основі запропонованої схеми було створено лабораторний стенд, який імітує принцип поляризаційного поділу променя. Імітаційна схема дозволяє знайомство та практичне вивчення принципів, закладених у спосіб комунікації, відмовившись при цьому від коштовних оптичних та оптоелектронних приладів.

Квантові канали обміну інформацією принципово підвернені дії завад і перешкод. Передавання бітової послідовності квантовим способом призводить до неодмінного її спотворення збоку одержувача.

З метою узгодження переданої та прийнятої послідовностей має використовуватись додатковий, не квантовий канал комунікації. У силу того, що додатковий канал не є квантовим, він має гірші показники щодо інформаційної безпеки обміну. Тому для корегування послідовностей використовуються криптографічно стійкі алгоритми.

Корегувальні протоколи описані ідеологічно, без конкретних особливостей програмної чи технічної реалізації. У рамках даної роботи робиться спроба програмної реалізації одного з таких протоколів, відомого як протокол Бенета.

Основним принципом стійкості протоколу Бенета є попереднє перемішування бітів послідовностей, узгоджене між сторонами обміну. За цією ознакою протокол можна класифікувати як стеганографічний, тобто такий, який використовує «підсвідомий» канал – можливість попереднього договору сторін щодо особливостей комунікації. Дана особливість не знижує надійність протоколу, оскільки сучасні

методи стеганографії не поступаються за стійкістю перед криптографічними, проте вимагає вибору саме стеганографічного математичного апарату і методології при практичних реалізаціях протоколу.

З метою збереження інформації щодо вихідної послідовності у програмному коді передбачається створення двох масивів: A[] – для бітів послідовності, та B[] – для перестановки. Доступ до бітів змішаної послідовності здійснюється через подвійне індексування: A[B[i]]. Зазначений прийом дозволяє оперувати як з початковою, та і зі змішаною послідовністю, а також узгоджувати одну послідовність з кількома одержувачами, кожен з яких має відмінний спосіб перестановки, введенням кількох масивів B[].

Другим кроком алгоритму є розбиття змішаної послідовності на блоки за принципом невисокої імовірності помилки у блоці. Оскільки параметри каналу заздалегідь невідомі, розбиття масиву здійснюється непрямо – шляхом його проходження за допомогою вкладених циклів з кількостями повторень N та M, які у добутку дорівнюватимуть довжині послідовності L=NM:

for(i=0;i<N;i++) for(j=0;j<M;j++) { … A[B[M*i+j]] … }

Останнім кроком є корегування парності (у кодовому розумінні) блоків розбиття з послідовним вилученням останнього біту. Визначення парності не становить програмної проблеми, а вилучення останнього біту блоку легко реалізується зміною верхньої межі вкладеного циклу.

Створена програма може знайти використання при автоматизації роботи лабораторного стенду з вивчення квантових протоколів.

Висновки. Проведено огляд схем квантової криптографії, виявлено їх переваги та недоліки,запропоновано технічні зміни задля покращення застосовуваності. Серед розглянутих схем квантової криптографії перевагу надано схемі з поляризаційним розподіленням.

Розроблено програмне забезпечення, що реалізує квантові методи для криптоаналізу класичних захищених телекомунікаційних систем;

Розроблені алгоритми сумісного використання квантових і класичних каналів;

Адаптовано створені алгоритми для використання у складі лабораторного комплексу з вивчення принципів квантової комунікації.

УДК 004.05(081)

ПРОГРАМНИЙ ЗАСІБ ФОРМУВАННЯ НЕЧІТКИХ ЕТАЛОНІВ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ МЕТОДОМ ІНТЕРВАЛЬНИХ ОЦІНОК

Автор: *А.О. Гузенко, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *М.В. Турти, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Вступ. Моделювання в інформаційній безпеці широко застосовується при дослідженні об'єктів і процесів захисту інформації. На даний час спостерігається динамічний розвиток інтелектуальних систем, розширення спектру їх функціонального призначення в галузі інформаційної безпеки. Нечіткі дані використовуються в системах ідентифікації об'єктів і процесів, в системах управління технічними засобами захисту інформації, в процедурах прийняття рішень щодо управління інформаційною безпекою. В системах розпізнавання об'єктів та ситуацій базовою процедурою є порівняння даних об'єкта і образа на основі зіставлення їх функцій належності (ФН), які можуть формуватися багатьма методами [1, 2],. Однак засоби автоматизації формування нечітких еталонів (НЕ) за деякими з них, зокрема за методом інтервальних оцінок (МІО), відсутні. Тому розробка гнучкого програмного засобу з відкритим кодом, який дозволяв би формувати і обробляти НЕ і виводити результати у зручному для користувача вигляді є актуальною задачею.

Метою даної роботи є розробка програмного модуля формування нечітких еталонів методом інтервальних оцінок для автоматизованої системи формування і обробки нечітких еталонів (АСФОНЕ).

Для досягнення поставленої мети необхідно розв'язати наступні задачі: проаналізувати сфери використання нечітких еталонів в інформаційній безпеці; визначити особливості формування НЕ методами однозначної нечіткої логіки (ОНЛ) [2]; проаналізувати форми представлення вхідної і вихідної інформації блоку формування НЕ методом інтервальних оцінок за класичною теорією (КТ) та ОНЛ у складі АСФОНЕ; розробити алгоритми визначення функцій належності (ФН)

за методом інтервальних оцінок за КТ та ОНЛ в та відповідний програмний модуль; сформулювати практичні рекомендацій щодо використання розробленого програмного модуля в інформаційній безпеці.

Основна частина. ФН, отримані МІО, можна використовувати для вибору, якщо немає чіткої межі між допустимим і недопустимим та між ідеальним і незадовільним станами. Функція належності в цьому випадку трактується як можливість твердження, що об'єкт відповідає будь-якому лінгвістичному визначенню, наприклад, "захищений". Розглядається ситуація, коли відомий зв'язок між деяким параметром X і критерієм вибору Y. Цей метод ґрунтується на припущенні того, що експерт може визначити інтервал $[y_{\min}, y_{\max}]$ значень критерію y, як відповідь на пропозицію вибрати, наприклад, "надійний" об'єкт або "захищений об'єкт".

Нехай y_x – результат вимірювання характеристики Y об'єкта, тоді $Y_{\max}$ є границею "ідеальної"області, тобто якщо $y_x > y_{\max}$, то об'єкт визнають як такий, що ідеально відповідає поняттю "захищений". Можливість такого твердження $\mu_A(x) = 1$. Тут $\tilde{A}$ – суб'єктивна подія, тобто об'єкт, з точки зору експерта, знаходиться в стані "захищений". Якщо $y_x = y_{\min}$, то $\mu_{\tilde{A}}(x) = 0$. Якщо $y_{\min} < y_x < y_{\max}$ маємо $0 < \mu_{\tilde{A}}(x) < 1$. Якщо експерт вважає, що з наближенням значення y_x до границі $y_{\max}$ можливість визнання об'єкта "захищений" лінійно зростає, то оцінку $\mu_{\tilde{A}}(x)$ знаходять за формулою:

$$\mu_{\tilde{A}}(x) = \begin{cases} 0, & \textit{якщо} \quad y_x \le y_{\min}; \\ \dfrac{y_x - y_{\min}}{y_{\max} - y_{\min}}, & \textit{якщо} \quad y_{\min} < y_x < y_{\max}; \\ 1, & \textit{якщо} \quad y_x \ge y_{\max}. \end{cases} \qquad (1)$$

Одні відповіді експерта можуть визначати лінійну модель, інші – опуклу (вгору або вниз) функцію. У будь-якому випадку наявність трьох значень функції $\mu_{\tilde{A}}(x)$ (вказане експертом, 0 і 1) дозволяє цілком відновити її в інтервалі $[y_{\min}, y_{\max}]$. Експертам пропонується оцінити $y_{\min}, y_{\max}$ і y_x в кількох точках x. Шляхом апроксимації даних отримуємо аналітичні вирази функцій, які є рівневим обмежен-

нями $y_{\min} = f_{\min}(x)$ і $y_{\max} = f_{\max}(x)$, а також $y_x = f_x(x)$, вид функцій рівневих обмежень дозволяє відобразити судження експерта з приводу характеру рівневих обмежень. Для ряду значень x за формулою (1) розраховують $\mu_{\tilde{A}}(x)$, завдяки чому можлива побудова шуканої функції належності.

Вхідні дані для цього методу отримані в результаті оцінок експертів і рівневі обмеження накладаються на кожне із значень параметра x.

Розроблений програмний модуль функціонує в діалоговому режимі і дозволяє: задавати кількість експертів, які беруть участь у формуванні НЕ; повідомляти експертам про обраний метод формування НЕ та мету опитування; визначати вагові коефіцієнти експертів рівними, або зовнішнім оцінюванням замовником еталону, або взаємною оцінкою експертів; визначати межі носія функції належності (ФН) (кількість оцінюваних точок в області визначення ФН, розмір експертного запиту) шляхом зваженої експертної оцінки; визначати бажану кількість питань і питання, що пропонуються кожним експертом для включення в експертний запит (рис.1); визначати зваженим експертним оцінюванням питання для включення в експертний запит, межу бальної оцінки питань експертного запиту, нижню та верхню (рис.1) границі оцінювання та бальну оцінку для кожного питання, включеного до експертного запиту, з точки зору достатньої відповідності НЕ, що формується; автоматично розраховувати сформовану ФН; виводити на екран дисплея результати роботи програмного модуля: кількість і координати оцінюваних точок в області визначення ФН; питання експертного запиту, шкалу оцінювання питань; інтервали оцінювання кожного питання; результати зваженої експертної оцінки всіх числових даних; повідомлення про помилки та сформований нечіткий еталон у вигляді нечіткої множини (НМ) $A^M = \{x, (\mu_A(x)); x \in X\}$.

Для забезпечення цілісності даних в модулі передбачено захист від помилок введення при: відмінності від шкали Сааті даних, що вводяться експертами при визначенні вагових коефіцієнтів експертів, при завданні кількості оцінюваних точок носія НМ, при оцінюванні питань до

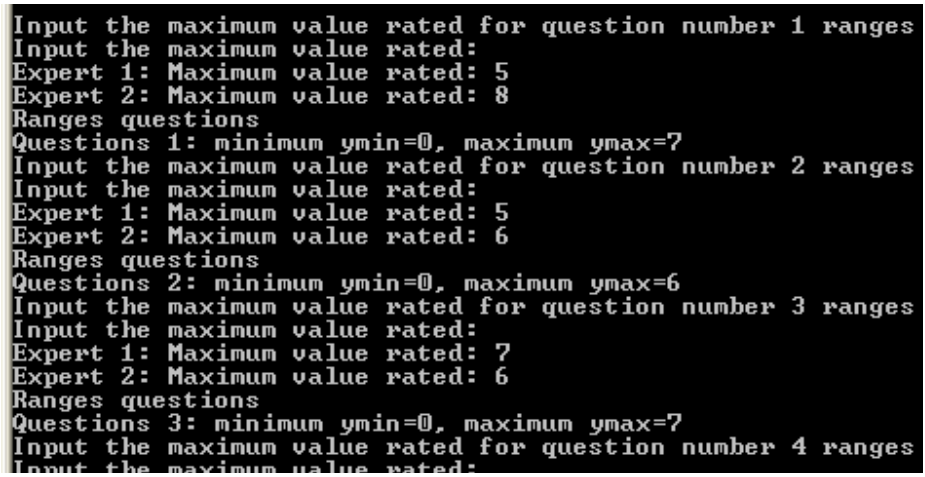


Рисунок 1 – Визначення максимальної оцінки для кожного питання експертного запиту

експертів; недотриманні відносин порядку для меж носія НМ; виходу за припустимі межі значень y_x, $y_{\min}$, $y_{\max}$ в оцінюваних точках.

ФН, отримані МІО, можуть бути нормальними і субнормальними, опуклими і неопуклими, унімодальними, полімодальними і толерантними, дискретними і непараметричними. З властивостей ФН, які можна отримати за методом МІО, випливає, що такі ФН не відповідають вимогам ОНЛ [2]. Параметризація ФН можлива за окремою процедурою, яка передбачає підбір і оцінювання якості кривої вирівнювання. Однак, це вносить додаткову похибку в суб'єктивно визначені $\mu_{\tilde{A}}(x_n)$.

Для обробки ФН, створених МІО, придатні методи узагальненої відстані Хеммінга, α -рівневої відстані і впорядкування на базі відношень. Якщо сформовані ФН виявляються нормальними, опуклими та унімодальними, то для подальшої обробки може бути застосований також метод впорядкування нечітких чисел.

Проведено верифікацію розробленого програмного модуля на тестовому прикладі [1] формування НЕ «ЗАХИЩЕНІСТЬ КОМП'ЮТЕРНОЇ СИСТЕМИ». Захищеність комп'ютерної системи визначається в [1] на підставі комплексу реалізованих превентивних

заходів захисту, що характеризується за сформованим експертним запитом з чотирьох питань, які оцінюються за шкалою 0…10 балів:

- зберігаються свіжі копії даних за межами Вашої організації?
- часто проводиться резервне копіювання даних?
- проводиться антивірусний контроль системи?
- завжди видаляються непотрібні файли?

Межі зміни діапазону шкали відповідей заданються експертом окремо для кожного компонента експертного запиту. Для зазначених питань встановлені межі дорівнюють відповідно [0;3], [0;5], [0;10], і [0;4]. Отримані експертні оцінки y_x для кожного питання складають за тестовим прикладом відповідно $y_{x1}=3$, $y_{x2}=5$, $y_{x3}=10$, $y_{x4}=4$. Розраховані МІО в [1] значення ФН за цими даними співпадають з результатами, виданими розробленим програмним модулем (рис.2).

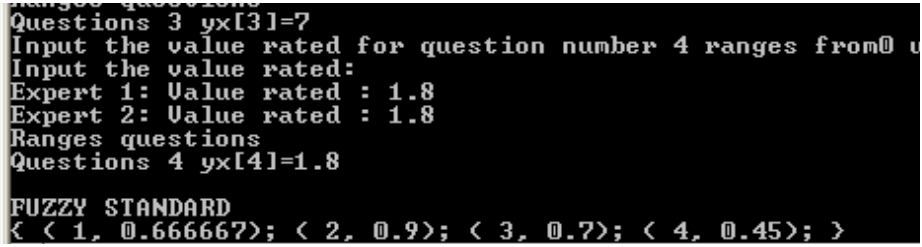


Рисунок 2 – Виведення результату за тестовим прикладом

Висновки. Таким чином, в даній роботі проаналізовані сфери використання НЕ в інформаційній безпеці, сучасні методи формування НЕ за КТ; визначені особливості формування НЕ методами ОНЛ і невідповідність МІО вимогам ОНЛ, форми представлення вхідної і вихідної інформації блоку формування НЕ МІО за у складі АСФОНЕ; розроблені алгоритми і програмний модуль визначення ФН за МІО за КТ для АСФОНЕ. Проведена апробація і успішна верифікація розробленого програмного модуля на тестовому прикладі. Перевагами методу інтервальних оцінок є можливість оцінювання об'єкта дослідження за багатьма показниками, а недоліком – специфічні процедури висновку

при порівнянні об'єкту та еталону. Програмний модуль може працювати у складі АСФОНЕ, використовуватися як окремий модуль для формування нечітких еталонів, вбудовуватися в системи розпізнавання образів або системи прийняття рішень, використовуватись на лабораторних роботах з дисциплін, пов'язаних із штучним інтелектом галузі знань 1701 «Інформаційна безпека».

Список літератури:

1. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: "МК-Пресс", 2006. – 320 с.

2. Турти М.В. Теорія однозначних нечітких систем та нейронні мережі: Монографія. Частина 1. – Миколаїв: Вид-во Європейський університет, Миколаївська філія, 2007. –140 с.

УДК 004.056.55

ПРОГРАММНЫЙ МОДУЛЬ ДЛЯ ИЗУЧЕНИЯ АЛГОРИТМА СОЗДАНИЯ ЦИФРОВОЙ ПОДПИСИ НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ

Автор: *Д.М. Емельянов, студент, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев*

Научный руководитель: *О.А. Щелконогов, ст. преподаватель, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев*

Целью работы являлось создание программного модуля для изучения принципов формирования цифровой подписи (ЦП) на основе эллиптической криптографии для лабораторного практикума по криптологии.

Актуальность темы продиктована тем, что в учебном пособии [1], которое является основным при проведении лабораторных работ по предмету «Основы криптографии и криптоанализа» отсутствуют работы по изучению алгоритмов цифровой подписи, в частности, основанные на использовании эллиптических кривых. В настоящее же время стандарты ЦП многих стран, в т.ч. Украины (ДСТУ 4145-2002), основаны на использовании эллиптических кривых.

Наиболее существенный выигрыш при использовании эллиптических алгоритмов достигается за счет уменьшения длины ключа при соизмеримой криптостойкости.

В криптографии эллиптические кривые рассматриваются над двумя типами конечных полей: простыми полями нечётной характеристики (GF(p), где p > 3 – простое число) и полями характеристики 2. В рассматриваемом программном модуле реализован алгоритм ЦП при использовании эллиптических кривых над простыми полями нечетной характеристики. Прототипом послужил известный алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm) [2].

При разработке программного модуля были созданы рабочие модели всех функций по формированию ключей, созданию подписи и ее проверки в среде MathCad (рис. 1). Сам программный модуль написан

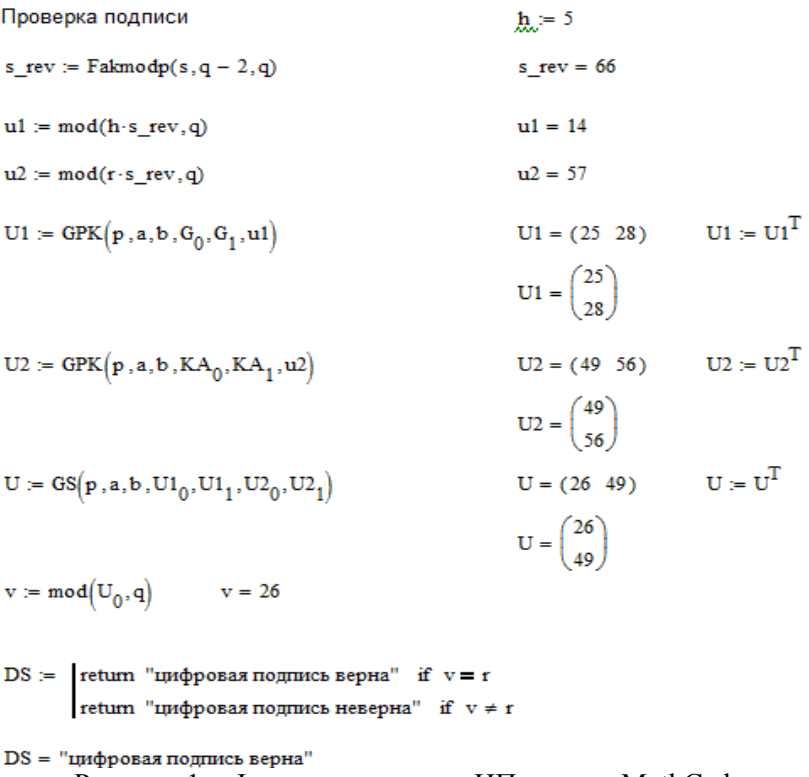


Рисунок 1 – Функция проверки ЦП в среде MathCad

на языке C++ в среде программирования Borland C++ Builder 6.0. Программа имеет простой, интуитивно понятный графический интерфейс (рис. 2). Функционально она носит учебно-демонстрационный характер и поэтому имеет ограничения (отсутствует оптимизация по быстродействию, ограничена размерность чисел, используются простые числа специального вида).

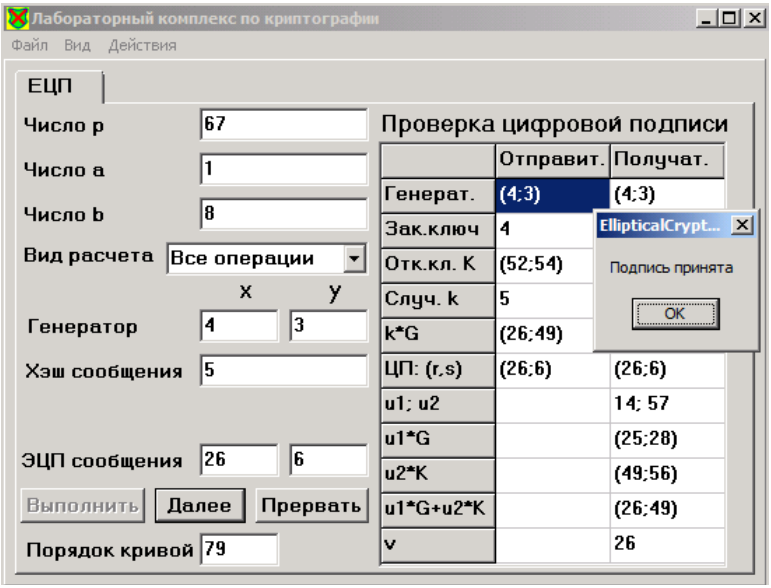


Рисунок 2 – Рабочее окно программного модуля

Выводы. В работе рассмотрен алгоритм цифровой подписи? - CDSA. Был создан программный модуль на его основе, правильность работы которого была проверена с помощью рабочей модели этого алгоритма в среде MathCad. Были разработаны методические указания для лабораторной работы с целью использования ее в учебном процессе по предмету «Основы теории криптографии и криптоанализа» для специальности 6.17010201.

Список литературы:

1. Блінцов В.С. Гальчевський Ю.Л. Практикум з криптології: Навчальний посібник. – Миколаїв: НУК, 2005. – 172 с.

2. The Elliptic Curve Digital Signature Algorithm. [Електронний ресурс] –http://cs.ucsb.edu/~koc/ccs130h/notes/ecdsa-cert.pdf.

УДК 004.056

РОЗРОБКА АЛГОРИТМУ ВИЯВЛЕННЯ МОДИФІКАЦІЇ ЦИФРОВОГО АУДІОЗАПИСУ МЕТОДОМ ФРАКТАЛЬНИХ ПЕРЕТВОРЕНЬ

Автор: *Е.Д. Заліян, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *С.М. Нужний, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Вступ. Широке застосування цифрових диктофонів, відеокамер та фотоапаратів призвело до появи нового джерела загроз для інформаційної безпеки держави, пов'язане з можливістю створення підроблених цифрових аудіо та відеозаписів і фотозображень з високим ступенем маскування слідів таких дій [1]. Це надало великі можливості для різного роду провокацій, спрямованих на деструктивні інформаційно-психологічні впливи на населення будь-якої країни шляхом, наприклад, підроблених аудіо, відеозаписів і цифрових фотографій у ЗМІ.

Поширення заяв про те, що виявити цифрову підробку неможливо, призвело до того, що піддаються сумніву будь-які цифрові матеріали, що надаються як докази.

Аналіз спеціалізованої технічної літератури показує [2,3], що фактично в кожній постанові слідчого або визначенні суду про призначення судової криміналістичної експертизи матеріалів і засобів аудіо-, відеозапису ставляться питання відносно монтажу представленої фонограми, її оригінальності, ідентифікації пристрою запису, за допомогою якого вона фіксувалася.

Автентична фонограма повинна відповідати критеріям безперервності, безпосередність запису звукових сигналів від першоджерел, одночасності запису мовних сигналів від різних джерел, дотримання тимчасової і лінійної послідовностей записів сигналу, повноти відображення мовної події. Іншими словами, фонограма автентична, якщо

вона не піддавалася змінам ні в процесі запису акустичних сигналів, ні після її фіксації на носій [1-3].

Метою даної роботи є розробка алгоритму перевірки на автентичність цифрових аудіозаписів (фонограм), які мають значну ступінь зашумлення, заснованих на їх фрактальних перетвореннях.

Основна частина. Для перевірки автентичності фонограм і записуючого пристрою застосовують вейвлетні базиси і мультимасштабний аналіз. У основу такої перевірки закладені принципи виявлення і аналізу самоподібних структур, що виділяються з сигналограми на основі використання вейвлет-перетворення, і наступного їх аналізу. При цьому в звуковому файлі спочатку виділяються паузи. Для цього використовується багатопрохідний складний алгоритм з автоматиною корекцією порогу виділення. На виділених ділянках обчислюється вейвлет-спектр сигналів, що містяться в них. Для цього застосовується операція згортки цих сигналів з вейвлетом Морле, використовуваного як базис, тобто:

$$S(f) = s(t) \otimes \psi(t) = s(t) \otimes \sqrt{\pi f_в} e^{j2\pi f_ц t} e^{\frac{t^2}{2}}$$

де $S(f)$ – вейвлет-спектр сигналів що досліджуються; $s(t)$ – сигнал що досліджується; $\psi(t)$ – вейвлет Морле; $f_в$– верхня частота перетворення; $f_ц$– центральна частота вейвлета.

Для роботи з вейвлет-портретом сигналу використовується наступний математичний апарат:

$$S_3(a,b) = \frac{a}{2\pi |a|^{\frac{1}{2}}} \int_{-\infty}^{\infty} S_3(j\omega) \Psi^*(a\omega) e^{j\omega b} d\omega =$$

$$= \frac{aA_{m1}\omega_{Д1}}{2\pi^{\frac{1}{4}} \pi |a|^{\frac{1}{2}}} \sin\frac{\omega_0 T_1}{2} \left[\sum_{k_1=-\infty}^{\infty} \frac{1}{(\omega_0 - k_1\omega_{Д1})} e^{j(\omega_0 - k_1\omega_{Д1})b} \times \right.$$

$$\left. \times \left(e^{-\frac{\left[a(\omega_0 - k_1\omega_{Д1}) - \omega_C\right]^2}{2}} - e^{-\frac{a^2(\omega_0 - k_1\omega_{Д1})^2}{2}} \cdot e^{-\frac{\omega_C^2}{2}} \right) + \right.$$

$$+\sum_{k_1=-\infty}^{\infty}\frac{1}{\left(\omega_0+k_1\omega_{Д1}\right)}e^{j\left(\omega_0+k_1\omega_{Д1}\right)b}\times$$
$$\times\left(e^{-\frac{\left[a\left(\omega_0+k_1\omega_{Д1}\right)-\omega_C\right]^2}{2}}-e^{-\frac{a^2\left(\omega_0+k_1\omega_{Д1}\right)^2}{2}}\cdot e^{-\frac{\omega_C^2}{2}}\right)\Bigg]$$

Подальша обробка зашумленого сигналу проводиться за формулою:

$$S_6(a,b)=\frac{a}{2\pi|a|^{\frac{1}{2}}}\int_{-\infty}^{\infty}S_6(j\omega)\Psi^*(a\omega)e^{j\omega b}d\omega=\frac{a\omega_{Д1}\omega_{Д2}A_{m3}}{\pi^{\frac{1}{4}}\pi|a|^{\frac{1}{2}}}\times$$
$$\times\sin\frac{\omega T_1}{2}\cdot\Bigg[\sum_{k_1=-\infty}^{\infty}\sum_{k_2=-\infty}^{\infty}\frac{\sin\left(\frac{\omega_0+k_1\omega_{Д1}}{2}\right)T_2}{\left(\omega_0+k_1\omega_{Д1}+k_2\omega_{Д2}\right)}\times\frac{1}{\left(\omega_0+k_1\omega_{Д1}\right)}\times$$
$$\times\left(e^{-\frac{\left[a\left(\omega_0+k_1\omega_{Д1}+k_2\omega_{Д2}\right)-\omega_C\right]^2}{2}}-e^{-\frac{a\left(\omega_0+k_1\omega_{Д1}+k_2\omega_{Д2}\right)^2}{2}}\cdot e^{-\frac{\omega_C^2}{2}}\right)\times$$
$$\times e^{jb\left(\omega_0+k_1\omega_{Д1}+k_2\omega_{Д2}\right)}+\sum_{k_1=-\infty}^{\infty}\sum_{k_2=-\infty}^{\infty}\frac{\sin\left(\frac{\omega_0-k_1\omega_{Д1}}{2}\right)T_2}{\left(\omega_0-k_1\omega_{Д1}-k_2\omega_{Д2}\right)}\times$$
$$\times\frac{1}{\left(\omega_0-k_1\omega_{Д1}-2k_2\omega_{Д2}\right)}\cdot\sin\frac{\left(\omega_0-2k_2\omega_{Д2}\right)T_1}{2}\times$$

$$\times\left(e^{-\frac{\left[a\left(\omega_0-k_1\omega_{Д1}-k_2\omega_{Д2}\right)-\omega_C\right]^2}{2}}-e^{-\frac{a\left(\omega_0-k_1\omega_{Д1}-k_2\omega_{Д2}\right)^2}{2}}\cdot e^{-\frac{\omega_C^2}{2}}\right)\times$$

$$\times e^{jb\left(\omega_0-k_1\omega_{Д1}-k_2\omega_{Д2}\right)}\Big]$$

На базі проаналізованого матеріалу було проведено вейвлет-перетворення очищеного від шуму аудіо сигналу. Результати порівняння результатів очищення методами фільтрації та вейвлет-перетворення приведені на рис.1. На графіку синім кольором (лінія 1) позначено первинний сигнал, який є зашумленим, зеленим (лінія 2) – сигнал, який був ощиреним за допомогою звичайних фільтрів, червоним (лінія 3) – сигнал, що був очищений від шумів за допомогою вейвлет-перетворень.

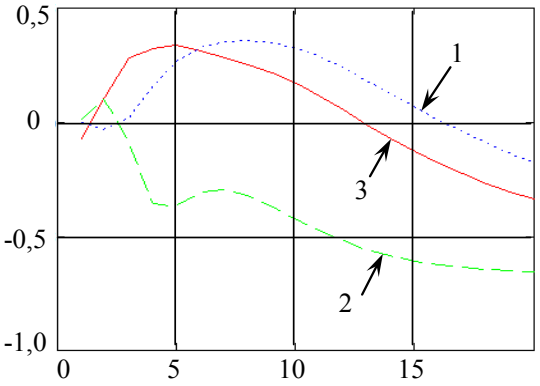


Рисунок 1 – Порівняння методів очистки сигналу від шумів

Було доведено, що фрактальні перетворення здатні з великою вірогідністю виявляти модифікацію цифрового аудіозапису після їх вейвлетної очистки.

Висновки

На підставі теоретичних та практичних досліджень запропоновано алгоритм фонескопічних досліджень зашумлених цифрових аудіозаписів

з метою визначення їх автентичності та показано, що використання вейвлет-перетворення для очистки сигналу від сторонніх шумів дає значно якісніші результати, в порівнянні зі звичайними методами очищення.

Список літератури:

1. *Бєлкін Р.С.* Курс криміналістики / Р. С. Бєлкін. – М., 1997. – Т. 1. – 387 с.

2. *Рибальский О.В.* Автентичність сигналограмм //О.В. Рибальский// Вісник Державного університету інформаційно – комунікаційних технологій. – К., 2006, № 4, т. 4. – С. 259 – 262.

3. *Рибальський О.В.* Застосування вейвлет- аналізу для виявлення слідів цифрової обробки аналогових і цифрових фонограм у судово- акустичній експертизі / О. В. Рибальський. – К.: НАВСУ, 2004. – 167 с.

УДК 004.056:534.212:53.086.6

УДОСКОНАЛЕННЯ ЛАБОРАТОРНОГО СТЕНДУ З ДОСЛІДЖЕННЯ ПРОСТОРОВОГО РОЗПОДІЛУ ВІБРАЦІЙ

Автор: *О.А. Захарченко, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *Д.М. Самойленко, к.ф.-м..н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв / Збройні Сили України*

Віброакустичний канал є одним з основних для розповсюдження, у тому числі і витоку мовної інформації. Знайомство з принципами утворення та поширення вібраційних хвиль, а також методами розвідки та захисту віброакустичного каналу є неодмінними задачами при підготовці фахівців з інформаційної безпеки.

У роботі [1] запропоновано схему стенда для дослідження поверхневих вібрацій. За допомогою стенду було виявлено ряд особливостей, зокрема утворення стійких інтерференційних картин у малих резонаторах. У той же час головними недоліками розробленого стенду є мале співвідношення сигнал/шум (на рівні 2-3 дБ) та можливість отримання сигналу тільки з одного точкового п’єзодатчику.

Підвищення чутливості та збільшення співвідношення сигнал шум (SNR) повинно підвищити точність вимірів вібраційної картини, яка знімається за допомогою стенду, що дозволить проводити дослідження у матеріалах з високим показником загасання поверхневих хвиль. Збільшення кількості датчиків до двох дає змогу одночасно проводити дослідження розповсюдження вібрації у різних точках об'єкту, що надасть можливість розрізнювати, корисний сигнал і шум через кореляційний аналіз даних від датчиків.

Головною причиною малого SNR можна вважати особливості будови вібродатчика. Виготовлений з п'єзоелектрика датчик має високий внутрішній опір (сотні МОм), і утворює корисний сигнал у вигляді незкомпенсованої статичної напруги. Для типових режимів роботи стенду напруга на датчику не перевищує 20 мВ. За таких умов електромагнітні наведення на кабель стають порівняними з корисним сигналом.

Покращення SNR, відповідно, потребує виготовлення активного датчика на основі пасивного п'єзоелементу. Принципова електрична схема активної частини датчика наведена на рис. 1. Високий внутрішній опір п'єзоелементу обмежує вибір елементної бази першого підсилювального каскаду польовим транзистором або диференціальним підсилювачем з високоомним входом [2]. Останньому надано перевагу в силу простоти та універсальності.

Слід зазначити, що п'єзоелемент є дуже чутливим до ударів. Торкання датчиком твердої поверхні, що досліджується, може спровокувати стрибок напруги у десятки вольт. Для захисту перших підсилювальних каскадів використано обмежувач напруги, який складено з двох напівпровідникових діодів, (D1,D2) включених у зустрічних напрямках. У відповідності до ВАХ н/п діодів запропонована ланка пропускатиме без змін сигнали з напругою до 0,5-0,6 В і відсікатиме більші. З урахуванням того, що п'єзоелемент не видає великих струмів, вимоги до потужності діодів є мінімальними.

Роздільний конденсатор С1 використовується для відсікання постійної складової. Резистор R3 введено для запобігання самозбудження підсилювача через великий вхідний опір джерела сигналу.

Первинний каскад підсилювача виконано за схемою повторювача (підсилювача струму). Другий каскад – за класичною схемою неінвертуючого підсилювача. Резистори R1,R2 задають коефіцієнт підсилен-

ня. Для забезпечення стабільної роботи коефіцієнт підсилення обраний на рівні 15-20 дБ.

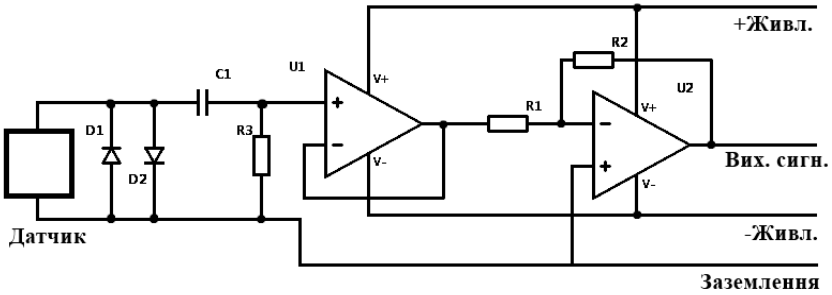


Рисунок 1 – Схема що пропонується для використання в якості підсилювача сигналу.

Випробування датчика, виготовленого за запропонованою схемою, дозволило одержати SNR ні рівні 20 дБ, що на 17-18 дБ краще за попередні результати.

У якості перспектив подальших досліджень у обраному напрямку можна відзначити заходи із додаткового покращення SNR шляхом накопичення та усереднення корисного сигналу, а так впровадження АЦП для можливості цифрової обробки та спрощеної трансляції даних до ЕОМ.

Список літератури:

1. Петухов І. Стенд для дослідження поверхневих вібраційних резонансів. [Текст] / І.В. Петухов; Д.М. Самойленко // Матеріали всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». – Миколаїв: НУК, 2013. – С.169-170.

2. Титце У., Шенк К. Полупроводниковая схемотехника. Том I /Пер. с нем. – М.: ДМК Пресс, 2008. – 832 с.

УДК 004.056

АНАЛИЗ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СОЦИАЛЬНЫХ СЕТЯХ

Автор: *А.Н. Клочко, студент, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев*

Научный руководитель: *М.В. Турты, к.т.н., доц., Национальный университет кораблестроения имени адмирала Макарова, г. Николаев*

Введение. Социальная сеть сейчас является бесценным источником персональных данных абсолютного большинства людей. Особенностью социальных сетей является то, что пользователь добровольно указывает все необходимые персональные данные. Персональные данные подлежат защите, согласно [1], однако вопрос о достаточной защищенности персональных данных в социальных сетях на данный момент является недостаточно изученным.

Целью данной работы является анализ уязвимостей социальной сети ВКонтакте с точки зрения защищенности персональных данных**.**

Не смотря на то, что за конечным пользователем остается право выбора данных, которые он укажет на сайте при регистрации, структура социальных сетей подобрана таким образом, что бы мотивировать человека не только заполнить все пункты при регистрации, но и указывать достоверную информацию о себе. Осуществляется это за счет предложения пользователям определенной функциональности, для корректной работы которой необходимы точные сведенья о возрасте, месте учебы, работы и т.д. Эти и другие данные используются социальной сетью для составления вероятных списков друзей и знакомств, поиска одноклассников, однокурсников и коллег. С учетом расширения интеграций различных социальных сетей и мессенджеров между собой, в конечном счете, интернет-ресурсы получают сведения о человеке, о круге его знакомств. В качестве примера можно привести расширения для браузера Google Chrome под названием VK Messages Visual Statistics [2].

Как видно из графиков рис.1-3, социальные сети содержат огромное количество приватной информации о пользователе. Естественно, одной из основных задач, которые возникают перед администрацией социальной сети, является защита данных пользователя от несанкционированного доступа.

Дополнительной сложностью в вопросе о защите информации в социальной сети является классическая схема компромисса между информационной безопасностью и функциональностью социальной сети.

Рисунок 1 – Статистика сообщений ВКонтакте

Рисунок 2 – Графики сообщений за последние 24 часа

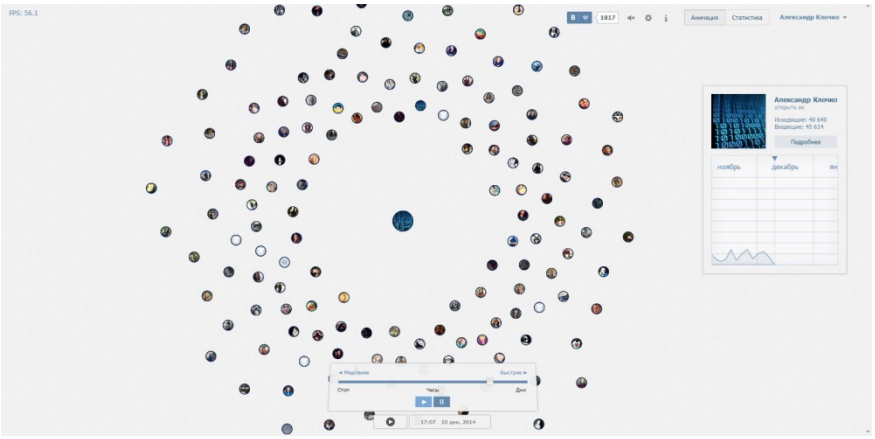


Рисунок 3 – Визуализация переписок ВКонтакте

Одной из наиболее популярных социальных сетей является сеть ВКонтакте. В результате проведенных исследований была выявлена уязвимость в системе параметрического поиска пользователей, при помощи которой был получен доступ к дате рождения и семейному положению пользователей независимо от заданных пользователями настроек приватности.

Как показал проведенный анализ, причиной наличия данной уязвимости является организация процедур защиты и поиска персональных данных в сети, Скрипт параметрического поиска имеет доступ к полям базы данных, в которых хранятся вышеуказанные данные без учета настроек приватности. Ключевым условием для успешной эксплуатации уязвимости является сбор достаточного количества информации для идентификации пользователя в диапазоне 1...20 возвращаемых скриптом значений. Пользователь с нужным id-номером будет отображаться в списке возвращаемых результатов поиска при условии, если данные указанные пользователем в своем профиле совпадут с данными переданными поисковому скрипту. Перебирая все значения даты рождения и семейного положения, анализируя результаты скрипта поиска, можно получить скрытые данные пользователя. Изучения платформы vk api с целью автоматизировать процесс эксплуатации уязвимости выявил еще ряд уязвимостей системы безопасности ВКон-

такте. В настройках приватности есть возможность ограничить аудиторию людей, которые могут просматривать пользовательский профиль. Так же эти ограничения касаются индексации профиля поисковыми ботами (рис.4).

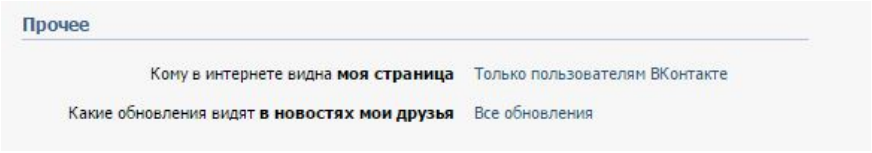


Рисунок 4 – Настройка видимости профиля

При указанных как на рис.4 настройках профиля страница пользователя для не авторизованного пользователя будет иметь вид рис.5

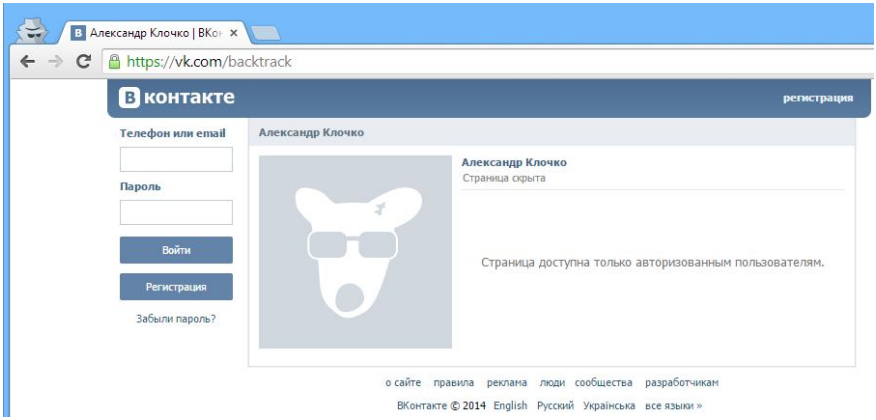


Рисунок 5 – Страница пользователя, чей профиль защищен настройками приватности

Тем не менее, используя средства api VKontakte базовые сведенья о пользователе все-таки получить удалось.

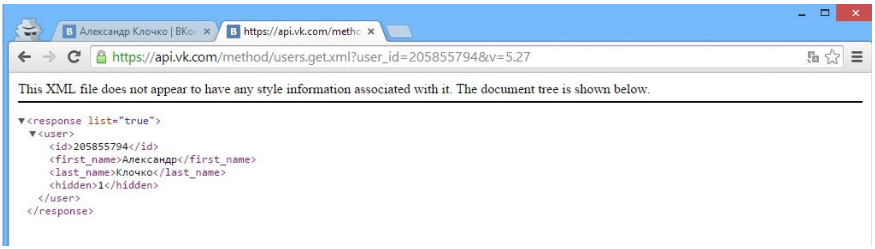


Рисунок 6 – VK API. Работа со скрытым профилем

Выводы. В работе проанализирована защищенность персональных данных в социальной сети ВКонтакте. Выявлены ряд уязвимостей, в том числе уязвимости, которые могут быть использованы злоумышленником для несанкционированного доступа к персональным данным пользователя, в том числе в автоматизированном режиме. Полученные выводы подтверждены в процессе эксплуатации разработанного программного обеспечения.

Список литературы:

1. Закон України «Про захист персональних даних», від 01.06.2010 № 2297-VI.
2. http://vk.cc/3fTVMT

УДК 004.056.55

ПРОГРАМНИЙ МОДУЛЬ ДЛЯ ВИВЧЕННЯ АЛГОРИТМІВ СТИСНЕННЯ ЗОБРАЖЕНЬ

Автор: *Р.М. Ларін, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *О.О. Щелконогов, ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Метою роботи є створення програмного модуля для вивчення алгоритмів стиснення зображень для лабораторного практикума по криптологии.

Актуальність роботи забезпечується зростаючим використанням передачі мультимедійної інформації через глобальну мережу, підвищенням ефективності роботи обчислювальних машин і як наслідок появою нових алгоритмів стиску, а також відсутністю доступного програмного забезпечення для цілей навчання.

Класичними алгоритмами стиснення вважаються алгоритми стиснення без втрат (алгоритм Хаффмана, алгоритм RLE, LZW), а також алгоритми стиснення з втратами (фрактальний алгоритм стиснення, алгоритм wavelet, алгоритм JPEG). Блок-схема алгоритму стиснення JPEG, за якою реалізовувалась програма наведена на рисунку 1.

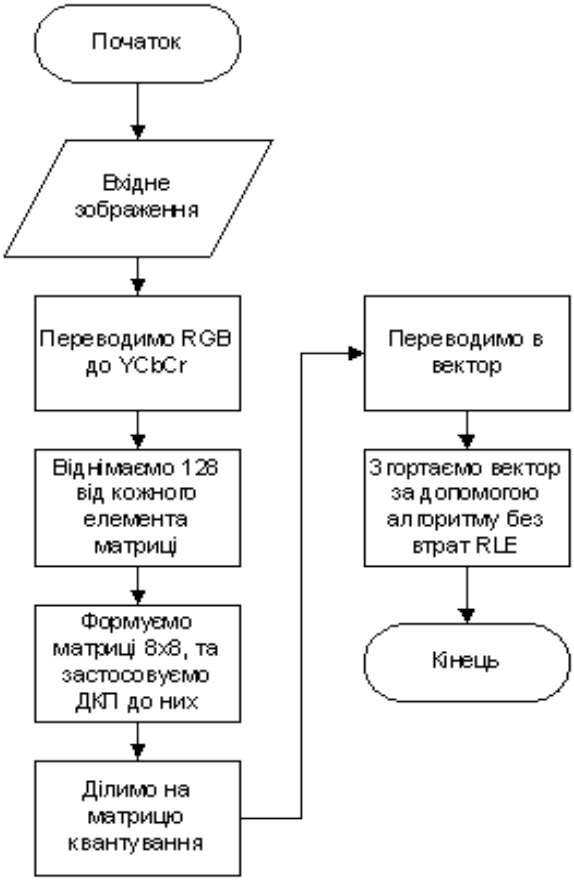


Рисунок 1 – Блок-схема алгоритму стиснення JPEG

JPEG – один з найновіших і досить потужних алгоритмів. Практично він є стандартом де-факто для повнокольорових зображень. Оперує алгоритм областями 8x8, на яких яскравість і колір змінюються порівняно плавно. Внаслідок цього, при розкладанні матриці такої області в подвійний ряд по косинусам значущими виявляються тільки перші коефіцієнти. Таким чином, стиснення в JPEG здійснюється за рахунок плавності зміни кольорів.

ДКП розкладає зображення по амплітудах деяких частот. Таким чином, при перетворенні ми отримуємо матрицю , в якій багато коефіцієнти або близькі , або рівні нулю.

Для цього використовується квантування коефіцієнтів. У самому простому випадку – це арифметичний побітовий зрушення вправо. При цьому перетворенні втрачається частина інформації , але можуть досягатися великі коефіцієнти стиснення.

Інтерфейс програми розробленої в ході дипломної роботи зображений на рисунку 2.

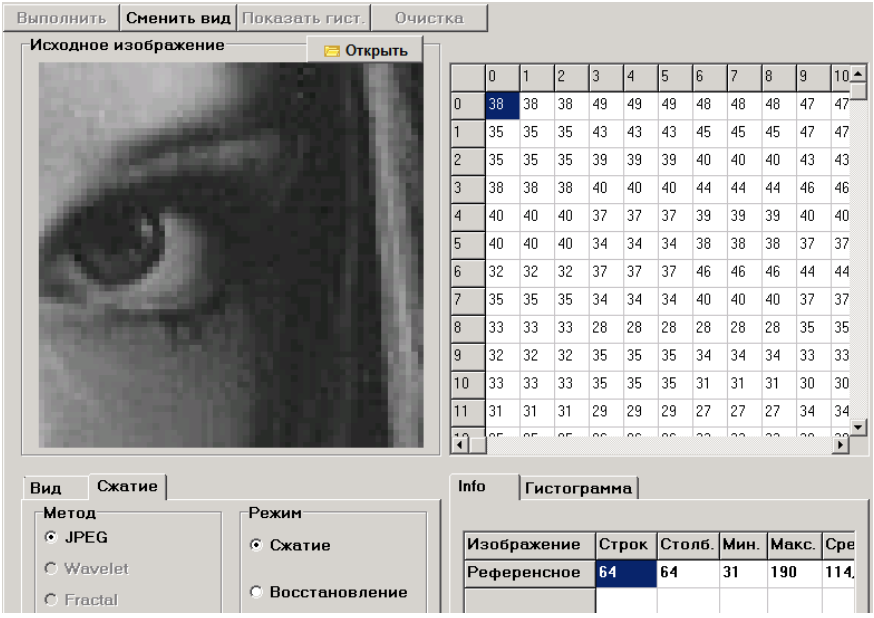


Рисунок 2 – Робоче вікно програми

Висновки

На основі опису обраного методу алгоритмів стиснення були розроблені алгоритми програмного модуля.

На основі розроблених алгоритмів був створений програмний модуль для вивчення алгоритму стиснення зображення. Правильність роботи програми була верифікована розрахунками на калькуляторі і у програмі MathCad.

Розроблене програмне забезпечення може бути використане в навчальному процесі по предмету «Цифрова обробка сигналів» для спеціальності 7.17010201 „Системи технічного захисту інформації, автоматизація її обробки".

УДК 004.056

ФОРМУВАННЯ НЕЧІТКИХ ЕТАЛОНІВ АТАК В КОМП'ЮТЕРНІЙ МЕРЕЖІ МЕТОДОМ ПОБУДОВИ ЕКСПОНЕНЦІЙНОЇ ФУНКЦІЇ

Автор: *О.М. Мильченко, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *М.В. Турти, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Вступ. Розробкою методів і методик захисту інформації на основі процедур обробки нечітких даних займаються багато вітчизняних і зарубіжних науковців, в тому числі в Національному університеті кораблебудування [1-6]. Однак на даний час відсутні рекомендації щодо доцільних методів формування НЕ для вирішення конкретних прикладних задач. Першим кроком до розробки таких рекомендацій є аналіз типових задач інформаційної безпеки, що вирішуються з використанням НЕ, і послідовне дослідження ефективності різних методів формування НЕ з точки зору тривалості і використовуваних ресурсів як для процедур формування НЕ, так і для їх подальшої обробки.

Нечіткі системи широко використовуються в інформаційній безпеці використовуються як системи ідентифікації, навігації, управлін-

ня, систем виявлення уразливостей в початкових кодах тощо, внаслідок зручності врахування числових та якісних факторів, в тому числі визначених експертом на інтуїтивному рівні. Для складання системи індитифікації віддалених атак можна використати їх ознаки, які є нечіткими еталонами (НЕ).

Метою даної роботи є формування нечітких еталонів атак в комп'ютерній мережі методом побудови експоненційної функції для інтегрального програмного засобу формування і обробки нечітких еталонів.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

визначити ознаки сучасних атак в комп'ютерних мережах;

визначити ознаки сучасних атак в комп'ютерних мережах, для яких можуть бути побудовані нечіткі еталони;

визначити доцільність формування нечітких еталонів ознаки сучасних атак в комп'ютерних мережах методом експоненційної функції (МЕФ) за класичною теорією і ОНЛ;

побудувати НЕ атак в комп'ютерній мережі за допомогою МЕФ.

Основна частина. Обрані для моніторингу ознаки наведені в [4], звідки випливає, що НЕ атак в комп'ютерних мережах можуть бути представлені у вигляді нечітких чисел (НЧ), лінгвістичних змінних (ЛЗ) і правил. Найпростішим є НЕ у вигляді НЧ, для побудови якого можна безпосередньо застосовувати розроблений програмний блок автоматизованої системи формування і обробки НЕ (АСФОНЕ), описаний в [1]. Ідентифікація атаки в цьому випадку здійснюється процедурами порівняння нечітких множин (НМ), наявними в блоці обробки НЕ АСФОНЕ. Для НЕ у вигляді лінгвістичних змінних наявні декілька НЧ на одному універсумі, тому в цьому випадку формування НЕ передбачає багаторазове використання системи з різними вхідними даними. Якщо ідентифікація атаки здійснюється за певним правилом, то додатково потрібно задіювати в процесі моніторингу блок побудови правил та логічного висновку за правилами, які можуть використовувати порівняння різних термів ЛЗ, що є НЧ, представленими в АСФОНЕ у вигляді НМ.

Виявлення факту того, що порти системи піддаються, наприклад, скануванню, може базуватися на аналізі мережного трафіку і порівняння кількості і відносного віку життя віртуальних каналів з еталонними значеннями.

За допомогою розробленого програмного блоку [5], що реалізує МЕФ, отримані НЕ для термів лінгвістичних змінних «кількість віртуальних каналів» КВК=={«дуже мала» (ДМ) «мала» (М) «середня» (С) «велика» (В) «дуже велика» (ДВ)} (рис.1 – 3), «відносний вік віртуального каналу» ВВК=={«малий» (М) «середній» (С) «великий» (В)} (рис.2), що дозволяють ідентифікувати сканування портів в мережі і підміну одного із суб'єктів TCP-з'єднання в мережі Internet.

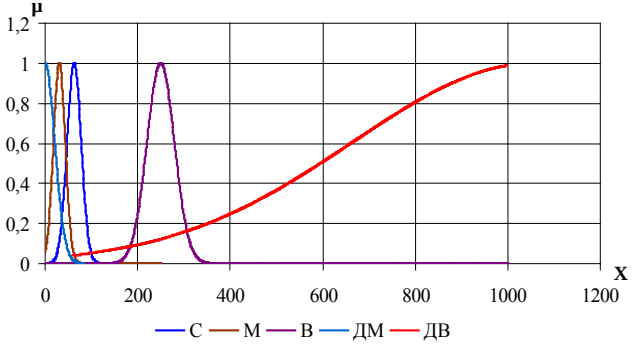


Рисунок 1 – Еталон КВК за КТ

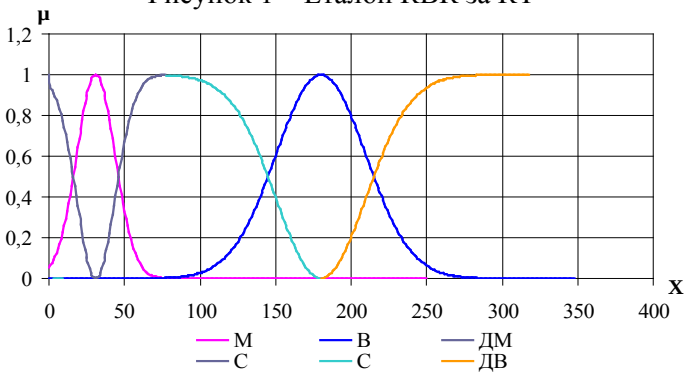


Рисунок 2 – Еталон КВК за ОНЛ, сформований методом парних термів

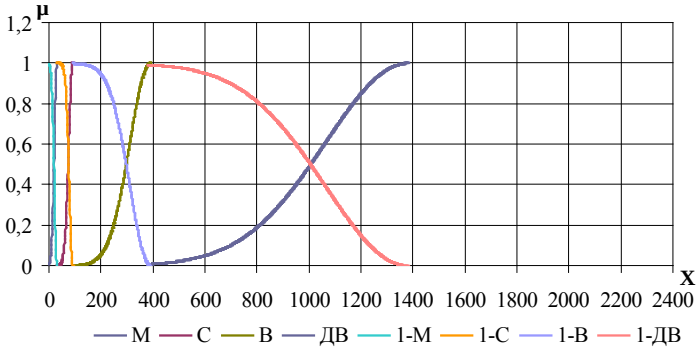


Рисунок 3 – Еталон КВК за ОНЛ, сформований методом зростаючих ділянок

НЕ КВК було сформовано у відповідності до класичної теорії [1] та до теорії однозначної нечіткої логіки [6] (методом парних термів (рис.2) та методом зростаючих ділянок термів (рис.3)).

Розроблена система правил для виявлення сканування портів, підміни одного із суб'єктів TCP-з'єднання в мережі Internet, Ping of deadth, SYN flooding adth, Smurf.

Висновки. В результаті аналізу сучасних методів атак на комп'ютерні мережі були визначені ознаки сучасних віддалених придатні для моніторингу атак. Показана непридатність ознак, за якими проводиться класифікація віддалених атак, для моніторингу атак. Показано, що перевагою застосування параметричних НЕ, побудованих із застосуванням експоненційної функції є можливість спрощення деяких процедур обробки НЕ, зокрема тих з них, що пов'язані із визначенням α –рівневих множин, оскільки вони можуть бути визначені автоматично, а не в процесі експертного опитування. Це дозволяє реалізувати адаптовну систему, яка працює в режимі реального часу. Доведено, що логічна умова $\sum_{i=1}^{5}\mu(x_i)=1$ у відповідності з ОНЛ не порушується і графіки ФН отримуються з мінімальною похибкою параметризації при використанні методу зростаючих термів ОНЛ порівняно з класичним методом ЕФ та методом парних термів ОНЛ

при побудові ФН НЧ, які не є симетричними відносно вертикальної вісі, проведеної в точці, що відповідає максимуму ФН. Розроблені НЕ та система правил для виявлення наступних видів атак: підміна одного із суб'єктів *TCP*-з'єднання в мережі *Internet, Ping of deadth, SYN flooding adth, Smurf*, сканування портів.

Розроблений програмний блок може використовуватися як окремий модуль, або вбудовуватися в АСФОНЕ чи в системи ідентифікації, навігації, управління, системи виявлення уразливостей в початкових кодах, системи оцінювання ефективності захисту інформації.

Список літератури:

1. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: "МК-Пресс", 2006. – 320 с.
2. Крищук А.Ф Мультиагентний метод діагностування комп'ютерних систем на наявність ботнет-мереж, [Електронний ресурс]. – http://lib.khnu.km. ua:8080/jspui/handle/123456789/83
3. Мігунов В.О. Програма обробки нечітких еталонів //Матеріали Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».-Миколаїв: НУК, 2011. – С.97-101.
4. Мильченко О.М. Формування нечітких атак в компю'терних мережах методом побудови експоненційної функції // Всеукраїнський форум молодих науковців «Макарівські читання-2014».- Миколаїв: НУК, 2013. – С.61.
5. Мильченко О.М. Програмний засіб формування нечітких еталонів в інформаційній безпеці методом побудови експоненційної функції //Матеріали ІІІ Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».-Миколаїв: НУК, 2013. – С.187-193.
6. Турти М.В. Теорія однозначних нечітких систем та нейронні мережі: Монографія. Частина 1. – Миколаїв: Вид-во Європейський університет, Миколаївська філія, 2007. –140 с.

УДК 004.056

РОЗРОБКА МЕТОДИКИ АНАЛІЗУ ГАУСОВИХ ШУМІВ В ЦИФРОВОМУ АУДІОЗАПИСУ ДЛЯ ВИЯВЛЕННЯ ОЗНАК МОДИФІКАЦІЇ ФОНОГРАМИ

Автор: *А.В. Михайлуца, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *С.М. Нужний, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Вступ. Розвиток і широке поширення комп'ютерних засобів обробки й монтажу цифрових записів, доступність детальної інформації про виконання таких дій на сьогоднішній день привели до ситуації, коли створення підробленої фонограми може виявитися простим завданням навіть для непрофесіонала. Саме тому вдосконалювання методик експертної оцінки автентичності цифрових записів є надзвичайно важливим науково-технічним і соціальним завданням [1,2].

Основна частина. Не підлягає сумніву важлива роль звукозаписів в профілактиці й розкритті злочинів. Але також відомо, щоб фонограма стала доказом у справі, не повинне бути сумнівів у її автентичності.

Метою розробки є вдосконалення алгоритму дослідження звукозаписів (фонограм), на основі методики аналізу гаусових шумів, для виявлення ознак їх модифікації.

Запропонований алгоритм призначений для використання в криміналістичних дослідженнях цифрових аудіофайлів (фонограм) з метою встановлення їх автентичності технічним засобам, на яких проводився первинний запис фонограм [1].

Висновки. Була розглянута можливість визначення факту несанкціонованого втручання (модифікації) цифрових фонограм методом контролю гаусових шумів та показано, що існуючі методики не задовольняють в повній мірі вимогам по однозначності ідентифікації наявності таких впливів, що обґрунтовує необхідність проведення додаткових досліджень; в роботі запропоновано використання віконного перетворення, як методу виявлення особливо небезпечних місць монтажу – пауз в розмові дикторів. Для їх виявлення рекомендується використання віконних перетворень Gaussian 10 та Rectangular

Список літератури:

1. *Бєлкін Р.С.* Курс криміналістики / Р. С. Бєлкін. – М., 1997. – Т. 1. – 387 с.
2. *Рибальский О.В.* Автентичність сигналограмм //О.В. Рибальский// Вісник Державного університету інформаційно – комунікаційних технологій. – К., 2006, № 4, т. 4. – С. 259 – 262.

УДК 003.26

ЦИФРОВІ ВОДЯНІ ЗНАКИ У ЗАСТОСУВАННІ ДО АУДІКОНТЕЙНЕРІВ

Автор: *К.М. Новосьолова, студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *Д.М. Самойленко, к.ф.-м..н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв / Збройні Сили України*

Сучасна стеганографія об'єднує у собі сукупність методів, які ґрунтуються на принципах приховування інформації, вираженої у термінах комп'ютерних та телекомунікаційних технологій. Зі зростанням популярності та швидким розвитком цифрових технологій у всіх галузях діяльності, високої актуальності набуває проблема захисту інформації, зокрема, проблема підтвердження автентичності цифрового твору. Більшість відомих стеганографічних методів можна класифікувати за ознаками, показаними представленими у роботі [1]. Апробована раніше методика внесення стегоінфорамації у текстові складові частини інформаційного ресурсу, для підтвердження його автентичності передбачає використання саме методу знаків однакової форми як найбільш ємнісний і такий, що не змінює форматування при масштабуваннях сторінки.

Для підвищення ступеня захисту інформаційних ресурсів варто періодично змінювати зміст стеганографічного повідомлення. Пропонується використання дати і часу в якості змісту стеганографічної інформації.

Для різних методів представлення дати і часу була розрахована мінімальна бітова довжина приховуваного повідомлення. Для розрахунку оптимальної довжини динамічного стегоконтейнера був проведений ана-

ліз частот літер української абетки. Збереженість природних значень частот забезпечить додаткову прихованість та камуфлювання стегоінформації. Результати показують, що максимальну ємність матиме стегоконтейнер з заміною декількох символів української абетки одночасно. Мінімальна довжина стекогонтейнеру становить 113 літер, що дозволяє використовувати метод для ресурсів з незначним текстовим наповненням.

Основним завданням автентифікації, як послуги безпеки, є розмежування прав доступу до інформації різних користувачів одного інформаційного ресурсу, а тому, основним показником надійності системи виступає імовірність атаки з успішним несанкціонованим доступом.

Особливу небезпеку становлять атаки підміни. Подібні атаки полягають у спробі підміни стегоінформації за результатами аналізу декількох перехоплених повідомлень.

Теоретико-інформаційні обмеження на імовірність атаки успішного вторгнення розвинені у роботі [2] і відомі як межа Сіммонса. Згідно з зазначеними обмеженнями імовірність успішної атаки задовольняє нерівність

$$\log_2 P_d \geq H(MES) - H(E) - H(M), \qquad (1)$$

де P_d – імовірність успішної атаки (deceived probability).

Результати адаптування методу оцінки імовірності вторгнення до текстової стегосистеми становлять: мінімальна бітова довжини методу (32 біти) обумовлює найгірший випадок, максимальна (256 біт), відповідно, визначає найкращий варіант.

Числові величини матимуть наступний вигляд:

– найгірша імовірність успішної атаки на стегосистему становить $P_{d,\max}=3{,}9\cdot10^{-11}$ (близько 4-х успіхів на 100 мільйардів спроб),

– найкраща $P_{d,\min}=10^{-78}$ порівняна з криптографічною стійкістю.

При атаках підміни значення ентропій становлять:

– найгірша імовірність $P_{d,\max}=0{,}03$ (1 успіх на 30 спроб),

– найкраща $P_{d,\min}=9\cdot10^{-78}$ збільшується майже на порядок, проте залишається достатньо малою.

Зменшення стійкості до атак підміни пов’язане з особливостями методів представлення дати та часу, тому для покращення надійності слід призвести усі способи перетворення до однакової бітової довжини (прийомами урізання чи додавання «солі») а також використати

прийоми «перемішування», які широко застосовуються у криптографії, наприклад, за допомогою SP-мереж чи мереж Фейстеля.

Успішно апробована методика внесення цифрових водяних знаків у текстові контейнери [3] може бути адаптована для використання в аудіо файлах. Слід зазначити, що методи інтервенції стего у аудіо файли досить широко вивчаються у зв'язку з захистом авторських прав та судових експертиз з підтвердження автентичності аудіо запису, створеного конкретним цифровим пристроєм, в основному диктофонного типу.

Приховування інформації у звукових файлах базується на обмеженнях психофізичного сприйняття звуку. Різні методики використовують різні особливості внесення стего, які для окремих задач мають позитивний ефект, для решти – негативний.

Серед вимог, які стосуються вибору методики виділяються наступні: 1) робота з окремим відліком, 4) відсутність впливу на спектральні характеристики (у даному контексті мова іде про сам метод), 5) однозначність, 6) прихованість від людини та технічних засобів, 7) обчислювальна складність.За результатами аналізу кожного з методів на відповідність виділеним вимогам до САЦВЗ було складено табл. 1.

Таблиця 1 – Порівняльна характеристика методів аудіо стеганографії

Метод	Задоволення вимоги				
	1)	4)	5)	6)	7)
1. Із збереженням гістограми контейнера	–	+	+	+	–
2.Кодування найменших значущих біт	+	+	+	+	+
3. Метод розширення спектру	+	–	+	+	+
4. Використання ехо-сигналу	–	–	+[1]	+[2]	–
5 Модифікація фази	–	–	+[1]	+[2]	–
6 Методи маскування	–	–	+[1]	+[2]	–

Примітки: [1] – за вірної синхронізації; [2] – лише від людини

Як випливає з табл. 1 найоптимальнішим для поставленої задачі є метод кодування найменших значущих біт. Головними перевагами над іншими методами виступили його простота, можливість роботи з одиночними відліками та відсутність принципових спотворень статистичних та спектральних характеристик контейнера.

Решту вимог до САЦВЗ має задовольнити спосіб формування стегопослідовності. Вимоги 4) та 8) можна вважати ключовими для обґрунтування вибору криптографічних методів створення стего. Вимога забезпечення статистично рівномірного розподілу може бути задоволена вибором крипто примітиву – хеш функції. Такі функції передбачають відсутність будь-яких кореляцій у генерованих бітах, що цілком еквівалентно вимозі 4).

Велика увага приділяється вимозі забезпечення статистично рівномірного розподілу, яка може бути задоволена вибором крипто примітиву – хеш функції. Такі функції передбачають відсутність будь-яких кореляцій у генерованих бітах.

Схема формування стегопослідовності може бути подана наступним чином:

на початку запису генератор стего (ГС) ініціалізується значенням дати, часу та унікального ідентифікатора пристрою (УІП);

вхідні аудіо дані (відлік АЦП) подаються на обробку, яка встановлює останній біт відліку відповідно до значення ГС, результат оброблення зберігається як A_i;

ГС повторює ініціалізацію з використанням A_i (замість часу) та УІП;

кроки 2-3 повторюються упродовж всього запису аудіо.

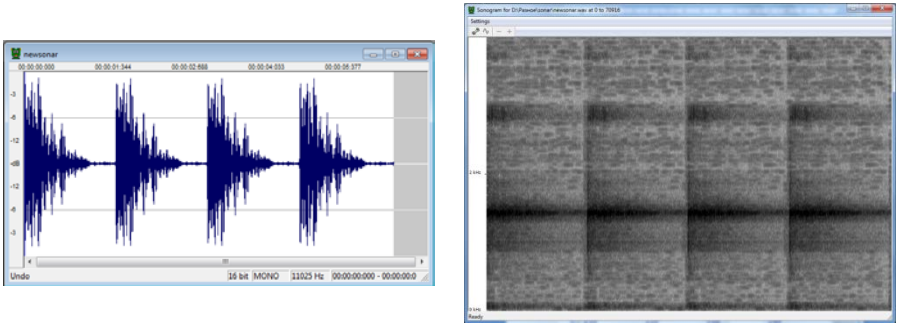
У якості процедури ініціалізації та встановлення стану ГС слід використати обчислення хеш-образу від суперпозиції даних ініціалізації. Вибір хеш функції обмежується лише обчислювальними можливостями пристрою запису. Вибір крипто перетворення DES (відповідно до ANSI X9.17) чи сучаснішого AES можна вважати межею доцільності збільшення обчислювальної складності алгоритму роботи ГС.

Покращення цілісності через урахування попередньої інформації можна реалізувати використанням режиму шифрування зі зворотним зв’язком за шифротекстом.

Реалізація даної методики дала змогу провести досліди на рівень обмеження психофізичного сприйняття людиною звуку. Поступове

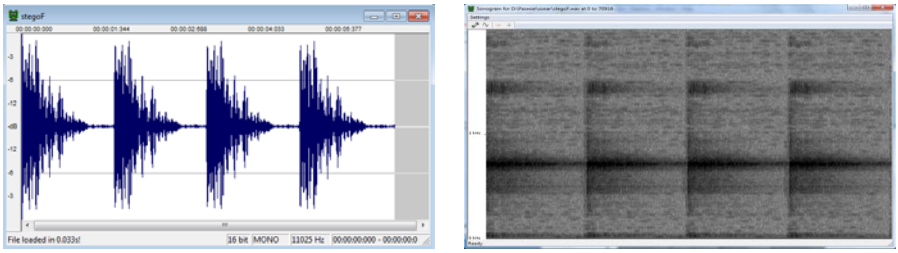
збільшення кількості змінених останніх бітів аудіо відліку і прослуховування отриманого результату виявило максимальну межу кількості змінених останніх біт,при якій вже відчуваються перешкоди, що становить 4 біти Отже при зміні лише одного чи двох останніх бітів аудіо відліку прослуховування перешкод неможливе, що є підтвердженням стійкості до атак підміни.

Зміни, що відбуваються у аудіо файлі проаналізовані за допомогою аналізу спектральної густини потужності звукового сигналу від часу (рисунок 1,2,3).



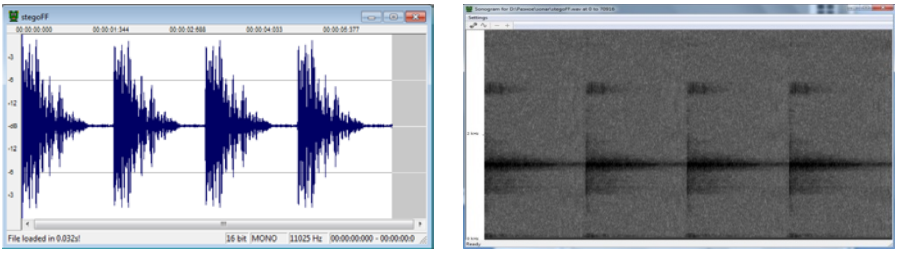
а) б)

Рисунок 1 – Вихідний файл: а) спектограмма, б) сонограмма



а) б)

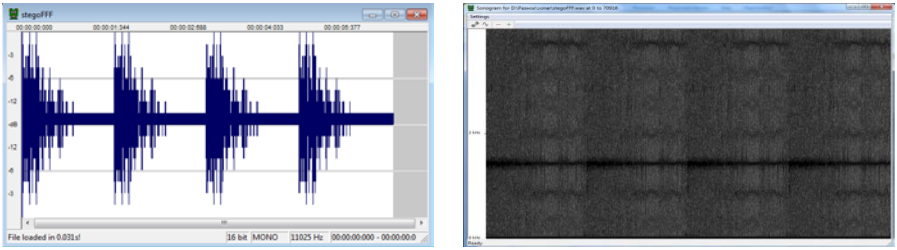
Рисунок 2 – Аудіофайл із зміненими чотирьма останніми бітами у кожному аудіо відліку: а) спектограмма, б) сонограмма



а) б)

Рисунок 3 – Аудіофайл із зміненими восьми останніми бітами у кожному аудіо відліку: а) спектограмма, б) сонограмма

Згідно з результатами, що зображені на сонограммах (рисунок 4б, 4б) можна зробити висновок, що при модифікації 12 і більше останніх біт кожного аудіо відліку суттєво змінюється структура аудіо файлу.



а) б)

Рисунок 4 – Аудіофайл із зміненими дванадцятьома останніми бітами у кожному аудіо відліку: а) спектограмма, б) сонограмма

Отже, недоцільність зміни 12 і більше бітів визначена не лише на основі психофізичного сприйняття звуку людиною, а і підтверджено аналізом структури аудіо файлу. І тому для інтервенції стегоінформації до аудіо файлу необхідно використовувати від 1 до 11 останніх біти.

УДК 004.056

РОЗРОБКА АВТОМАТИЗОВАНОЇ СИСТЕМИ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Автор: *О.В.Подима, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *М.В. Турти, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Вступ. Широке впровадження інформаційних технологій зумовило поширення значних масивів інформації у телекомунікаційних і обчислювальних мережах. Разом з тим значно розширилися можливості для несанкціонованого отримання інформації за допомогою нових технічних засобів.

Функціональний профіль захищеності визначає вимоги до комплексу засобів захисту (КЗЗ) щодо послуг захисту та рівнів їх гарантій. Рівні гарантій є складовою оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НСД) і можуть використовуватися при розв'язку двох типів задач: задачі експертизи та задачі проектування КЗЗ. При цьому оцінка гарантій здійснюється за окремими групами критеріїв і є досить складною задачею, що підлягає автоматизації в рамках автоматизованої системи оцінки захищеності інформації в комп'ютерних системах від НСД. Процедури оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу є досить складними, що зумовлює необхідність їх автоматизації.

На Україні автоматизацією процесів роботи з нормативними документами займаються спеціалісти в ряді вищих навчальних закладів [1-3, 6-8], зокрема – в Харківському Національному університеті радіоелектроніки та Національному університеті кораблебудування [1, 6-8], однак на даний час така система не реалізована [2].

Метою даної роботи є розробка автоматизованої системи оцінки захищеності інформації в комп'ютерних системах (АСОЗІКС) від несанкціонованого доступу (НСД).

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

– на основі аналізу нормативно-правової бази оцінки захищеності інформації в автоматизованих системах від НСД доступу та розробленої інформаційної моделі захищеної АСОЗІКС від НСД розробити алгоритми визначення критеріїв гарантій і функціональних послуг захисту для процесів проектування та аналізу відповідних систем захисту;

– визначити засоби реалізації розроблюваних алгоритмів та апробувати їх дієвість на моделі бази даних системи оцінки захищеності інформації в комп'ютерних системах від НСД;

– розробити АСОЗІКС від НСД з врахуванням діючої нормативно-правової бази.

Основна частина.

Стандартні функціональні профілі будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогоднішній день функціональних послуг, що дозволяють протистояти даним загрозам і забезпечувати виконання вимог, які пред'являються.

Розроблена система базується на НД ТЗІ [4, 5] і містить наступні функціональні блоки:

– Блок інтерфейсу (рис.1);

– Блок вводу даних (про користувачів, категорії технічних засобів, наявність вузлів з різною політикою безпеки, даних для визначення вимог до послуг захисту, заявлений профіль захищеності, умов функціонування КС, пріоритетів забезпечення властивостей конфіденційності, цілісності і доступності даних, бажані функціональні послуги);

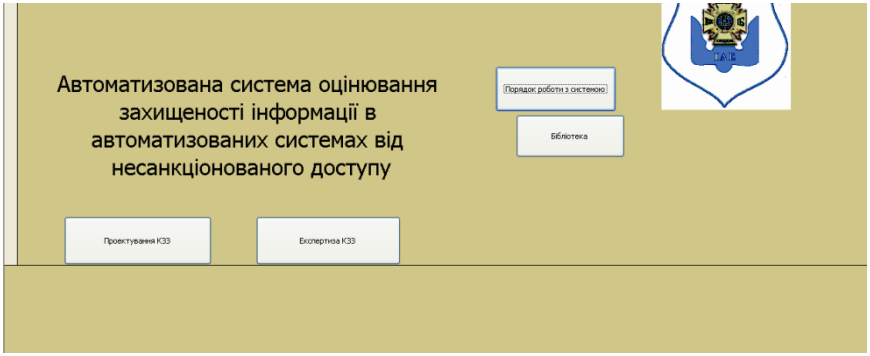


Рисунок 1 – Інтерфейс розробки

– Блок стандартних функціональних профілів захищеності;
– Блок функціональних послуг захисту інформації;
– Блок критеріїв гарантій послуг захисту інформації;
– Блок висновків (щодо відповідності/невідповідності КЗЗ заявленому профілю захищеності, визначений профіль захищеності);
– Блок пояснень висновків (рекомендації щодо усунення недоліків та інформація про завищені показники при експертизі КС, спектр функціональних послуг, що повинен забезпечувати КЗЗ, і вимоги для забезпечення їх рівнів гарантій при проектуванні АС);
– Блок виводу;
– Блок запитів;
– Блок бібліотеки діючої нормативно-правової бази.

Висновки. Розроблена система створює комфортні умови проведення процедур експертизи та проектування комплексу засобів захисту і повністю відповідає нормативно-правовій базі НД ТЗІ.

Список літератури:

1. Баронова О.А., Петров В.Є. Модуль захисту персональних даних та конфіденційної інформації в системі документообігу ВУЗу //Матеріали Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».-Миколаїв: НУК, 2011. – С.127-129.
2. Гунченко А.П. Інформаційна модель автоматизованої системи захищеного документообігу для АС 3 класу з розробкою блоку прийняття рішень // Всеукраїнський форум молодих науковців «Макарівські читання-2013». – С.33-35.
3. Лєншин А.В. Методи аналізу та побудови функціональних профілів захищеності // Матеріали II Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».-Миколаїв: НУК, 2012. – С.70-73.
4. 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;jsessionid=AFD6198C23CB1F96ABAFD7189BBDCE03?showHidden=1&art_id=101853&cat_id=89734&ctime=1344501024406.

5. НД ТЗІ 2.5-005 -99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу [Електронний ресурс] – Режим доступу: http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/article;jsessionid=AFD6198C23CB1F96ABAFD7189BBDCE03?showHidden=1&art_id=101870&cat_id=89734&ctime=1344501089407.

6. Подима О.В. Алгоритм оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу // Матеріали III Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».- Миколаїв: НУК, 2013. – С.197-201.

7. Подима О.В. Алгоритм оцінки рівнів гарантій захищеності інформації в комп'ютерних системах від несанкціонованого доступу // Всеукраїнський форум молодих науковців «Макарівські читання-2014».- Миколаїв: НУК, 2014. – С.69.

8. Подима О.В. Інформаційна модель автоматизованої системи оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу // Всеукраїнський форум молодих науковців «Макарівські читання-2013».- Миколаїв: НУК, 2013. – С.114-115.

СИСТЕМА БЕЗКОНТАКТНОЇ ІДЕНТИФІКАЦІЇ ДАЛЕКОГО РАДІУСУ ДІЇ

Автор: *Л.О. Ракутіна, студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *С.Л. Трибулькевич, викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Однією з найбільш популярних технологій, що реалізує задачі захищеного обміну інформацією, безконтактної ідентифікації об'єктів, автентифікації осіб, управління доступом, є радіочастотна ідентифікація *RFID* (*radio frequency identification*). *RFID* — метод автоматичної ідентифікації об'єктів, в якому за допомогою радіосигналів зчитуються або записуються дані, що зберігаються в так званих транспондерах (мітках). Основним з недоліків даної технології є малий радіус дії типових

пристроїв. Збільшення радіусу дії супроводжується погіршенням показників безпеки, тому постає задача реалізації додаткових заходів із захисту сигналів, якими обмінюються базова станція та мітка. [1]

Система ідентифікації, що розробляється, складається з транспондера, зчитувача та ПЕОМ. Транспондер містить в собі мікроконтролерний та *Wi-Fi*-модулі. Складовими частинами мікроконтролерного модуля є контролер, пам'ять, стабілізатори живлення, інтерфейс *RS*-232, порти *USB*, роз'єми для підключення *Wi-Fi*-модуля, кнопки. У якості зчитувача використовується точка доступу *Wi-Fi* та мережне обладнання. [2]

Контролер забезпечує мережеву взаємодію шляхом реалізації 5 рівнів моделі *OSI* (мережевий, транспортний, сеансовий, представлення, прикладний). Пам'ять використовується для зберігання мережевих налаштувань та мережевої інформації. Інтерфейси периферійного обладнання слугують для розширення можливостей системи шляхом введення нових додаткових функцій, наприклад, *GPS*-трекер, лічильник мото-годин, реєстратор помилок, також можливе застосування різноманітних зовнішніх датчиків. *Wi-Fi*-модуль апаратно реалізує фізичний та канальний рівні моделі *OSI* та виконує шифрування, а тим самим, і захист даних, що передаються по відкритому каналу. [3]

Для забезпечення підключення транспондера, що розробляється, до мережі *Ethernet*, було програмно реалізовано всі необхідні протоколи стеку *TCP (UDP, ICMP, IP, ARP, Ethernet)*.

Принцип роботи пристрою полягає в тому, що мікроконтролерний модуль буде приймати дані по послідовному порту, а потім передавати їх по повітрю за допомогою *Wi-Fi*-модуля (рисунок 1).

Висновок: система володіє достатньо високою захищеністю даних, що передаються відкритими каналами, її радіус дії достатньо великий в порівнянні з класичними RFID-системами. Пристрій можна використовувати для ідентифікації транспортних засобів, збирання даних, накопичених за час перебування поза зоною зчитувача. Розроблена система володіє великими можливостями по розширенню функцій. До недоліків можна віднести залежність від джерела живлення, достатньо велику вартість дослідного зразка, яку можна знизити при серійному виробництві.

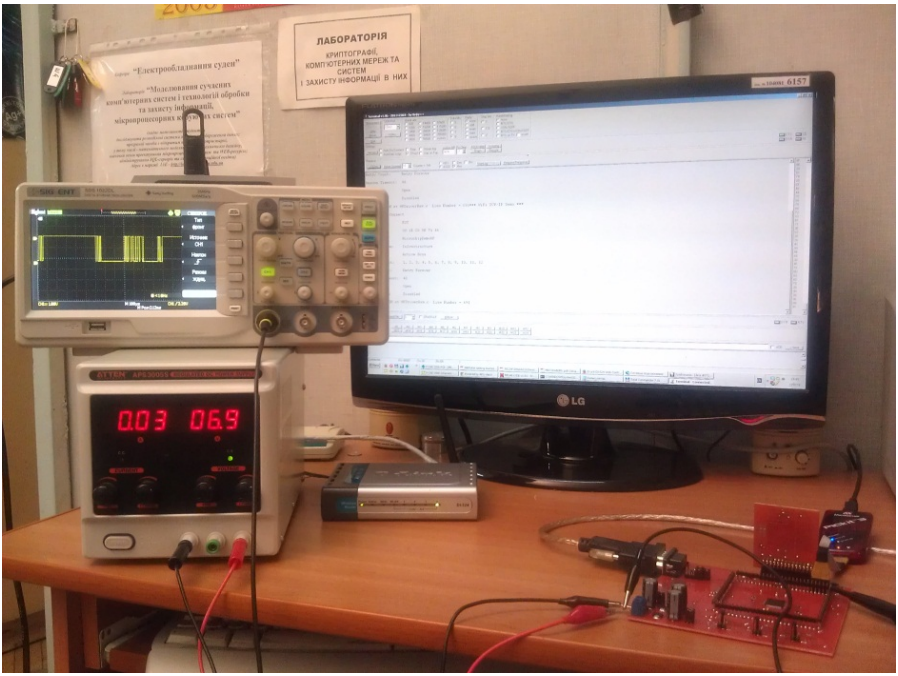


Рисунок 1 – Випробування дослідного зразка

Список літератури:

1. Ракутіна, Л.О. Активна система радіоідентифікації на основі бездротових технологій/ Л.О. Ракутіна // Всеукраїнський конкурс студентських наукових робіт за напрямком «Суднобудування та водний транспорт» – Миколаїв: НУК, 2014.
2. Из чего состоит система *RFID*? [Електронний ресурс] // Режим доступу: *http://posmagazin.ru/articles/18/120/* , заголовок з екрану.
3. Ракутіна Л.О. Система безконтактної ідентифікації далекого радіусу дії / Ракутіна Л.О. // Всеукраїнський форум молодих науковців «Макаровські читання -2014». – Миколаїв: НУК, 2014.

УДК 681.335

АВТОМАТИЗАЦІЯ АНАЛІЗУ НАВЧАЛЬНО-МЕТОДИЧНИХ КОМПЛЕКСІВ ДИСЦИПЛІН КАФЕДРИ

Автор: *В.В. Ровєнських, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *О.А. Баронова, ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Випускова кафедра є важливою управляючою ланкою в організації учбового процесу, яка відповідає за якість підготовки студентів. Аналіз навчально-методичного забезпечення кафедри і окремих дисциплін можливо використовувати як ресурс для керування якістю навчання.

Основна мета роботи – підвищення ефективності управління учбовим процесом на основі автоматизації збору, обробки, зберігання та ефективного використання навчально-методичного забезпечення кафедри.

Інформаційна система аналізу навчально-методичного забезпечення кафедри включає базу даних, у якій зберігаються документи загальної частини навчально-методичного забезпечення кафедри (ОКХ, ОПП, засоби діагностики, навчальні плани освітньо-професійних рівнів бакалавр, спеціаліст, магістр) і методичні матеріали по дисциплінам кафедри (робочі навчальні плани та програми; навчальні програми з вибіркових навчальних дисциплін; навчальні посібники; інструктивно-методичні матеріали до семінарських, практичних і лабораторних занять; індивідуальні семестрові завдання проблемного характеру для самостійної роботи студентів з навчальної дисципліни; методичні матеріали для студентів з питань самостійного опрацювання фахової літератури, написання курсових і дипломних проектів та робіт). Захищена автоматизована система зберігання і аналізу НМКД кафедри має запити та звіти, які формируються базою даних дозволяють аналізувати повноту та якість забезпечення дисципліни методичними матеріалами. Результати аналізу можуть бути представлені візуально як діаграми та графіки.

Висновки. Аналіз навчально-методичного забезпечення кафедри і окремих дисциплін є ефективним засобом моніторингу і управління якістю навчального процесу ВЗО.

Список літератури:

1. Баронова О.А., Ровенских В.В. Автоматизація управління якістю навчання на рівні кафедри// Матеріали Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». – Миколаїв: НУК, 2013. – С. 11-13.

УДК 004.056

РОЗРОБКА ПРОГРАМНОГО ЗАСОБУ ПОРІВНЯННЯ НЕЧІТКИХ ЕТАЛОНІВ

Автор: *В.В. Тригуб, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *М.В. Турти, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Вступ Одним з напрямів використання нечітких знань є обробка даних за допомогою нечітких еталонів (НЕ). Розв'язок таких задач, як правило, пов'язаний з високою трудомісткістю процедур аналізу нечітких даних та залежністю кінцевого результату від суб'єктивних факторів. Крім того, робота з НЕ передбачає в більшості випадків наявність бібліотеки еталонів і повторюваність типових процедур обробки даних, і тому ефективно може виконуватися тільки в автоматизованому режимі. Автоматизація цих процедур особливо важлива при роботі в реальному часі, тобто в режимі, в якому працюють всі системи моніторингу інформаційної безпеки і системи контролю доступу.

Метою даної роботи є розробка програмного засобу порівняння нечітких еталонів в складі автоматизованої системи обробки нечітких еталонів.

Для досягнення поставленої мети були розв'язані наступні задачі: проведено аналіз сучасних методів обробки НЕ; розроблені алгоритми порівняння НЕ за певними методами і програмний блок порівняння НЕ.

Огляд літератури [1-6] дозволив визначити, що методи обробки функцій належності (ФН) можна поділити на процедури, призначені для обробки окремих нечітких множин (НМ) і множини НМ. Доведено, що всі операції з окремими ФН можуть виконуватися як із ФН, створеними за класичною теорією, так і створеними за теорією однозначної нечіткої логіки (ОНЛ). Єдина відмінність полягає в тому, що за теорією ОНЛ ФН обов'язково є унімодальними, нормальними і параметричними, тобто ці властивості є наперед визначеними.

Операції з окремими НМ можуть бути розділені на операції перетворення ФН, до яких відносяться операції нормалізації, концентрування, розтягування і операція розбиття НМ A на α-рівневі підмножини, операції визначення властивостей ФН та операції визначення параметрів ФН, до яких відносяться вісі інші операції.

Операції над множиною НМ виконуються як послідовність операцій над парою НМ і можуть бути розділені на операції групування НМ, які використовуються в системах прийняття рішень для визначення надійності висновку за нечіткими свідоцтвами і включають операції перетину, об'єднання, декартового добутку НМ, доповнення НМ до універсальної множини або до іншої НМ, різниці НМ, визначення опуклої комбінації НМ, та операції порівняння НМ.

В АСФОНЕ для пари нечітких множин (нечіткого еталону та нечіткого числа, що відповідає досліджуваному об'єкту) можуть застосовуватися для порівняння операції впорядкування та порівняння за формою ФН.

Доведено, що для ФН, побудованих за ОНЛ застосовуються всі методи, але функції методів впорядкування на базі відношень та α-рівневого методу повинні звертатися в цьому випадку до додаткових функцій, що реалізують відповідні етапи попереднього перетворення даних.

Якщо одна ФН визначена за теорією ОНЛ, а друга – за будь-яким методом класичної теорії, то операції порівняння відповідають класичній теорії, але також є спрощеними внаслідок спрощення процедур визначення параметрів, за якими здійснюється порівняння, для ФН, побудованої за ОНЛ.

Оскільки порівняння шляхом впорядкування може здійснюватися лише за методами, які мають певні властивості, то в розробленому програмному блоці передбачена перевірка відповідності властивостей введених НМ і властивостей, що є необхідними для кожного методу. При цьому використовується алгоритм порівняння векторів властивостей ФН, при однакових вагових коефіцієнтах властивостей, який враховує наявність протирічних властивостей «нормальність» – «субнормальність», «унімодальність» – «полімодальність», «дискретність» – «непервність», «параметричність» – «непараметричність».

Порівняння НЕ може здійснюватися одним обраним методом або за групою методів, визначеною експертами шляхом вибору з множини доступних методів. Отримані висновки щодо відмінності порівнюваних НЕ за кожним із обраних методів можуть різнитися між собою, бо певний метод порівняння використовує власний набір специфічних параметрів, визначених за порівнюваними нечіткими множинами. Крім того, різні набори параметрів для різних методів порівняння обумовлюють різну значимість висновків, отриманих за кожним методом, для узагальнюючого висновку, що враховано в розробленому узагальненому алгоритмі.

Розроблений програмний блок може використовуватися як окремий модуль, або вбудовуватися в АСФОНЕ чи в системи ідентифікації, навігації, управління, системи виявлення уразливостей в початкових кодах, системи оцінювання ефективності захисту інформації.

Висновки.

1. В роботі на основі проведеного аналізу особливостей побудови інтелектуальних систем з використанням НЕ; сучасних методів обробки НЕ, форм їх представлення була розроблена структура блоку порівняння НЕ у складі автоматизованої системи формування і обробки НЕ і алгоритми основних операцій порівняння нечітких чисел.

2. Розроблено програмний модуль порівняння нечітких множин.

3. Визначено галузі застосування розробленого програмного модуля в інформаційній безпеці:

– навчальний процес підготовки фахівців галузі знань 1701 «Інформаційна безпека» в рамках курсів «Методи системного аналізу», «Теорія статистичних рішень і ситуаційного аналізу», «Розпізнавання образів в системах захисту інформації»;

– біометричні криптографічні системи, системи комп'ютерного зору, системи аналізу фаз процесу роботи програмного забезпечення та ін.

Список літератури:

1. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: "МК-Пресс", 2006. – 320 с.

2. Турти М.В. Теорія однозначних нечітких систем та нейронні мережі: Монографія. Частина 1.- Миколаїв: Вид-во Європейський університет, Миколаївська філія, 2007.-140 с.

3. Биометрические криптографические системы и их применение [Электронный ресурс]/ О.В. Куликова, О.П.Цветочкин // EUROCRYPT. – 2005. – №11. – с.53-57. – Режим доступу: www.pvti.ru/data/file/bit/bit_3_2009_10.pdf.

4. Многокритериальное упорядочивание объектов в ассоциативных структурах фактор-множеств [Электронный ресурс] / Ю. В. Кандырин, А. М. Кошелев// Известия ВолгГТУ. – 2007. – №9 (35). – с. 107-111. – Режим доступу: www.vstu.ru/research/pub/izvestiya/aktualnye-problemy-upravleniya/ 2007-09.pdf.

5. Организация интеллектуальных вычислений. [Электронный ресурс]: Тема 11. Нечеткая логика: Конспект лекций. – 2012 – Режим доступу: www.victoria.lviv.ua/html/oio/html/theme11_rus.htm.

6. Мігунов В.О. Програмна обробка нечітких еталонів // Матеріали Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».- Миколаїв: НУК, 2011. – С.97-101.

УДК 004.056

ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕДУР ТЕСТУВАННЯ ЗАХИСТУ ЛАЗЕРНОГО ВИПРОМІНЮВАННЯ ВІД ОПТИКО-ЕЛЕКТРОННОЇ РОЗВІДКИ

Автор: *Д.Ю.Турчанінов, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *М.В. Турти, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Вступ. Оскільки за своїми небезпечними наслідками оптико електронна розвідка (ОЕР) займає особливе місце серед загроз національної безпеки України, то користувачі повинні чітко усвідомлювати можливості засобів ОЕР, їх ключові параметри і характеристики (потенціальний вплив на результат застосування), переваги і недоліки класів апаратури при вирішенні певних завдань при реалізації заходів спостереження та безпеки. Складність і різноманітність засобів ОЕР та відповідних засобів протидії обумовлюють необхідність автоматизації робіт при

розробці заходів захисту від ОЕР та проведенні досліджень ефективності засобів захисту від ОЕР. Тому розробка лабораторного стенду, призначеного для проведення досліджень і здобуття практичних навичок студентами в цій галузі є актуальною задачею, розв‘язок якої [1-6] базується на нормативних документах технічного захисту інформації, частина з яких має обмежений доступ, однак деякі вирішувані при цьому питання висвітлюються у відкритому друці.

Метою даної роботи є розробка програмного забезпечення процедур тестування захищеності об’єктів від засобів ОЕР.

Для досягнення поставленої мети необхідно розв’язати наступні задачі:

– за відкритими джерелами інформації проаналізувати сучасний стан розвитку методів та засобів ОЕР та засобів захисту від ОЕР;

– визначити впливові фактори та їх пріоритети для ефективного захисту лазерного випромінювання від ОЕР;

– визначити функціональний склад лабораторного стенду на основі визначених впливових факторів та відповідної автоматизованої системи розрахунку норм захисту;

– розробити структуру лабораторного стенду захисту лазерного випромінювання від ОЕР на базі ПЕОМ та відповідної автоматизованої системи розрахунку норм захисту;

– розробити і апробувати алгоритми роботи програмного забезпечення стенду.

Основна частина. Проведений аналіз відкритих літературних джерел дозволив визначити фактори, що впливають на ефективність засобів ОЕР та засобів протидії ОЕР [7] для ефективного захисту лазерного випромінювання від оптико-електронної розвідки. З принципів побудови і структури сучасних засобів ОЕР та засобів захисту від неї випливає, що впливовими факторами є частота та довжина хвилі випромінювання, кут падіння променя та площа на яку він падає.

За результатами розрахунків методом аналізу ієрархій можна зробити висновок, що найбільш критичним для ефективного захисту лазерного випромінювання від ОЕР є показник факторів, пов'язаний з властивостями лазерного випромінювання. Тому при захисті лазерного випромінювання від засобів ОЕР найбільшу увагу необхідно приділити саме йому.

Проведений аналіз дозволив аргументовано сформувати функціональний склад лабораторного стенду (рис.1).

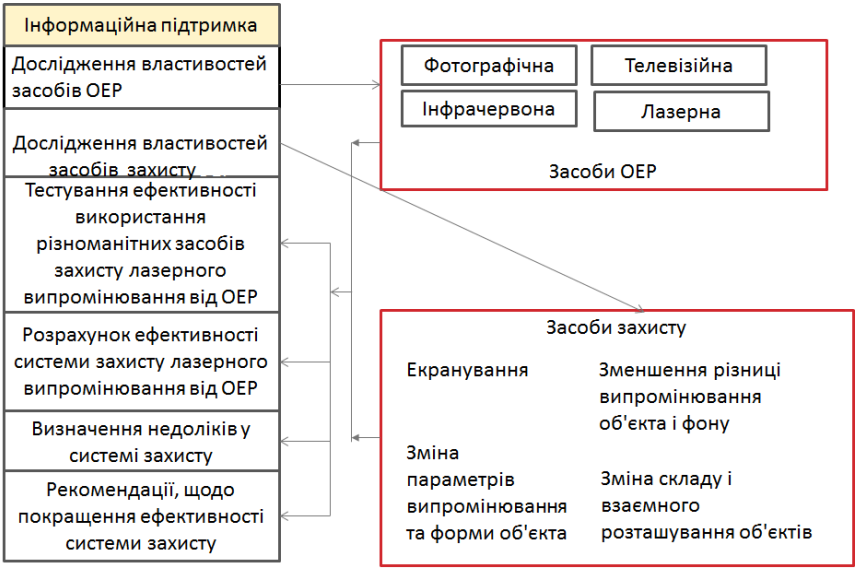


Рисунок 1 – Функціональний склад стенду

Лабораторний стенд захисту лазерного випромінювання від засобів ОЕР на базі ПЕОМ призначений для виконання наступних видів робіт: дослідження властивостей засобів ОЕР; дослідження властивостей засобів захисту від ОЕР; тестування ефективності використання різноманітних засобів захисту лазерного випромінювання від ОЕР; розрахунку ефективності системи захисту лазерного випромінювання від ОЕР; визначення недоліків у системі захисту; видачі рекомендації, щодо покращення ефективності системи захисту. До лабораторного стенду додається автоматизована система розрахунку норм захисту (рис.2), до складу якої входить відкрита бібліотека діючої нормативно-правової бази і відповідних сайтів за тематикою розробки. Функціями такої автоматизованої системи є надання інформаційної підтримки при створенні систем захисту лазерного випромінювання від ОЕР

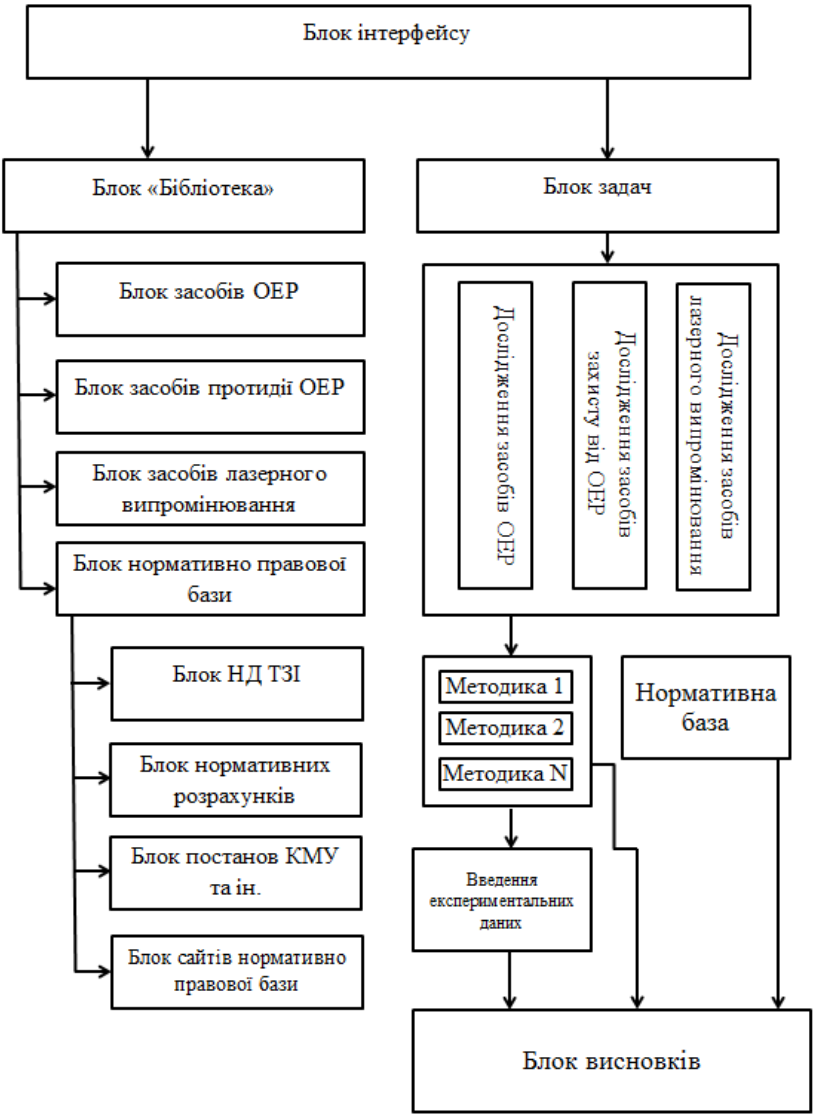


Рисунок 2 – Структура та функціональний склад
блоку розрахунку норм захисту

на основі бази відкритих та закритих нормативних документів; опис та автоматизація стандартизованих розрахунків ефективності систем захисту та розрахунків їх складових; надання рекомендацій, щодо створення систем захисту лазерного випромінювання від ОЕР; надання інформації щодо сучасних напрямів розвитку наукових досліджень і апаратно-програмного забезпечення в галузі.

Стенд має функціонувати за наступним алгоритмом: моделюється процес зняття інформації засобами ОЕР з лазерного випромінювання. аналізуються канали витоку інформації; застосовуються заходи протидії засобам ОЕР; розраховується ефективність використання саме цих засобів; отриманий результат ефективності зіставляється з існуючими нормами захисту (у випадку наявності системи захисту інформації бази даних норм захисту і системи контролю доступу, що гарантує наявність у відповідних користувачів форм допуску) (рис.3).

Рисунок 3 Реалізація блоку задач

В якості засобів ОЕР повинні використовуватися макети, що дозволяють змінювати параметри вихідного випромінювання.

Джерелом сигналу є пластини з різних матеріалів, з яких знімаються дані з джерела інформативного сигналу засобами ОЕР.

В якості активних перешкод використовуються пластини різних матеріалів, що мають відмінні параметри та характеристики, наприклад залізо, алюміній, сітки, скляні пластини з покриттям фольгою, плівкою тощо, на яких встановлені засоби активного захисту, місце розташування яких може змінюватися.

В якості пасивної перешкоди використовуються ті ж самі пластини без засобів активного захисту.

Дослідження ефективності захисту інформації на стенді повинні проводитися із застосуванням вібраторів різних конструкцій і з різними алгоритмами роботи при змінній системі кріплення пластин, з додатковими засобами освітлення об'єкту, змінному фоні, змінній прозорості середовища (блоки захисту з різною прозорістю і структурою), в тому числі складні блоки, заповнені водою із вбудованими засобами утворення турбулентності.

До системи обробки інформації відносяться датчики, які дозволять заміряти зміну основних параметрів лазерного випромінюванні при дослідах на виході засобу ОЕР та на об'єкті, а також ПЕОМ на якій здійснюється обробка отриманих результатів та порівняння їх з нормованими параметрами (об'єм HDD – 80 Гб, тактова частота 2,8 ГГц, 2 Гб оперативної пам'яті; 40 Мб вільного місця на диску для СУБД, 6 Мб вільного місця на диску для папки проекту; клавіатура; маніпулятор типу "миша"; відеокарта 1 Гб; операційна система Windows). Передбачається, що конструкція стенду дозволяє змінювати розташування засобів ОЕР для дослідження залежності якості зняття інформації засобами ОЕР від дальності та кута падіння променя на джерело інформативного сигналу.

Висновки. Розроблений проект лабораторного стенду має функціональний склад, структуру, апаратне і програмне забезпечення, що дозволяють використовувати його як для проведення досліджень (дослідження моделей засобів ОЕР, засобів протидії ОЕР, ефективності захисту інформації від засобів ОЕР), так і для проведення лабораторних робот при підготовці фахівців галузі знань 1701 «Інформаційна безпека». Розроблене програмне забезпечення дозволяє здійснювати інформаційну підтримку головних функцій стенду та автоматизувати процедури розрахунку і визначення відповідності нормам основних показників ефективності захисту лазерного випромінювання від ОЕР.

Список літератури:

1. НДТЗІ 2.2-002-06 Протидія технічним розвідкам. Норми захисту параметрів лазерного випромінювання від оптико-електронної розвідки;
2. НДТЗІ 2.2-004-06 Протидія технічним розвідкам. Норми з протидії засобам фотографічної та оптико-електронної розвідок;

3. НДТЗІ 2.3-009-06 Протидія технічним розвідкам. Методика контролю виконання норм захисту параметрів лазерного випромінювання від оптико-електронної розвідки;

4. НДТЗІ 2.3-011-06 Протидія технічним розвідкам. Методики контролю виконання норм з протидії засобам фотографічної та оптико-електронної розвідок;

5. НД ТЗІ 2.4-002-06 Протидія технічним розвідкам. Рекомендації із захисту параметрів лазерного випромінювання від оптико-електронної розвідки;

6. НДТЗІ 2.4-004-06 Протидія технічним розвідкам. Рекомендації з протидії засобам фотографічної та оптико-електронної розвідок.

7. Турчанінов Д.Ю. Функціональний склад стенду захисту лазерного випромінювання від оптико-електронної розвідки //Матеріали Всеукраїнського форуму молодих науковців «Макарівські читання -2014». – Миколаїв: НУК, 2014. – С.84.

8. Турчанінов Д.Ю. Розробка структури стенду захисту лазерного випромінювання від оптико-електронної розвідки // Матеріали III Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті». – Миколаїв: НУК, 2013. – С.219-223.

УДК 004.056.5: 534.[784: 835]: 621.391.883

ЗАДАЧА ВРАХУВАННЯ ПРОФЕСІЙНОЇ ПІДГОТОВЛЕНОСТІ ЗЛОВМИСНИКА В ОЦІНЦІ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ ЗА КРИТЕРІЄМ РОЗБІРЛИВОСТІ МОВИ

Автор: *О.Є. Феоктистова, студентка, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *Ю.І. Касьянов, ст. викладач, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Вступ. Розбірливість мови вже давно є одним з основних критеріїв в оцінці якості каналів мовного зв’язку, бо від неї залежить, чи зрозуміє слухач почуту інформацію, чи ні [1, 2]. Останнім часом критерій розбірливості мови почали використовувати і області інформаційної

безпеки для оцінки захищеності мовної інформації (оцінці ефективності заходів захисту) [3].

Важливим фактором в сприйнятті інформації є професійна підготовленість слухача. Якщо слухач сприймає (зловмисник перехвачує) мовне повідомлення, тематична направленість якого входить в коло його інтересів і є йому близькою, то кількість правильно сприйнятої інформації (розбірливість мови) звісно буде більшою. Однак, врахування цього фактору в оцінці якості каналів мовного зв'язку і оцінці захищеності мовної інформації від витоку технічними каналами повинно бути прямо протилежним, оскільки при оцінці якості чи ефективності потрібно виходити з найгіршого варіанту.

Найгіршим варіантом в визначенні якості каналів мовного зв'язку є випадок передачі незнайомої слухачеві (за тематикою) інформації. Тому для оцінки тут використовують розбірливість елементів мови, що не несуть смислового навантаження, зокрема складів [4].

У випадку оцінки захищеності мовної інформації потрібно орієнтуватись на професійно підготовленого зловмисника, для якого підслухана інформація є тематично знайомою та цілісною за смислом. Тому тут при оцінці потрібно використовувати закінчені смислові тексти. Врахування цього фактору є недостатньо проробленим.

Метою цієї роботи є визначення впливу професійної підготовленості зловмисника на розбірливість сприйнятої мовної інформації.

Основна частина. Першим кроком до мети є вибір методу дослідження. Існуючі методи та методики визначення розбірливості мови розділяють на суб'єктивні та об'єктивні. Наразі до суб'єктивних методів відносяться такі, в яких мовний чи слуховий апарат людини є складовою частиною вимірювальної системи, а до об'єктивних – методи, в яких весь вимірювальний процес виконується приладами без участі органів чуття людини. Об'єктивні методи вимірювання розбірливості мови досить перспективні в силу можливості значного прискорення й здешевлення процедури вимірювання. Але для визначення впливу підготовленості слухача треба проводити експерименти по розбірливості повідомлень з участю дикторів і аудиторів, тому об'єктивні методи є недоцільними.

Суб'єктивні методи базуються безпосередньо на експертних оцінках і виконуються з участю експертів: дикторів і аудиторів. Розріз-

няють "чисто" суб'єктивні методи, при яких в оцінюванні розбірливості мови приймає участь одна єдина пара диктор-аудитор, і об'єктивізовані суб'єктивні методи де розбірливість мови оцінюється різними групами дикторів і аудиторів з наступним усередненням отриманих результатів (рис. 1).

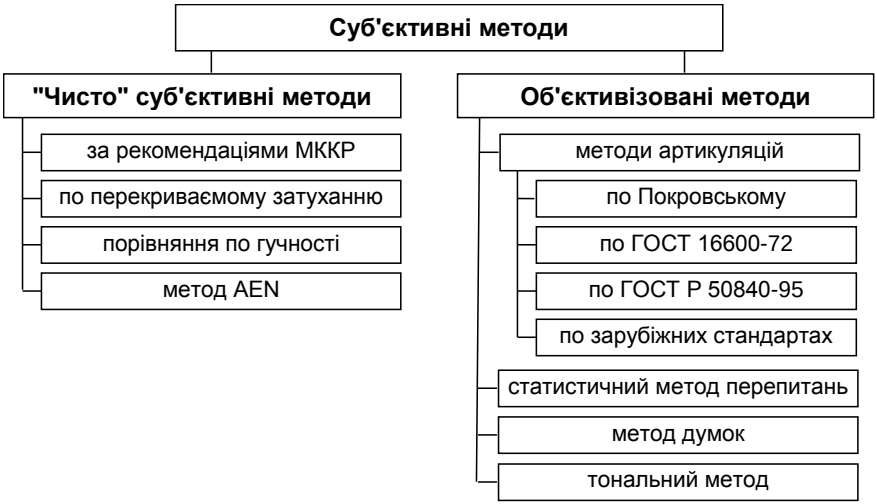


Рисунок 1 – Суб'єктивні методи

Артикуляційні випробування є суб'єктивним методом оцінки розбірливості – це найбільш прямий й очевидний, а іноді й єдиний, спосіб дослідження якості каналу мовного зв'язку. Суть таких випробувань полягає у тому, що диктори зачитують (відтворюють) спеціально складену таблицю елементів мови (звуків, складів, слів або фраз), аудитори прослуховують її і роблять запис у відповідному аркуші, після чого підраховується число помилок, зроблених останніми. Мірою розбірливості є відношення числа правильно прийнятих по випробовуваному каналу елементів мови до загального числа переданих елементів, виражене у відсотках. Головними перевагами методу артикуляційних випробувань є його універсальність [5], тобто можливість кількісної оцінки розбірливості для будь-якого типу каналу передачі мовних сигналів.

Висновки. В ході роботи буде проведено експеримент з залученням декількох людей з різною професійною підготовленістю до текстів з різною тематикою. Це дасть нам змогу визначити на скільки підготовленість слухача впливає на коефіцієнт розбірливості мови.

Як висновок можна сказати, що вирішення даної задачі дозволить поліпшити адекватність і точність оцінки захищеності мовної інформації.

Список літератури:

1. Покровский Н.Б. Расчет и измерение разборчивости речи / Н.Б. Покровский. – М.: Гос. изд-во литературы по вопросам связи и радио, 1962. – 392 с.
2. Сапожков М.А. Речевой сигнал в кибернетике и связи / М.А. Сапожков. – М.: Гос. изд-во литературы по вопросам связи и радио, 1963. – 452 с.
3. Хорев А.А. К оценке эффективности защиты акустической (речевой) информации / А.А.Хорев, Ю.К. Макаров // Специальная техника. – 2000. – № 5. – С. 46 – 56.
4. Передача речи по трактам связи. Методы оценки качества, разборчивости и узнаваемости: ГОСТ Р 50840-95. – М.: Госстандарт России, 1997.
5. Козлачков С.Б. Методические аспекты оценки защищенности речевой информации [Электронный ресурс] / С.Б. Козлачков. – bnti.ru – Режим доступу: http://www.bnti.ru/showart.asp?aid=1003&lvl=04.03.01.

УДК 004.056

ПРОГРАМНИЙ ЗАСІБ ФОРМУВАННЯ НЕЧІТКИХ ЕТАЛОНІВ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПРЯМИМ І ЗВОРОТНІМ ОЦІНЮВАННЯМ

Автор: *М.І. Чумак, студент, Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Науковий керівник: *М.В. Турти, к.т.н., доц., Національний університет кораблебудування імені адмірала Макарова, м. Миколаїв*

Для ефективного визначення стану безпеки інформації необхідно використовувати спеціальні інтелектуальні засоби, зокрема нечіткі еталони (НЕ), процедури створення яких підлягають автоматизації [1, 2].

Метою роботи є розробка програмного блоку формування нечітких еталонів (НЕ) методом прямого і зворотного оцінювання (МПЗО) для вирішення задач інформаційної безпеки.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– проаналізувати властивості функцій належності (ФН) нечітких множин (НМ) і методи формування ФН нечітких чисел (НЧ) за класичною теорією (КТ) та теорією однозначної нечіткої логіки (ОНЛ);

– розробити алгоритм і відповідний програмний блок визначення ФН за допомогою МПЗО для роботи у складі автоматизованої системи формування і обробки НЕ (АСФОНЕ);

– сформулювати практичні рекомендацій щодо використання методу прямого і зворотного оцінювання для формування нечітких еталонів в інформаційній безпеці.

Основна частина. Метод прямого і зворотного оцінювання (МПЗО) містить два підходи до визначення функції належності (ФН) – пряме і зворотне оцінювання. ФН визначається кожним суб'єктом окремо за допомогою багаторазового оцінювання даних та подальшого усереднення відповідей. Передбачається, що суб'єктивне поняття $\tilde{A}$ розбиває область дослідження X на частини X_0, X_1 і X_H. Частини X_0 і X_1 утворені об'єктами $\left[x_{\min}\right]$ та $\left[x_{\max}\right]$ відповідно, тобто такими, щодо яких у суб'єкта не виникає сумнівів стосовно того, чи мають вони властивості A чи ні, а частина X_H є областю невизначеності. Таким чином, вхідними даними для методу МПЗО є: при прямому оцінюванні – ступені належності, які призначає експерт для пред'явлених об'єктів; при зворотному – ступені належності для вибору відповідних об'єктів. Розроблений алгоритм для блоку, що реалізує МПЗО, наведено на рис.1.

Оскільки МПЗО не формує параметричні ФН, то цей метод непридатний для формування нечітких еталонів за теорією однозначної нечіткої логіки в класичному вигляді. Тому запропонована модифікація МПЗО відповідно до теоретичних основ ОНЛ, яка полягає в тому,

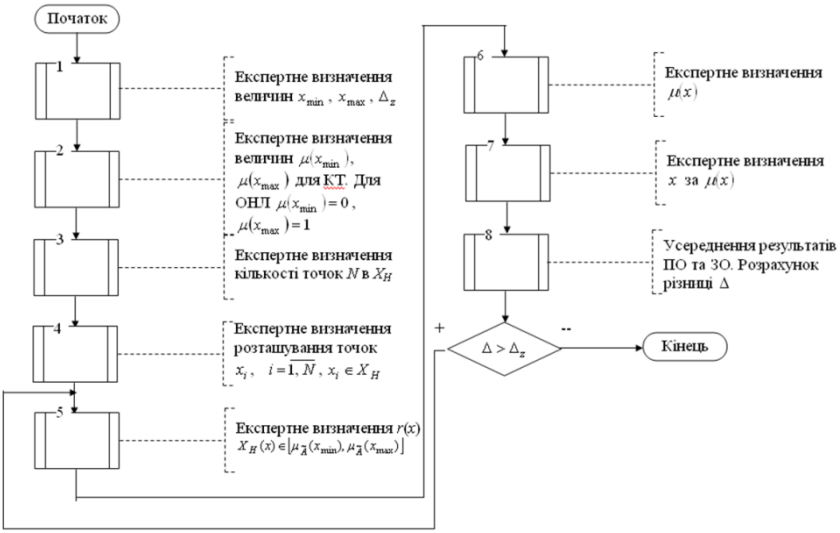


Рисунок 1 Алгоритм роботи блоку МПЗО

що при заданих $x_{\min}$ та $x_{\max}$ використовуються два терми, що відповідають $x_{\min}$ та $x_{\max}$, для яких експерт (група експертів) абсолютно впевнений у висновках «Властивість відсутня» та «Властивість наявна» відповідно, тобто $\mu(x_{\min})=0$, $\mu(x_{\max})=1$. Якщо прийняти, що із зростанням x зростає впевненість експерта в наявності певної властивості, наприклад лінійно, то ФН нечіткого еталону, отриманого методом прямого і зворотного оцінювання точно співпаде з ФН терму «Властивість наявна», побудованого за ОНЛ. Аналогічні результати можна отримати, якщо обрати нелінійну форму ФН та застосувати правила парних термів або зростаючих ділянок термів [3] для побудови ФН НМ «Властивість відсутня».

В роботі оцінено ефективність МПЗО. За критерії якості НЕ для систем, що базуються на процедурах порівняння нечітких параметрів об'єкта і раніше сформованих нечітких еталонів в режимі реального часу, які є типовими для галузі інформаційної безпеки, прийняті параметри, що впливають на швидкість отримання нечітких характеристик об'єкта і швидкість виконання процедур порівняння, їх здатність за-

безпечувати визначеність висновку процедур порівняння і можливість використання одного НЕ, сформованого експертним шляхом, в різних системах з різними методами обробки. Оскільки навіть при наявності одного циклу в методі прямого і зворотного оцінювання відбувається подвійне опитування експертів, то цей метод непридатний для використання в адаптовних системах, що автоматично виконують класифікацію об'єктів.

Розроблений програмний модуль забезпечує: діалоговий режим роботи з експертами; можливість задавати кількість експертів, які беруть участь у формуванні нечіткого еталона; можливість повідомляти експертам про обраномий метод формування НЕ і цілі опитування; можливість визначати вагові коефіцієнти експертів; можливість визначати межі носія ФН із захистом від помилок введення; можливість задавати кількість оцінюваних точок в області визначення із захистом від помилок введення; можливість задавати розташування оцінюваних точок в області визначення ФН із захистом від помилок введення; можливість визначати координати оцінюваних точок в області визначення ФН із захистом від помилок введення можливість визначати зваженим експертним оцінюванням тип припустимої похибки оцінювання ФН (абсолютна чи відносна похибка) із захистом від помилок введення; можливість задавати припустиму похибку оцінювання ФН заданого типу шляхом зваженої експертної оцінки із захистом від помилок введення; можливість визначати зваженим експертним оцінюванням значення функції належності в певних точках носія при прямому оцінюванні; можливість визначати зваженим експертним оцінюванням значення координат носія по заданих значеннях функції належності функції належності в певних точках носія при зворотному оцінюванні; можливість визначати похибку визначення ФН і порівнювати її із заданим припустимим значенням (рис.2); автоматичну реалізацію процедури ітераційного уточнення ФН, шляхом мінімізації максимальних розбіжностей в оцінках координат універсуму і виведення результатів у вигляді НМ (рис.3).

```
Input a margin of error as a percentage of the distance between adjacent values
of x. 0<pdx<1
Expert 1: A margin of error as a percentage of the distance between adjacent val
ues of x :: 0.1
Expert 2: A margin of error as a percentage of the distance between adjacent val
ues of x :: 0.1
Expert 3: A margin of error as a percentage of the distance between adjacent val
```

Рисунок 2 – Визначення припустимої відносної похибки зваженою експертною оцінкою

```
1
FUZZY STANDARD
{ ( 5, 0.0571429); ( 7, 1); ( 8, 0.742857); ( 10, 0.471429); }
End
```

Рисунок 3 – Виведення НЕ, сформованого МПЗО

Оскільки програмний модуль працює в діалоговому режимі, то в реалізації алгоритму рис.1 передбачений захист від помилок введення, тобто передбачено виведення повідомлень про допущені помилки введення і рекомендацій щодо їх усунення при: відмінності від шкали Сааті даних, що вводяться експертами, при визначенні вагових коефіцієнтів експертів, завданні типів границь і розташування точок носія НМ, виборі типу припустимої помилки; недотриманні відносин порядку для меж носія НМ; перевищенні кількістю оцінюваних точок носія НМ, визначеною експертним шляхом, максимального можливого значення, розрахованого з міркувань цілісності координат для певних меж носія НМ у разі вибору експертами цілого типу координат; перевищенні розрахованого значення помилки над заданим припустимим значенням; запуску процедури уточнення ФН в точці з максимальною похибкою з метою наближення до заданої точності. постановки завдання перед експертами та інформації про метод формування нечіткого еталона; результатів визначення вагових коефіцієнтів експертів; результатів зваженого експертного оцінювання носія НМ у вигляді чіткої множини $X = \{x_1, x_2, \ldots, x_k, \ldots, x_n\}$, $k = \overline{1, n}$;

Проведено верифікацію розробленого програмного модуля на тестовому прикладі [1] формування НЕ “ДОСТАТНЯ ДОВЖИНА СЕКРЕТНОГО КЛЮЧА“ при заданій множині $X = \{5, 7, 8, 10\}$, яка визначає кількість символів довжини секретного ключа.

Висновки. Таким чином, на основі проведеного аналізу властивостей ФН і особливостей формування ФН нечітких чисел за класичною теорією та теорією ОНЛ розроблено алгоритм і відповідний про-

грамний блок визначення ФН за допомогою МПЗО для роботи у складі АСФОНЕ.

Доведено, що МПЗО за кількістю виконуваних процедур та задіяним обсягом пам'яті є досить витратним і в класичному варіанті непридатний для використання в адаптовних системах, що автоматично виконують класифікацію об'єктів.

Доведено, що модифікація МПЗО дозволяє шляхом введення операції параметризації ФН отримувати ФН, узгоджені з теоретичними основами однозначної нечіткої логіки. При цьому кількість виконуваних операцій скорочується більше ніж у 1,5 раза, а необхідний для збереження даних обсяг пам'яті – приблизно в два рази

Розроблений програмний модуль може використовуватися як окремий модуль, вбудовуватися в АСФОНЕ, вбудовуватися в системи розпізнавання образів (системи контролю доступу, моніторингу атак, оцінювання якості програмного забезпечення, оцінювання ефективності систем захисту інформації, а також використовуватися в навчальному процесі галузі знань 1701 «Інформаційна безпека».

Список літератури:

1. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: "МК-Пресс", 2006. – 320 с.
2. Турти М.В. Теорія однозначних нечітких систем та нейронні мережі: Монографія. Частина 1. – Миколаїв: Вид-во Європейський університет, Миколаївська філія, 2007. –140 с.
3. Мильченко О.М. Програмний засіб формування нечітких еталонів в інформаційній безпеці методом побудови експоненційної функції //Матеріали III Всеукраїнської науково-технічної конференції з міжнародною участю «Сучасні проблеми інформаційної безпеки на транспорті».-Миколаїв: НУК, 2013. – С.187-193.

ЗМІСТ

Секція 1. Інформаційна безпека транспортних засобів і систем ***3***

Проблеми забезпечення інформаційної безпеки в мобільних пристроях на базі ОС Android *Р.В. Баронов* 3

Особенности разработки СУИБ судна *Е.А. Баронова; С. Агакишиев* 7

Адмірал Макаров – засновник радіозв'язку та радіорозвідки на флоті *О.А. Баронова; В.С. Блінцов* 9

Сучасні задачі організації безпеки торгівельного судна *В.С. Блінцов* 12

Концепція створення багатосенсорної системи охорони акваторії порту *О.В. Блінцов; П.В. Майданюк* 16

Урахування автоматичної зміни режиму камер відеоспостереження з функцією «день-ніч» в системі адаптивного освітлення *Ю.І. Касьянов; А.В. Гавриш* 20

Захищена система внутрішньо-суднового зв'язку на базі комп'ютерної мережі судна *О.С. Медлярський; В.І. Корицький* 27

Методика вибору методу формування функцій належності для прикладних задач інформаційної безпеки *М.В. Турти* 30

Секція 2. Захист інформації на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах ***35***

Методи боротьби з бот-мережами *при* розподілених атаках на відмову в обслуговуванні *С.В. Дмитриченко; Р.В. Баронов* 35

Адаптація модуляційного методу визначення розбірливості мови до задач оцінки захищеності мовної інформації *Ю.І. Касьянов; Т.О. Кубарєва* 38

Критерій розбірливості мови в оцінці звукоізоляції *Ю.І. Касьянов; А.Ю. Нохріна; А.І. Кривда* 44

Система протидії дослідженню коду авторських програмних продуктів *С.С. Козирєв* 50

Нові підходи до забезпечення захищеності акустичної інформації *С.М. Нужний* 52

Классификация математических моделей радиоизлучений *В.В. Опарин* 56
Захист інформації в графічних файлах із використанням математичної моделі нелінійної стохастичної диференційної системи *С.Б. Приходько; В.Г. Безрукавий* 60
Захист інформації в аудіо файлах із використанням математичної моделі нелінійної стохастичної диференційної системи *С.Б. Приходько; М.Ю. Бойченко*....61
Удосконалення математичної моделі для створення послідовних випадкових чисел з рівномірним розподілом *С.Б. Приходько; В.В. Решетняк* 63
Удосконалення математичної моделі для генерації значень гаусівської випадкової величини на базі перетворення Джонсона із сім'ї S_U *С.Б. Приходько; Ю.О. Яблуновська*....64
Система радіочастотної ідентифікації по Wi-Fi *Л.О. Ракутіна; С.Л. Трибулькевич* 65
Вплив типу браузера на HTML код сторінки *Д.М. Самойленко* 67
Розподіл секрету при передачі ІзОД у мережних ресурсах *Д.М. Самойленко*....69
Зчитувач RFID стандарта Mifare 13,56 МГц з Ethernet інтерфейсом для систем безконтактної ідентифікації *С.Л. Трибулькевич; В.О. Мигиль*; А.М. Куса....71
Секція 3. Правові аспекти діяльності в галузі інформаційної безпеки....79
Криміналістичне дослідження нових зразків мисливської нарізної зброї іноземного виробництва *С.А. Матвієнко*....79
Правові аспекти інформаційної безпеки на морському торговельному транспорті *І.В. Підпала* 83
Удосконалення процедури збору доказової бази розслідування екологічних злочинів при забрудненні морського середовища шкідливими речовинами *О.В. Тимченко*....86
Информационный анализ правового механизма создания и возможности функционирования коммунального пароходства в Украине *Э.Б. Хачатуров; Н.В. Мишутин*....96

Секція 4. Підготовка кадрів у галузі знань «Інформаційна безпека» ***101***
Деякі питання вдосконалення викладання нормативно-правової бази захисту інформації *О.А. Баронова* 101
Впровадження закону України «Про вищу освіту»: завдання, проблеми та перспективи *О.В. Дашковська; В.П. Погребняк* 102
Розробка алгоритму виявлення модифікації цифрового аудіозапису методом фрактальних перетворень *С.М. Нужний* 106
Лабораторний комплекс по системам радіочастотної ідентифікації *С.Л. Трибулькевич* 110
Формалізація задачі розробки методичного забезпечення підготовки кадрів у галузі інформаційної безпеки *М.В. Турти* 114
Програмний модуль порівняння нечітких еталонів за властивостями *М.В. Турти; О.С. Дібрівний* 117
Опыт использования дипломного проектирования при создании программного комплекса по цифровой обработке сигналов *О.А. Щелконогов* 121
Секція 5. Школа молодих науковців ***125***
Програмний засіб формування нечітких еталонів в інформаційній безпеці методом рівневих множин *С.С. Бак* 125
Теоретико–інформаційний підхід до визначення розбірливості мови в оцінці захищенності мовної інформації *М.І. Батенко* 129
Удосконалення лабораторного стенду з вивчення квантових протоколів *М.С.Божко* 134
Програмний засіб формування нечітких еталонів в інформаційній безпеці методом інтервальних оцінок *А.О. Гузенко* 138
Программный модуль для изучения алгоритма создания цифровой подписи на основе эллиптических кривых *Д.М. Емельянов* 143
Розробка алгоритму виявлення модифікації цифрового аудіозапису методом фрактальних перетворень *Е.Д. Заліян* 146
Удосконалення лабораторного стенду з дослідження просторового розподілу вібрацій *О.А. Захарченко* 150

Анализ защищенности персональных данных в социальных сетях *А.Н. Клочко* 153
Програмний модуль для вивчення алгоритмів стиснення зображень *Р.М. Ларін* 157
Формування нечітких еталонів атак в комп'ютерній мережі методом побудови експоненційної функції *О.М. Мильченко* 160
Розробка методики аналізу гаусових шумів в цифровому аудіозапису для виявлення ознак модифікації фонограми *А.В. Михайлуца* 165
Цифрові водяні знаки у застосуванні до аудіконтейнерів *К.М. Новосьолова* 166
Розробка автоматизованої системи оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу *О.В.Подима* 172
Система безконтактної ідентифікації далекого радіусу дії Л.О. Ракутіна 175
Автоматизація аналізу навчально-методичних комплексів дисциплін кафедри *В.В. Ровєнських* 178
Розробка програмного засобу порівняння нечітких еталонів *В.В. Тригуб* 179
Програмне забезпечення процедур тестування захисту лазерного випромінювання від оптико-електронної розвідки *Д.Ю.Турчанінов* 182
Задача врахування професійної підготовленості зловмисника в оцінці захищеності інформації за критерієм розбірливості мови *О.Є. Феоктистова* 188
Програмний засіб формування нечітких еталонів в інформаційній безпеці прямим і зворотнім оцінюванням *М.І. Чумак* 191

Наукове видання

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ТРАНСПОРТІ

СПІБТ-2014

IV Всеукраїнська науково-практична конференція з міжнародною участю

22 – 23 грудня 2014 року

МАТЕРІАЛИ

(*українською та російською мовами*)

Відповідальна за випуск Трибулькевич В.В.
Макетування Мазанко В.Г.

Формат 60×84/16. Ум. друк. арк. 11,7. Тираж 100 прим. Зам. № 273.

Видавець і виготівник Національний університет кораблебудування, 54025, м. Миколаїв, просп. Героїв Сталінграда, 9

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції ДК № 2506 від 25.05.2006 р.