



Державна служба спеціального зв'язку  
та захисту інформації України

# Матеріали

XIX Міжнародної науково-практичної конференції

**«БЕЗПЕКА ІНФОРМАЦІЇ  
У ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ  
СИСТЕМАХ»**



25-26 травня 2017 року

м. Буча, Київська обл., ГНЦ «Зелена Буча»

Державна служба спеціального зв'язку  
та захисту інформації України

---

Пленарна записка

MOBILE ID - SIXTH KEY TO THE DIGITAL TRANSITION IN  
AZERBAIJAN AND CROSS-BORDER E-SERVICES

Jana Krimm

23

ПРОБЛЕМИ СТАН, ЕТАПИ ТА ПОПЕРЕДНІ РЕЗУЛЬТАТИ АНАЛІЗУ  
КАНДИДАТІВ НА СТАНДАРТИ ПОСТУПАЮТЬОЇХ ПРАКТИВІВ

Г. Д. Горбенко, О. О. Кузнецов, О. М. Понд, В. В. Олександров

Ю. І. Горбенко

24

КАНДАТІВ

В. В. Тимченко

Сторінка 12

інформації

ПОРЯДОК ЗАГЛЯДУ В АКТІВ ЕЛЕКТРОННОГО  
ІНФОРМАЦІЙНОГО ОБМІНУ В КАБІНЕТІ СИСТЕМ УКРАЇНИ

Р. В. Профуровська

26

СТРАХІТЬ ДО КРИТОГРАФІЇ РЕАЛІЗАЦІЇ

МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

А. В. Руденко, О. М. Бондаренко

27

ВИПУСК 19

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ БЛОКЧЕЙН ДИЖІТАЛІЗАЦІЇ

В МОЖЛИВОСТІ КОМУНІКАЦІЇ

А. М. Крик, С. С. Коваленко

28

ОСОБЛИВОСТІ АНАЛІТИЧНОЇ СИСТЕМИ РІВНЯ ПІДРОЗУ

В. Д. Федоренко, В. Д. Юрченко, В. І. Печенко

30

ПІДРОЗУМІВАННЯ АЛГОРИТМІВ ШІФРУВАННЯ

СКЛАДОВІ АЛГОРИТМИ СИГНАЛІВ

О. А. Замуць, С. О. Савченко, В. І. Морозов, В. В. Петров

32

ПО МАТЕРІАЛАМ ЗАБЕЗПЕЧЕННЯ КОМУНІКАЦІЙНОЇ

ІНФОРМАЦІЇ

М. В. Профуровська

34

Київ

25 – 26 травня 2017

# ЗМІСТ

## Пленарне засідання

MOBILE ID - SECURE KEY TO THE DIGITAL TRADE HUB IN  
AZERBAIJAN AND CROSS-BORDER E-SERVICES

Jana Krimpe

23

ПРОБЛЕМИ, СТАН, ЕТАПИ ТА ПОПЕРЕДНІ РЕЗУЛЬТАТИ АНАЛІЗУ  
КАНДИДАТІВ НА СТАНДАРТИ ПОСТКВАНТОВИХ ПРИМІТИВІВ

І. Д. Горбенко, О. О. Кузнецов, О. В. Потій, В. В. Онопрієнко,

Ю. І. Горбенко

24

АПАРАТНІ ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

В. В. Тат'янін

25

## Секція 1. Законодавчі та нормативні питання у сфері захисту інформації

ПОРЯДОК ЗАСТОСУВАННЯ ЕЛЕКТРОННОГО ТА ЕЛЕКТРОННОГО  
ЦИФРОВОГО ПІДПИСУ В БАНКІВСЬКІЙ СИСТЕМІ УКРАЇНИ

Р.В. Проскуровский

26

СТІЙКІСТЬ ДО КРИПТОАНАЛІТИЧНИХ АТАК НА РЕАЛІЗАЦІЮ  
КРИПТОВАЛЮТИ ETHEREUM ТА МОЖЛИВОСТІ ЗАХИСТУ ВІД  
НИХ

А.М. Кудін, О.М. Богуцький

27

ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ АВТЕНТИФІКАЦІЇ  
В МОДЕЛІ ТОНКОГО КЛІЄНТА

А.М. Кудін, А.С. Карпець

28

ОСОБЛИВОСТІ АНАЛІТИЧНОЇ ОЦІНКИ РІВНЯ ПЕМВ

В.І. Заболотний, В.Д. Кравченко, В.І. Перепада

30

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-  
ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ НА РІВНІ ДЖЕРЕЛА  
СКЛАДНИХ ДИСКРЕТНИХ СИГНАЛІВ

О.А. Замула, Є.О. Семенко, В.Л. Морозов, В.В. Денисюк

32

НОРМАТИВНЕ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ  
ІНФОРМАЦІЇ

М.І. Прокоф'єв

34

КРИТЕРІЇ БЕЗПЕКИ КІБЕРНЕТИЧНИХ СИСТЕМ І.Б. Яковів	99
АЛГОРИТМ РОБОТИ ГЕНЕРАТОРА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ КЛІТИННОГО АВТОМАТУ С.М. Білан, О.І. Левчук	100
ВИЗНАЧЕННЯ КРИТЕРІЇВ ВІДНЕСЕННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ДО КАТЕГОРІЇ КРИТИЧНИХ О.Ю.Юдін, М.В. Іщук	101
МОВЛЕННЄВА ІНФОРМАЦІЯ В КІБЕРПРОСТОРИ ТА ЗАВДАННЯ ЇЇ ЗАХИСТУ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ С.О. Іванченко, О.О. Черненко	102
ОГЛЯД ТА АНАЛІЗ ОСНОВНИХ ПОСТ КВАНТОВИХ МЕХАНІЗМІВ ПІДПISУ НА ОСНОВІ ГЕШ-ФУНКЦІЙ І.Д. Горбенко, В.А. Кулібаба, Н.В.Ковальова	104
ПІДХІД ДО ОЦІНКИ ДИФЕРЕНЦІЙНИХ ВЛАСТИВОСТЕЙ ПЕРСПЕКТИВНОГО СИМЕТРИЧНОГО БЛОКОВОГО ШИФРУ «КИПАРИС» М.Ю. Родінко, Р.В. Олійников, В.І. Руженцев, Р. Ю. Єлисеєв	105
МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В РОЗПОДІЛЕНИХ БАЗАХ ДАНИХ АСУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ І.Ю.Субач, О.М. Чаузов	107
МІРА ЛІНІЙНИХ СПОТВОРЕНЬ І ЇЇ ВПЛИВ НА ЙМОВІРНІСТЬ ВИЯВЛЕННЯ СИГНАЛУ І. Железаров, В.Я. Дворський, М.І. Прокоф'єв	108
ПОБУДОВА СИСТЕМ ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ ІЗ ВИКОРИСТАННЯМ ВЛАСТИВОСТЕЙ "ЗОЛОТОГО ПЕРЕТИНУ" Ю.Є. Яремчук, В.С. Катаєв	110
ПРОБЛЕМАТИКА ФОРМУВАННЯ СИСТЕМИ ПОНЯТЬ У ГАЛУЗІ КІБЕРБЕЗПЕКИ В.В. Цуркан	111
ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ТА СИСТЕМ ВИЯВЛЕННЯ КІБЕРНЕТИЧНИХ АТАК І.Ю.Субач, В.С. Рябчун, В.В. Фесьоха	112

УДК 621.391.7

Ю. Є. Яремчук, д.т.н., В. С. Катаєв

Вінницький національний технічний університет, Україна, Вінниця, Хмельницьке шосе, 95

## Побудова систем захисту мовної інформації із використанням властивостей "золотого перетину"

*Анотація:* Представлені результати досліджень можливості використання методу розміщення акустичних випромінювачів на основі принципу "золотого перетину" при побудові систем захисту мовної інформації.

*Summary:* We investigated the possibility of practical application of the method of placement of acoustic emitters in the design of acoustic protection information. The method is based on the principle of "golden section".

*Ключові слова:* Захист мовної інформації, акустичні канали витоку, золотий перетин.

Загроза витоку інформації через акустичні та віброакустичні канали є загальновідомою. Суть її полягає у тому, що мовна інформація, яка озвучується у виділеному приміщенні, поширюється у вигляді акустичних хвиль і за межі самого приміщення.

Для захисту від такого типу загроз існує багато різних методів та засобів, однак найчастіше використовуються засоби активного захисту. Проблема активного захисту полягає у тому, що у деяких випадках кількість проблемних точок у приміщенні може сягати значної кількості і, при встановленні на кожній із них активного захисту, загальний рівень акустичних завад буде на стільки високий, що на об'єкті створюються некомфортні умови.

Досліджувався принципово інший підхід вирішення даної проблеми. Як відомо, для досягнення високої якості звуковідтворення акустичні характеристики кімнати для прослуховування необхідно наблизити до певних оптимальних значень. Це досягається формуванням "акустично правильної" геометрії приміщення, а також за допомогою спеціальної акустичної обробки внутрішніх поверхонь стін і стелі. При цьому власні резонанси приміщення можуть вкрай негативно вплинути на якість звучання.

На основі принципу "золотого перетину" Джорджем Кардасом було запропоновано розміщення гучномовців у кімнаті для прослуховування.

Як розвиток цієї пропозиції ми запропонували метод розміщення акустичних систем у будь-якому прямокутному симетричному приміщенні з пропорційними розмірами. Установка акустичних систем у замкнутому приміщенні призводить до виникнення інтерференційних спотворень, обумовлених взаємодією прямого звуку колонок і відбитими звуковими хвилями від огорожувальних конструкцій. Використання принципу "золотого перетину" дозволяє розташувати колонки у кімнаті таким чином, щоб розузгодити частоти, на яких проявляються акустичні дефекти і виключити або значно зменшити унісон шкідливих резонансів.

Частоти, на яких виникає небажана акустична взаємодія, пропорційні відстані від гучномовців до стін приміщення і в основному розташовані у діапазоні 50-250 Гц. На звучання акустичної системи, розташованої у приміщенні прямокутної форми, найбільше впливають спотворення, обумовлені взаємодією хвилі гучномовця з найближчою боковою стіною, хвилі гучномовця з фронтальною стіною та хвилі гучномовця з дальньою боковою стіною. Таким чином, при побудові системи і визначенні місця розміщення акустичних колонок, необхідно враховувати не тільки розміри приміщення, але й його форму, відповідно варіанти розташування акустичних систем у кімнатах різної форми, і методи боротьби з небажаними акустичними дефектами будуть дещо відрізнятися, оскільки вони залежать від особливостей конкретного приміщення.

Застосування даного методу при побудові систем захисту мовної інформації дозволить створювати акустичні завади, які будуть поширюватись у приміщенні без втрат, тобто при тій самій вихідній потужності генератора шуму рівень акустичних завад у різних точках приміщення буде вищим. Таким чином для забезпечення захищеності інформації, а саме виконання норм щодо співвідношення сигнал/завада у даних точках можна буде знизити загальний рівень сигналів генераторів, разом з чим знизиться і загальний рівень шумів у приміщенні.