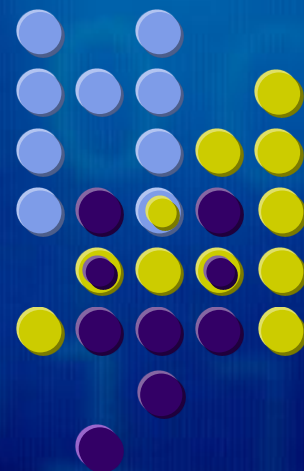


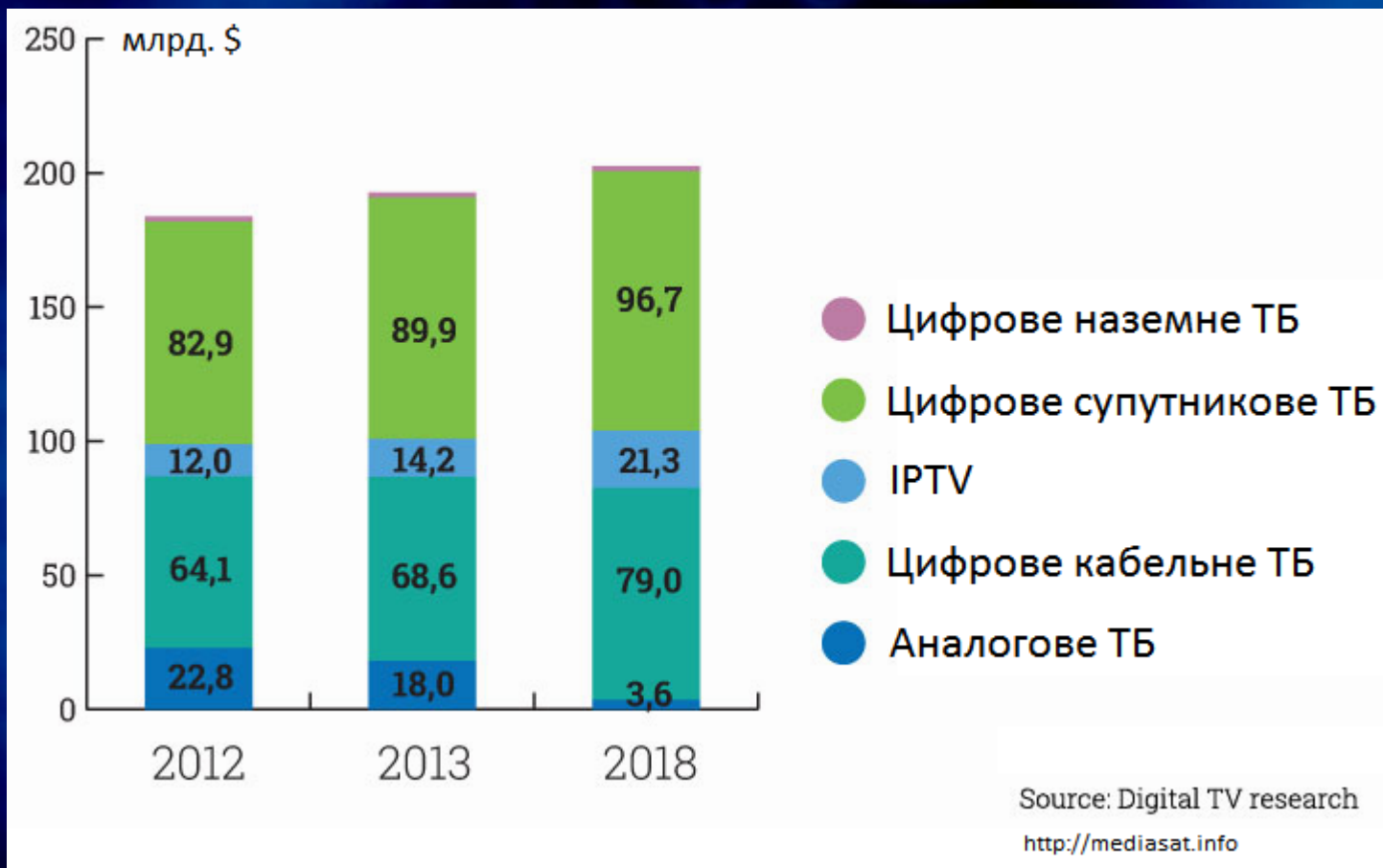
Стеганографічна обробка і захист контенту цифрового мовлення

Кафедра телекомунікаційних систем
tko@nau.edu.ua, ajiekc1980@gmail.com



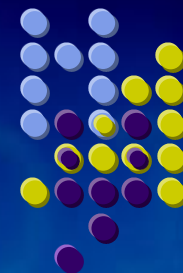
Сучасний стан проблеми

Глобальний розподіл прибутків платного ТВ за платформами

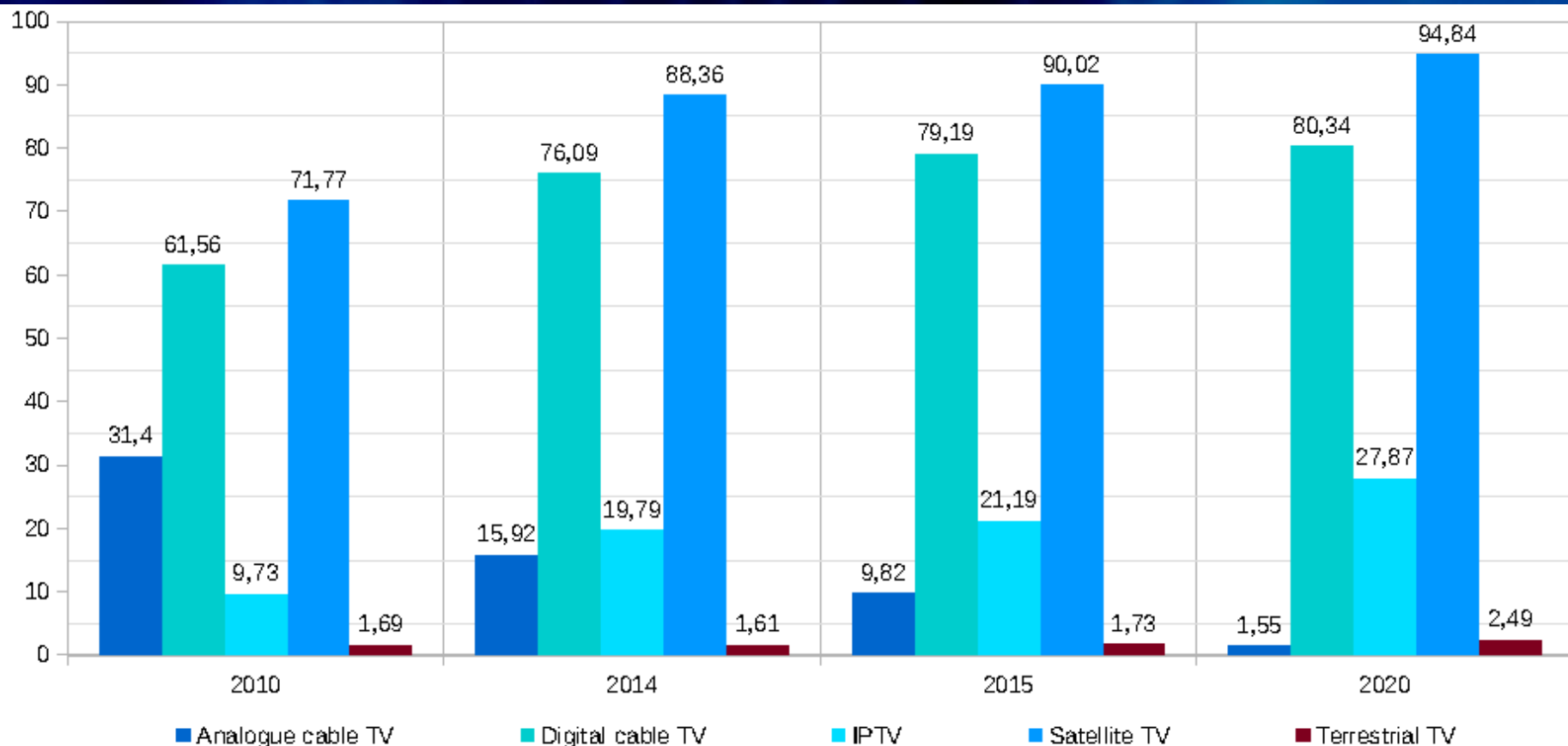


Джерело: **Digital TV Research** (<http://mediasat.info/2015/02/12/rynok-dth-v-ukraine-tekushhaya-situaciya/>)

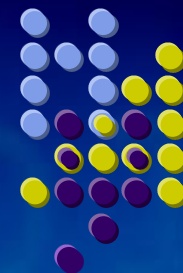
Сучасний стан проблеми



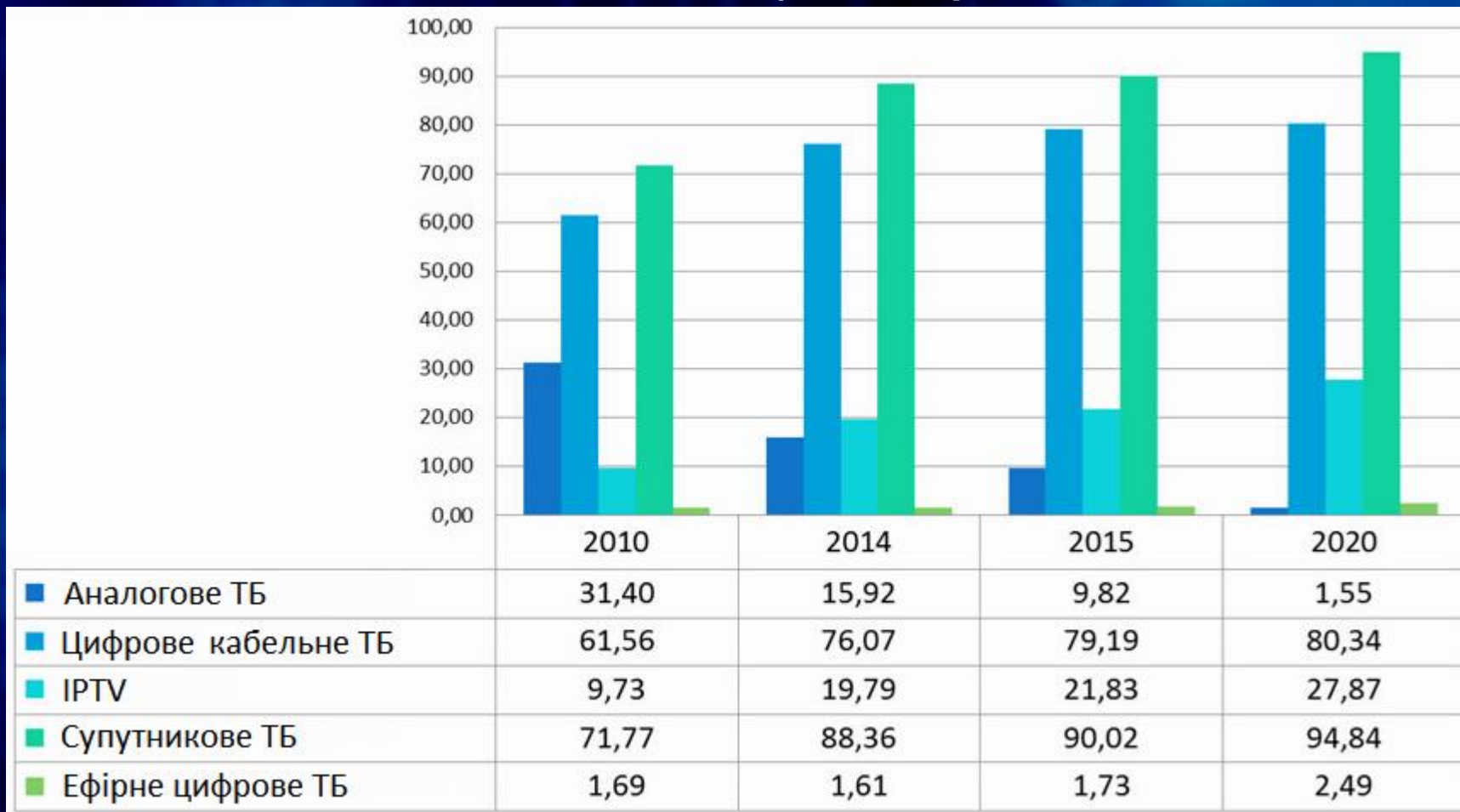
Прибутки платного ТВ у світі (млрд. \$)



Сучасний стан проблеми

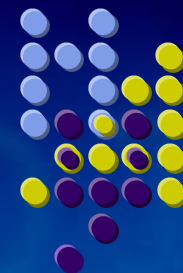


Розподіл прибутків платного ТВ у світі за платформами (млрд. \$)

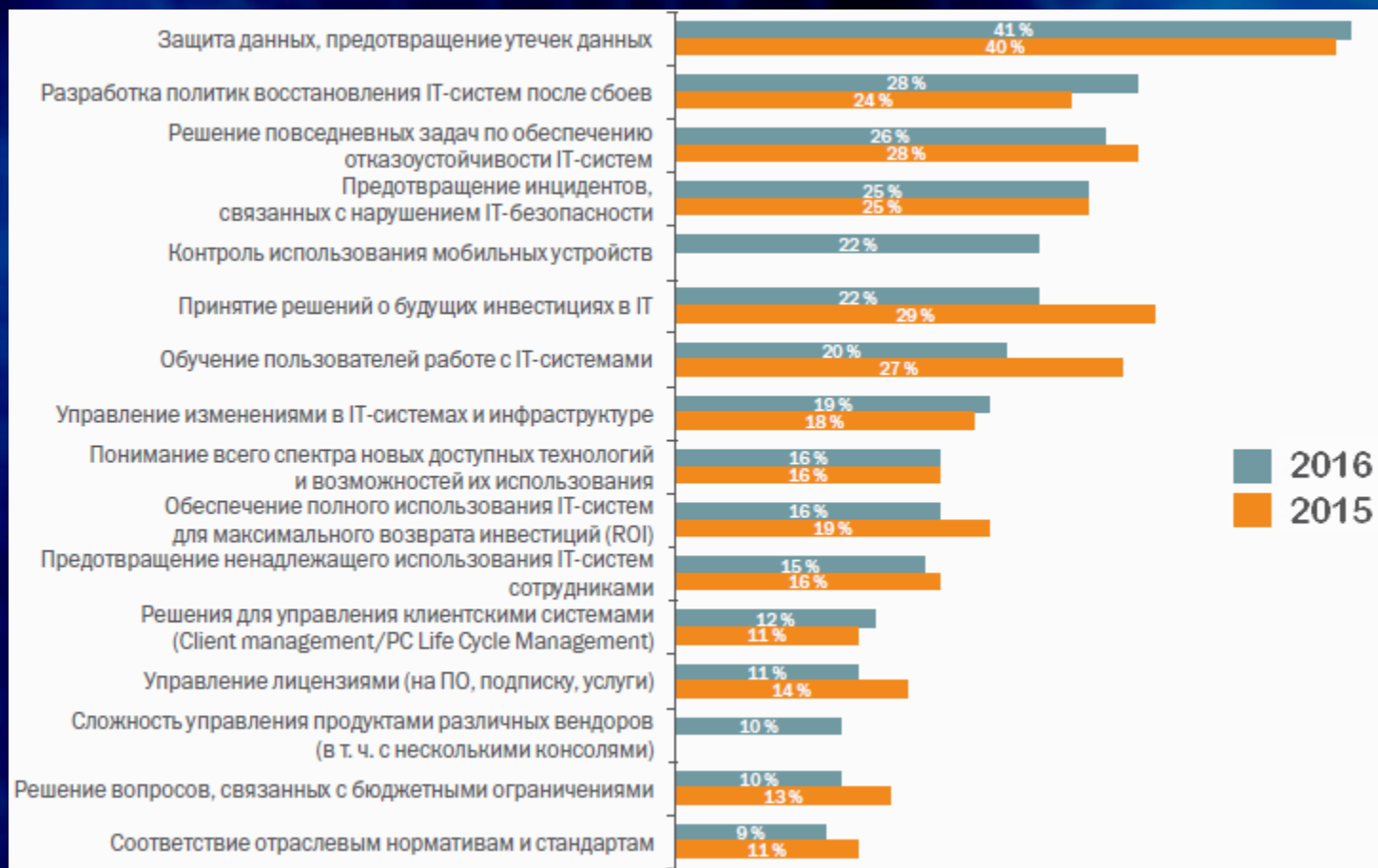


Джерело: **Digital TV Research** (<http://mediasat.info/2016/06/03/dth-market-ukraine/>)

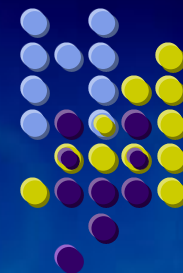
Сучасний стан проблеми



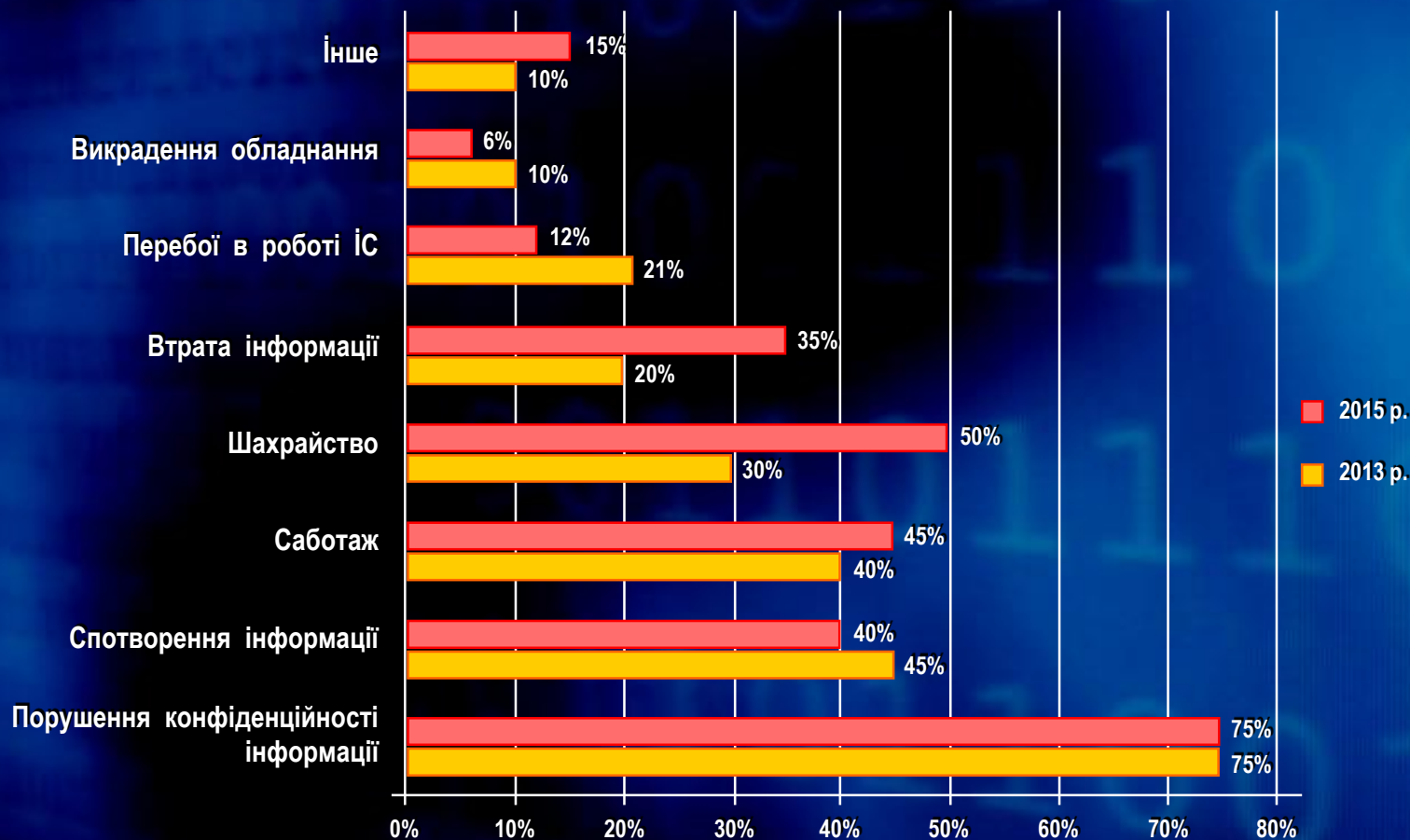
Розставлення пріоритетів ІТ-відділами компаній



Сучасний стан проблеми



ІТ-загрози для світових компаній



Джерело: *InfoWatch* (<http://www.infowatch.ru/>)

Сучасний стан проблеми



Серед завдань науково-технічного забезпечення розвитку телекомунікацій є:

- ⚡ підвищення ефективності їх використання з урахуванням обмеженості ресурсів, задіяних для розвитку;
- ⚡ проведення досліджень з впровадження новітніх технологій і забезпечення ефективності використання РЧР;
- ⚡ формування і надання великої кількості нових послуг;
- ⚡ впровадження цифрового телерадіомовлення;
- ⚡ розвиток аудіовізуальних систем і служб;
- ⚡ проведення досліджень методів аналізу і синтезу нових систем зв'язку і рішень з урахуванням специфіки існуючих телекомунікаційних мереж, світових інноваційних тенденцій, а також прогнозів перспективних шляхів розвитку телекомунікацій;
- ⚡ забезпечення дієвої захищеності авторських прав і прав інтелектуальної власності, з оперативним контролем доступу до сучасного медіапродукту і конфіденційної інформації.

Мета і задачі проекту



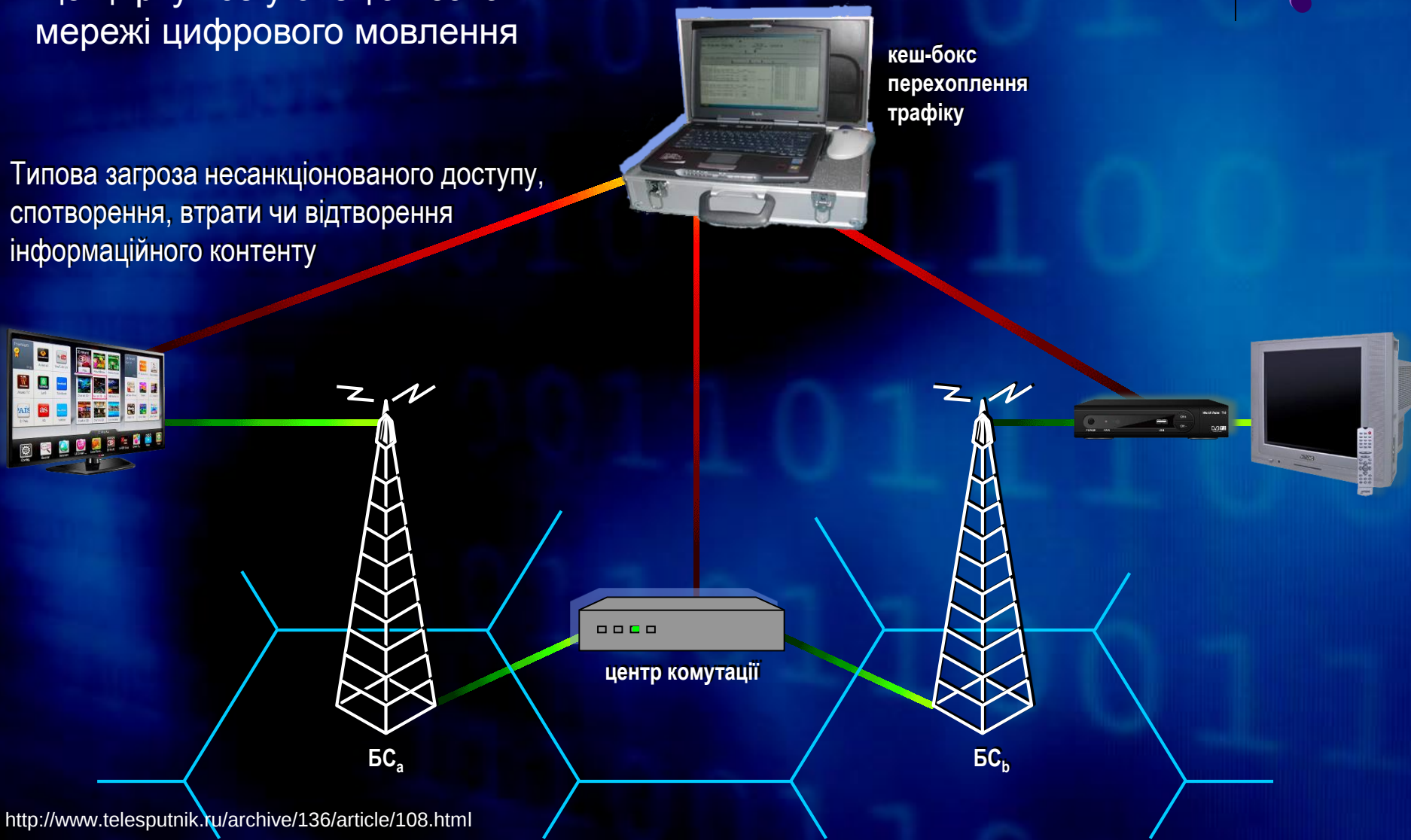
Мета проекту: підвищення ефективності використання мереж цифрового мовлення

Задачі проекту:

- 📌 аналіз принципів і особливостей цільової мережі цифрового мовлення, а також використовуваних в ній алгоритмів обробки контенту;
- 📌 формалізація концепції побудови, розробка структурної схеми і представлення математичних моделей систем стеганографічної обробки і захисту контенту цільової мережі цифрового мовлення;
- 📌 розробка програмних моделей стеганографічної обробки і захисту контенту цільової мережі цифрового мовлення;
- 📌 теоретичне обґрунтування й адаптація використання відомих методів і алгоритмів комп'ютерної стеганографії у складі модифікованої мережі цифрового мовлення;
- 📌 визначення ефективності застосування стеганографічних алгоритмів обробки і захисту контенту, передаваного модифікованою мережею цифрового мовлення.

Об'єкт проекту:

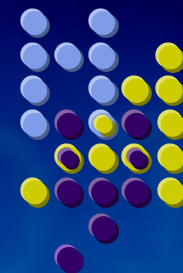
процеси обробки і захисту інформації,
що циркулює у спеціалізованій
мережі цифрового мовлення



Типова загроза несанкціонованого доступу,
спотворення, втрати чи відтворення
інформаційного контенту

Предмет проекту:

стеганографічна обробка і захист контенту спеціалізованої мережі цифрового мовлення.



Методи проектування:

- 📌 цифрова обробка сигналів;
- 📌 гармонічний і спектральний аналіз;
- 📌 дискретна математика і кодування;
- 📌 аналітичне та імітаційне комп'ютерне моделювання (програмування).

Комп'ютерна стеганографія



- **Головна задача стеганографії:**

приховання факту існування конфіденційних даних при їх передаванні, зберіганні, обробці.

- **Напрямки застосування стеганографії:**

- прихована передача даних (класична стеганографія);
- завадостійка автентифікація;
- захист даних від несанкціонованого копіювання;
- відстеження поширення інформації мережами зв'язку;
- пошук інформації в мультимедійних базах даних...

- **Методи комп'ютерної стеганографії:**

приховання повідомлень у цифрових даних, які, як правило, мають аналогову природу (мова, зображення, аудіо- чи відеозаписи). Можливе використання текстових файлів або виконувальних файлів програм.

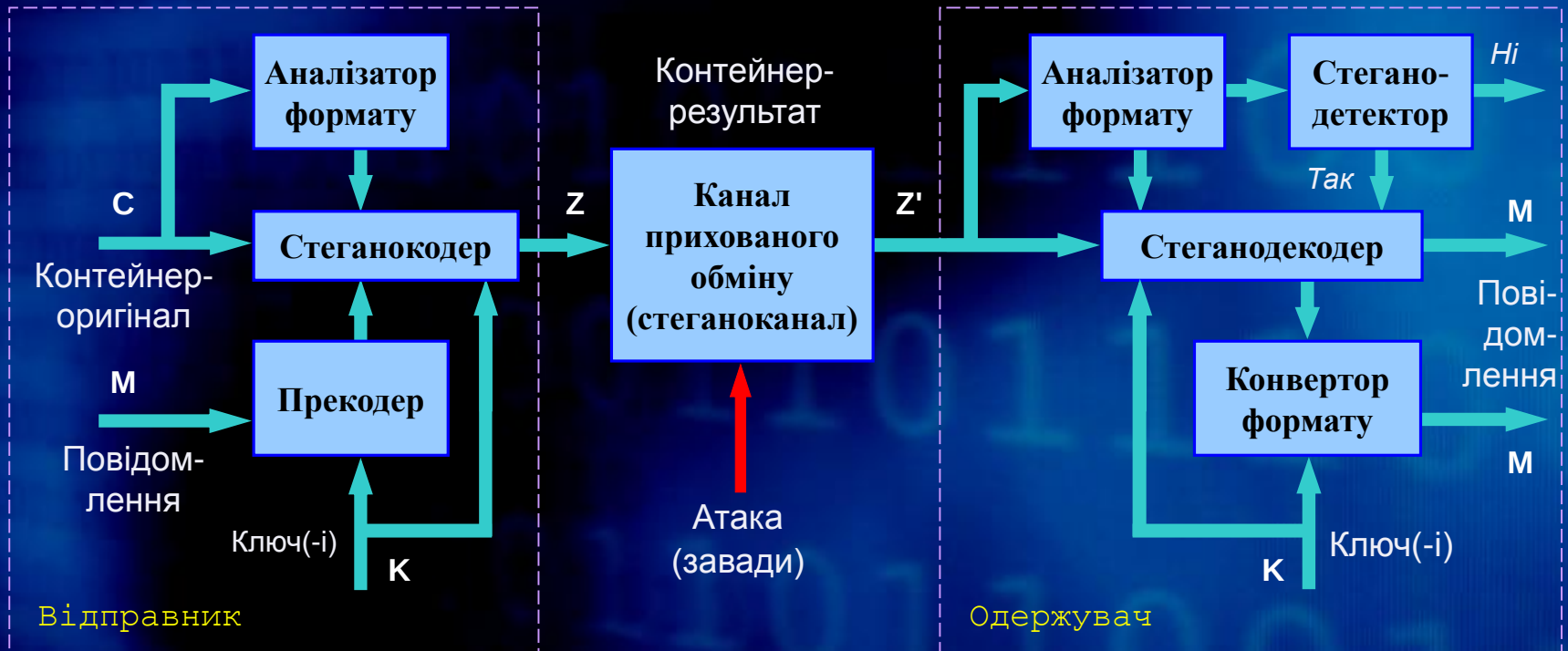
Стеганографічна система, як компонент цифрового мовлення



Проблемні ситуації у сфері цифрового мовлення,
що можуть бути вирішені шляхом стеганографічної обробки
його контенту:

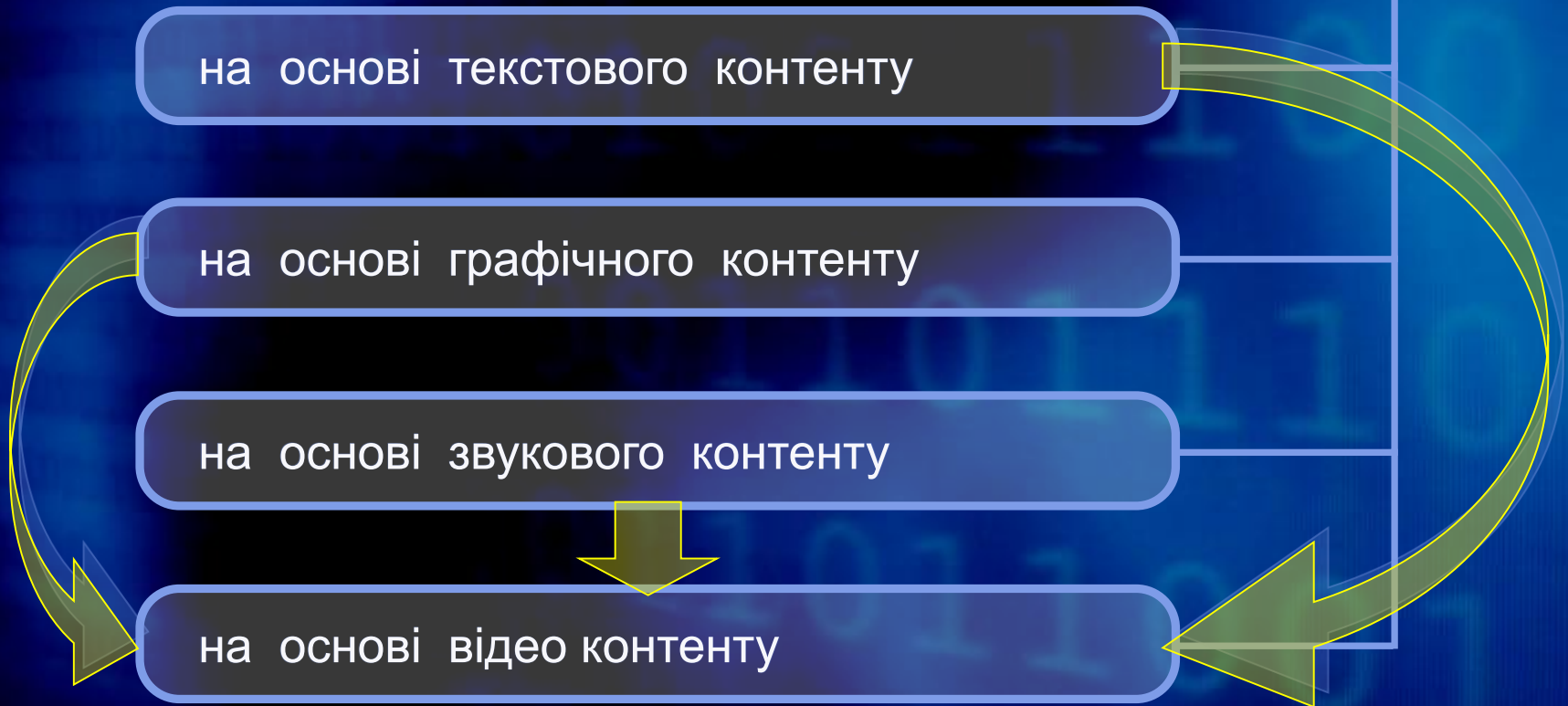
Сфери використання стеганографії у цифровому мовленні	
<u>Захист прав власності</u> Контроль за тиражуванням і розповсюдженням аудіо- та додаткової інформації	<u>Приховане передавання конф. інформації</u> Застосування у конфіденційних цілях, а також у випадках існування обмежень на використання криптографії
<u>Прихована анотація об'єктів</u> Оптимізація організації мультимедійних баз даних і контентосховищ радіомовників	<u>Приховане передавання додаткової інформації</u> Реконфігурація мультіплексу для збільшення економічних і технічних переваг від використання ЦМ

Структурна схема стеганографічної системи

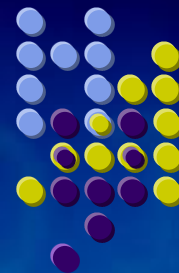


Типові групи стеганографічних систем

(за форматом контейнера)



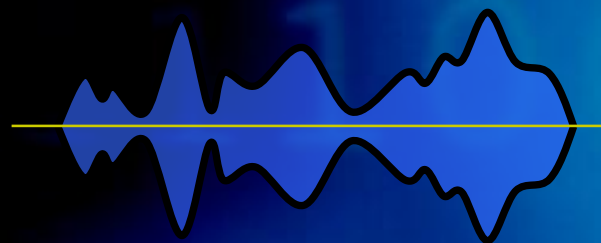
Стеганографічні системи



конфіденційні
дані



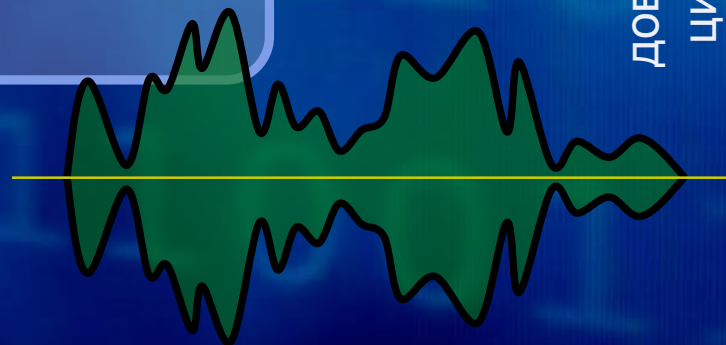
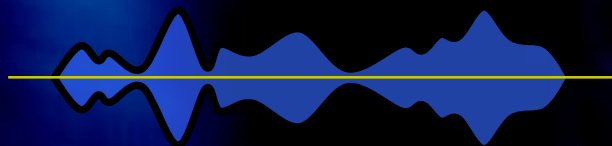
стеганограма



довільна програма
цифрового радіо

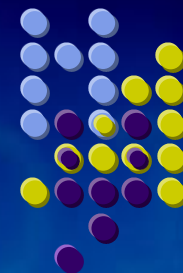
конфіденційна
на основі звукового контенту
телефонна розмова

стеганограма

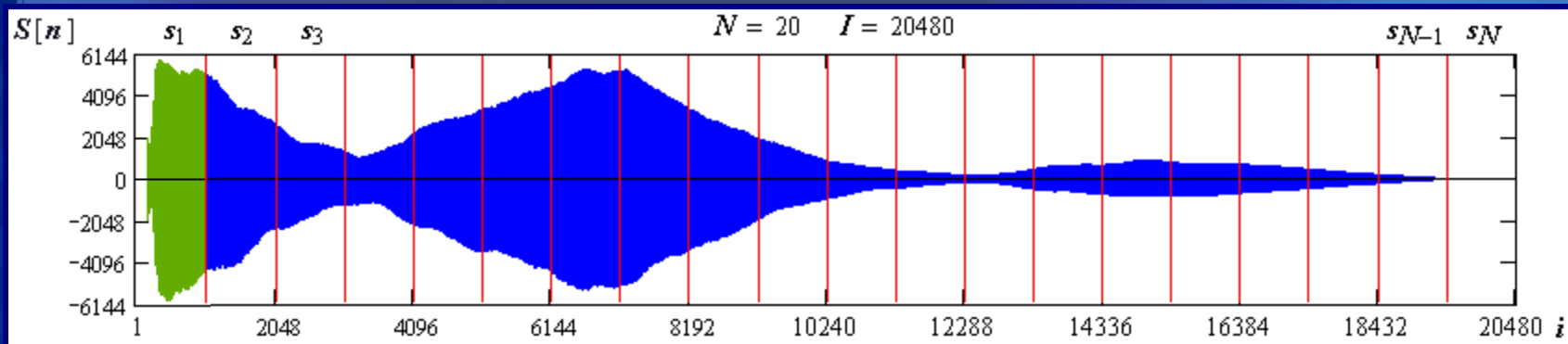


Приклад роботи стеганосистеми

(метод фазового кодування)

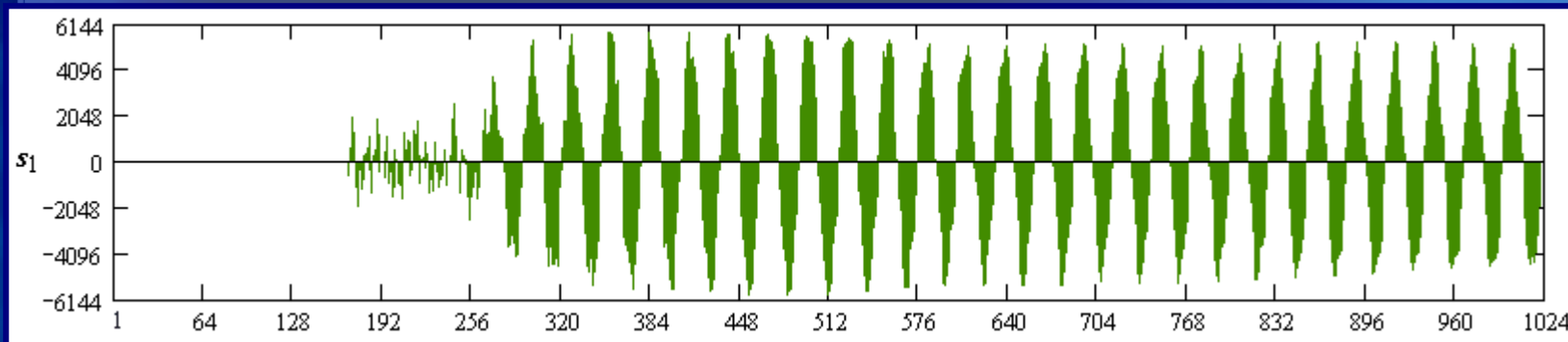
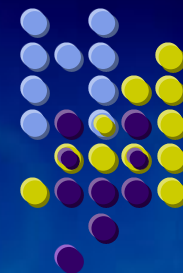


1. Аудіопослідовність $S[i]$, ($1 \leq i \leq I$) розбивається на серію N сегментів $s_n[i]$, ($1 \leq n \leq N$):



Приклад роботи стеганосистеми

(метод фазового кодування)



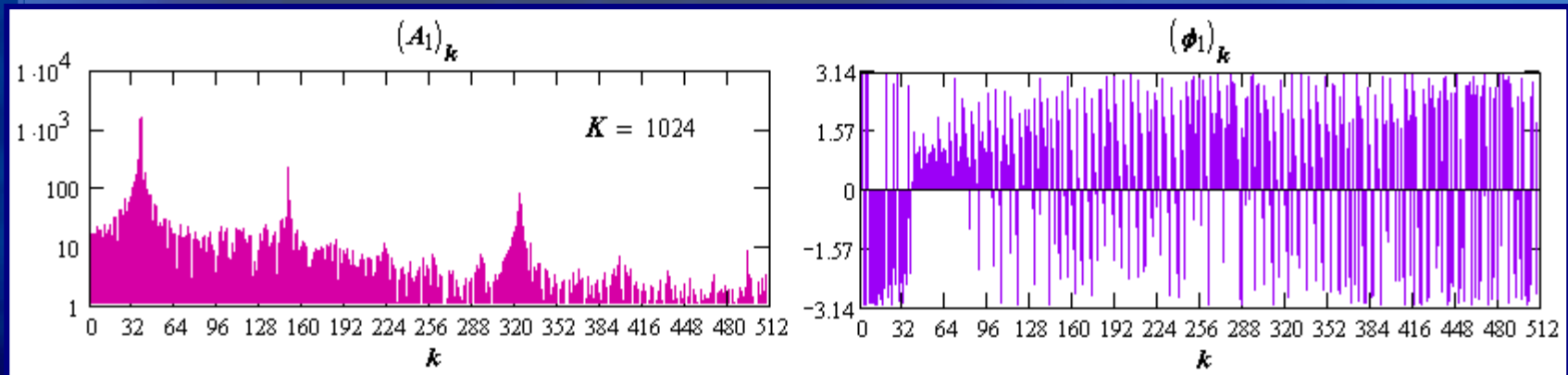
Приклад роботи стеганосистеми

(метод фазового кодування)



2. K -точкове ШПФ n -го сегменту ($K = I/N$), в результаті чого одержується n масивів фаз $\phi_n(\omega_k)$ і амплітуд $A_n(\omega_k)$ для $1 \leq k \leq K/2+1$.

Графічна інтерпретація амплітудного і фазового масивів для сегмента s_1 :



Приклад роботи стеганосистеми

(метод фазового кодування)



3. Запам'ятовується різниця фаз $\Delta\varphi$ між кожними сусідніми сегментами для $1 \leq n \leq N$:

$$\Delta\varphi_{n+1}(\omega_k) = \varphi_{n+1}(\omega_k) - \varphi_n(\omega_k);$$
$$\Delta\varphi_1(\omega_k) = 0.$$

4. Двійкова послідовність даних представляється як $\varphi_D = \pi/2$ або $\varphi_D = -\pi/2$, відображуючи відповідно "1" або "0":

$$\varphi'_1 = \varphi_D.$$

Приклад роботи стеганосистеми

(метод фазового кодування)



5. З урахуванням різниці фаз $\Delta\phi$ формується новий масив фаз для $n > 1$:

$$\phi'_1(\omega_k) = \phi_D$$

$$\phi'_2(\omega_k) = \phi'_1(\omega_k) - \Delta\phi_2(\omega_k)$$

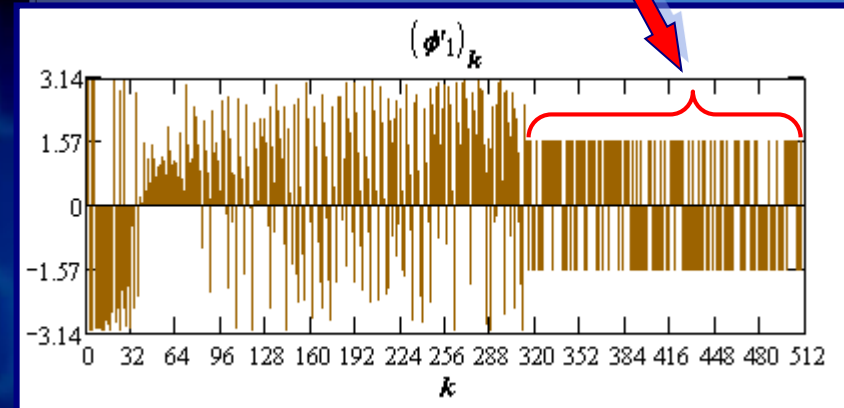
...

$$\phi'_n(\omega_k) = \phi'_{n-1}(\omega_k) - \Delta\phi_n(\omega_k)$$

...

$$\phi'_N(\omega_k) = \phi'_{N-1}(\omega_k) - \Delta\phi_N(\omega_k)$$

дані

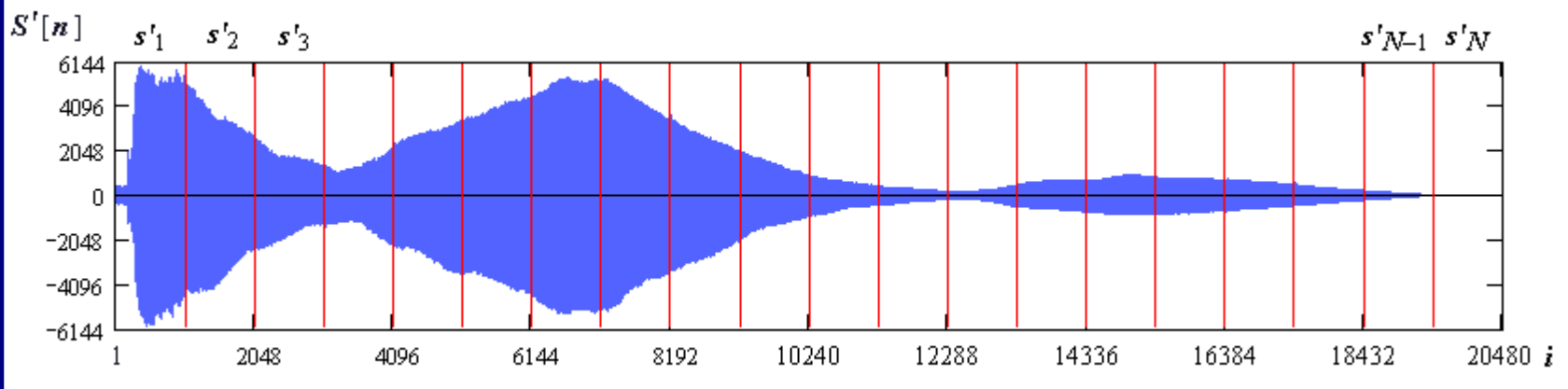


Приклад роботи стеганосистеми

(метод фазового кодування)



6. Відновлення сегментів шляхом застосування оберненого ШПФ до первинного масиву амплітуд $A_n(\omega_k)$ і модифікованого масиву фаз $\phi'_n(\omega_k)$.



Приклад роботи стеганосистеми

(метод фазового кодування)



7. Одержувачеві повинні бути відомими:

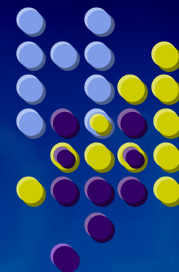
- номер і довжина сегмента, до якого було проведено вбудовування даних ;
- точки ШПФ і інтервал даних у одержаному масиві фаз для визначеного сегмента.

Двійковий елемент даних:

$-\pi/2 \rightarrow \text{"0"}$

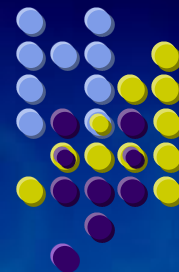
$+\pi/2 \rightarrow \text{"1"}$

Практичні зиски:



- 1) При розширенні сфер послуг, надаваних системою цифрового мовлення на основі стеганографічної обробки, зникає потреба у створенні окремих субканалів передавання додаткової інформації (конфіденційної, службової, сервісної тощо), що дає можливість:
 - а) збільшити кількість програм, трансльованих у смузі частот окремого каналу мовлення (збільшити ефективність і прибутки від використання обмеженого РЧР);
 - б) збільшити бітову швидкість цифрових потоків довільного набору програм або ж застосувати більш потужне завадостійке кодування введенням додаткової надмірності, підвищивши таким чином якість надаваних послуг.
- 2) Можливість використання мережі цифрового мовлення для організації радіомереж передавання конфіденційної інформації — завдяки прихованню самого факту існування відомостей з обмеженим колом доступу.

Вже зроблене у цьому напрямку:



1) Видано монографію*:

Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. — К. : «МК-Пресс», 2006. — 288 с.

2) Отримано патент на винахід:

Пат. 89054 UA, МПК Н 04 J 4/00. Спосіб цифрового радіомовлення з передаванням сервісної інформації стеганографічним каналом передавання даних, створеним на основі аудіоінформації радіо-програм, що транслюються, і пристрій для його реалізації / Бабак В.П., Конахович Г.Ф., Пузыренко О.Ю.; власник Нац. авіац. ун-т. — № а 2007 02490; заявл. 06.03.2007; опубл. 25.12.2009, Бюл. № 24.

3) Захищено кандидатську дисертацію:

Пузыренко О.Ю. Комп'ютерні системи стеганографічної обробки і захисту інформації у цифровому звуковому мовленні : 05.13.05. — К. : 2012, — 160 с.

4) Написано декілька десятків статей у фахових виданнях.

* Праця має більше 330 цитувань за базою *Google Scholar*.