Головним завданням цього дослідження є об’єднання в єдину математичну модель характеристик надійності та інформаційної безпеки. Для моделювання характеристик надійності та інформаційної безпеки можна використовувати марківські процеси і експоненціальний розподіл можливих подій. Як показник, що безпосередньо характеризує властивості системи, доцільно використовувати коефіцієнт готовності. Класичним підходом до моделювання мережі є приведення її до деревовидного графу. Одним з підходів є нормування коефіцієнту готовності ліній зв'язку та мереж передачі даних, але існуючі правила не застосовуються до корпоративних мереж передачі даних, побудованих поверх Інтернету, оскільки мережа, сформована таким чином, частково абстрагується від певного постачальника послуг.

З врахуванням вищесказаного, розробка методу оцінки ефективності функціонування вузла зв'язку корпоративної мережі з врахуванням інформаційної безпеки є актуальним науково-технічним завданням.

д.т.н., проф. Лєнков С.В. (ВІКНУ)
к.т.н., доц. Тітова В.Ю. (ХмНУ)
к.т.н., доц. Муляр І.В. (ХмНУ)
Дацюк Р.М. (ХмНУ)

Аналіз стеганографічних алгоритмів

Актуальність вивчення стеганографії постійно зростає, оскільки з поширенням персональних комп’ютерів, і особливо Інтернету, можливість конфіденційно передавати інформацію привертає увагу значної кількості людей. Переважна більшість теоретичних та практичних досліджень у галузі стеганографії присвячена розробці нових та вдосконаленню існуючих методів приховування даних. Кількість останніх постійно зростає з часом, але в сучасній науковій літературі відсутня чітка класифікація таких методів, що ускладнює пошук і не дозволяє повною мірою оцінити рівень існуючих досягнень для їх подальшого ефективного використання.

Аналізуючи процес розвитку комп’ютерної стеганографії, можна сказати, що в найближчі роки інтерес до розробки її методів буде дедалі більше зростати. Актуальність проблеми інформаційної безпеки постійно зростає і стимулює пошук нових методів захисту інформації. З іншого боку, швидкий розвиток інформаційних технологій дає можливість впроваджувати ці нові методи захисту.

Стеганографічні методи поряд із криптографічними займають важливе місце серед методів захисту інформації. Але якщо в криптографії наявність зашифрованого повідомлення саме по собі привертає увагу зловмисника, то в стеганографії прихований зв’язок залишається невидимим, що робить організацію цього процесу досить актуальною.

Загальною особливістю стеганографічних методів є те, що приховане повідомлення або додаткова інформація вбудовується в якийсь нешкідливий, непомічений об’єкт або контейнер, в результаті чого з’являється приховане повідомлення, яке потім відкрито транспортується до одержувача за каналом

зв'язку. або зберігаються як такі

Але, більшість стеганографічних алгоритмів дозволяють приховувати невеликі об’єми інформації. Але на практиці часто виникає потреба в прихованій передачі значних масивів даних. Тому дослідження в напрямку розробки методу, що приховує великі об'єми інформації в відомих графічних форматах, для їх подальшої передачі є актуальним.

Метою дослідження є розробка стеганографічних методів і алгоритмів, які вбудовують і приховують великі об'єми інформації в графічні зображення формату JPEG з подальшою передачею цієї інформації х.

Список використаних джерел:

1. Аграновский А.В. Стеганографія, цифрові водяні знаки і стеганоаналіз / Аграновский А.В., Балакін А.В., Грибунин В.Г., Сапожников С. - М.: Книга ВНЗ, 2009. - 220 с.

к.т.н., доц. Чешун В.М. (ХмНУ)
к.т.н., доц. Орленко В.С. (ХмНУ
к.т.н., доц. Шваб В.К. (ВІКНУ)
Гончар Р.М. (ХмНУ)
Халіманенко С.М. (ВІКНУ)

Оптимальне нерівномірне кодування в підвищенні криптостійкості шифрів

В умовах стрімкого розвитку інформаційних технологій, постійного збільшення обсягів інформації в кіберпросторі і зростання її цінності, а також через появу нових загроз щодо її цілісності і конфіденційності надзвичайної актуальності набувають заходи кібербезпеки. Одним із базових заходів є криптографічний захист даних, про що свідчить поява і масштабне використання великої кількості методів та алгоритмів симетричного й асиметричного шифрування з різними функціональними можливостями і принципами дії (алгоритми DES-базовий, подвійний і потрійний DES, IDEA, ГОСТ 28147, Діффі-Хелмана, RSA тощо) та спроби їх постійного вдосконалення.

Підвищення криптостійкості алгоритмів шифрування можна досягти попередньою підготовкою вхідних даних, в ході якого забезпечується порушення статистичних даних повторюваності символів вхідного тексту, тобто, збільшення характеристик його ентропії. Одним із варіантів такої підготовки вхідного тексту може бути застування методів оптимального нерівномірного кодування - ОНК (кодування Шеннона-Фано, Хафмана).

В узагальненому алгоритмі підготовки даних до криптографічного шифрування із застосуванням ОНК можна виділити три базових операції:

1. Заміна кодових комбінацій K_i символів вхідного тексту, що мають однакову розрядність, кодовими комбінаціями K_i' різної розрядності із урахуванням статистичних характеристик появи зазначених символів в тексті.

2. Формування двійкового представлення вихідного тексту у вигляді послідовності кодових комбінацій заміни K_i' різної розрядності.

3. Розподіл одержаної послідовності на кодові комбінації K_j'' однакової