УДК 681.511:3
DOI: 10.15587/2313-8416.2015.47796

АНАЛІЗ СТІЙКОСТІ СТЕГАНОГРАФІЧНИХ СИСТЕМ

© Н. М. Ліщина

В статті описана класифікація атак на стеганографічні системи, визначено умови в яких стеганосистеми будуть стійкими. Розглядаються теоретичні та практичні аспекти стеганографії. Для аналізу стійкості стеганографічних систем до виявлення факту передачі секретних повідомлень розглядається теоретико-інформаційна модель стеганографічних системи з пасивним зловмисником. Розглянуті умови забезпечення стійкості стеганосистем згідно побудованої моделі
Ключові слова: *стеганографічна система, модель порушника, стійкість, активні атаки, пасивні атаки, стеганографічний контейнер*

The classification of attacks on steganographic systems is described, the conditions in which steganographic systems will be strong are determined in the article. The theoretical and practical aspects of steganography are considered. To analyze the stability of steganographic systems to detect the fact of transfer secret messages it is considered information-theoretic model of the steganographic systems with the passive attacker. The conditions to ensure the stability of steganographic systems are considered according to the developed model
Keywords: *steganographic system, violator model, stability, active attacks, passive attacks, steganographic container*

1. Вступ

Порівняно з досить добре дослідженими криптографічними системами поняття та оцінка безпеки стеганографічних систем більш складні і допускають більшу кількість їх тлумачень. Зокрема, це пояснюється як недостатнім теоретичним та практичним опрацюванням питань безпеки стеганосистем, так і великою різноманітністю завдань стеганографічного захисту інформації. Стеганосистеми водяних знаків повинні виконувати завдання захисту авторських і майнових прав на електронні повідомлення при різних спробах активного зловмисника перекручування або стирання вбудованої в них автентифікуючої інформації. Системи цифрових відеозображень повинні забезпечити автентифікацію відправників електронних повідомлень. Таке завдання може бути покладене на криптографічні системи електронного цифрового підпису (ЕЦП) даних, але, на відміну від стеганосистем водяних знаків, відомі системи ЕЦП не забезпечують захист авторства не тільки цифрових, але й аналогових повідомлень, і в умовах, коли активний зловмисник вносить спотворення в повідомлення, що захищаються, та автентифікацію інформації. Інші вимоги з безпеки висуваються до стеганосистем, призначених для приховування факту передачі конфіденційних повідомлень від пасивного зловмисника. Також має свої особливості забезпечення імітостійкості стеганосистем до введення в прихований канал передачі неправдивої інформації [1].

2. Постановка проблеми

Як і для криптографічних систем захисту інформації, безпека стеганосистем описується та оцінюється їх стійкістю. Під стійкістю різних стеганосистем розуміється їх здатність приховувати від зловмисника факт прихованої передачі повідомлень, здатність протистояти спробам зловмисника зруйнувати, спотворити, видалити повідомлення, що таємно передаються, а також здатність підтвердити або спростувати справжність приховано переданої інформації.

3. Аналіз літературних даних

Аналіз стійкості стеганографічних систем висвітлюється у працях багатьох вчених. Даються основні уявлення про існуючі засоби, алгоритми і математичні моделі комп'ютерної стеганографії. Описуються моделі прихованого збереження і передачі інформації в інформаційно обчислювальних мережах, архітектури програмних комплексів стеганографічного перетворення інформації. Наводиться аналіз практичних аспектів реалізації програмних комплексів прихованої передачі інформації і методів стеганографічного перетворення [2]. Розглядаються теоретичні та практичні аспекти стеганографії, класифікація стеганосистем і методів вбудовування, детально досліджені питання підвищення пропускної здатності стеганоканала, забезпечення стійкості і непомітності впровадження, наведено більше 50 алгоритмів вбудовування даних [3]. На сьогодні розробка стеганосистем, стійких до виявлення наявності вкрапленої інформації або її псування, видалення або викривлення, у більшості випадків залежить від майстерності фахівців, що їх створюють. Проведення досліджень для розвитку теоретичної бази комп'ютерної стеганографії є актуальною задачею сьогодення.

4. Практична оцінка стійкості стеганографічних систем

Розглянемо визначення стеганостійкості, опишемо класифікацію атак на стеганосистеми і спробуємо визначити умови, в яких стеганосистеми можуть бути стійкими.

Досліджуємо стеганосистеми, завданням яких є прихована передача інформації. У криптографічних системах ховається вміст конфіденційного повідомлення від зловмисника, у той час як у стеганографії додатково ховається факт існування такого повідомлення. Тому визначення стійкості і зламу цих систем різні. У криптографії система захисту інформації є стійкою, якщо, маючи перехвачену криптограму,

зловмисник не здатний читати, що міститься в ній.

Назвемо в загальному випадку стеганосистему нестійкою, якщо протиборчі сторони здатні виявляти факт її використання.

Розглянемо базову модель стеганосистеми, в якій в стеганокодері використовується стеганографічна функція f вбудовування за секретним ключем секретного повідомлення M в контейнер C, а в стеганодекодері стеганографічна функція φ його добування по тому ж ключу. Зі стега по функції φ витягується вбудоване повідомлення і при необхідності контейнер. У результаті спотворення при вбудовуванні вплив випадкових і навмисних перешкод передачі, а також похибок при отриманні відновленого одержувачем повідомлення $\hat{M}$ може відрізнятися від оригіналу M.

Зі стега по функції ϕ витягується вбудоване повідомлення і при необхідності контейнер [4].

У результаті спотворення при вбудовуванні вплив випадкових і навмисних перешкод передачі, а також похибок при отриманні відновленого одержувачем повідомлення може відрізнятися від оригіналу M. Аналогічно, отриманий контейнер буде відрізнятися від вихідного С. Контейнер обов'язково буде спотворюватися при вбудовування секретного повідомлення. У ряді стеганосистем необхідно відновлювати контейнер, оскільки він фізично становить звичайні повідомлення кореспондентів відкритого зв'язку, під прикриттям яких здійснюється прихований зв'язок.

За ознакою використання ключа дана стеганосистема класифікується як симетрична. Логічно припустити, що стійкість стеганосистеми повинна забезпечуватися при використанні несекретних функцій вбудовування f і витягнення ϕ. Безпека стеганосистем має спиратися на такі принципи їх побудови, при яких якщо зловмисник не знає секретної ключової інформації, то навіть при повному знанні функцій вбудовування і витягнення прихованої інформації, законів розподілу прихованих повідомлень, контейнерів і стега він не здатний встановити факт прихованої передачі інформації.

Розглянемо класифікацію атак зловмисника, який намагається визначити факт прихованої передачі повідомлення та при встановленні цього факту намагався переглядати їх.

Атака тільки з стеганограмою. Зловмиснику відома одна або певна кількість стеганограм і він намагається визначити, чи не містять вони прихованих повідомлень, і якщо так, то намагається читати їх.

Зловмиснику дуже важко зламати стеганосистему в цій атаці. Це пояснюється тим, що при невідомості ні вихідного контейнера, ні якої-небудь частини прихованого повідомлення можна отримати дуже велику кількість помилкових розшифровок, серед яких жодній не можна віддати перевагу.

Атака з відомим контейнером. Зловмиснику доступні один або множина пар контейнерів і відповідних їм стеганограм. Зауважимо, що в цій атаці зловмисник знає вихідний вигляд контейнера, що дає йому істотні переваги порівняно з першою атакою. Наприклад, в якості відомого зловмиснику контейнера може служити студійний запис музичного твору, що передається радіомовним каналом з вбудованою інформацією.

Атака з обраним контейнером. Зловмисник здатний нав'язати для використання в стеганосистемі конкретний контейнер, що володіє якимись перевагами для проведення стеганоаналізу порівняно з усією безліччю контейнерів. Удосконалена версія цієї атаки: атака з адаптивно обраними контейнерами. Зловмисник нав'язує контейнер, аналізує отриманий стег.

Атака з відомим повідомленням. Зловмиснику відомо вміст одного або декількох прихованих повідомлень і він намагається встановити факт їх передачі або використовування стеганоключа.

Якщо зловмиснику відомі деякі приховані повідомлення та відповідні їм стеганограми, то його завданням є визначення ключа стеганосистеми для виявлення та читання інших приховано переданих повідомлень, або при неможливості визначення ключа завданням зловмисника є побудова методів безключового читання або визначення факту передачі прихованої інформації.

Атака з обраним повідомленням. Зловмисник здатний нав'язати для передачі по стеганосистемі конкретне повідомлення і він намагається встановити факт його прихованої передачі, при цьому використовується секретний ключ. Також можлива атака з адаптивно обраним повідомленням, в яке зловмисник послідовно підкидає приховану інформацію підбираємого повідомлення та ітеративно зменшує свою невизначеність про використання стеганосистеми та її параметри.

Крім того, можливі різні поєднання перерахованих атак, у яких зловмисник здатний знати або вибирати контейнери в яких таємно передаються повідомлення. Ступінь ефективності атак на стеганосистему зростає у міру збільшення знань зловмисника про використовувані контейнери, приховані повідомлення, об'єм перехвачених стеганограм і його можливостей з нав'язування обраних контейнерів та повідомлень.

Введемо моделі зловмисника, який намагається протидіяти прихованій інформації. Дотримуючись К. Шеннон, назвемо першою з цих моделей теоретико-інформаційну. Нехай, як це прийнято для систем захисту інформації, для стеганосистем виконується принцип Кергоффа: зловмисник знає повний опис стеганосистеми, йому відомі ймовірнісні характеристики прихованих повідомлень, контейнерів, ключів, формуються стеганограми. Зловмисник має необмежені обчислювальні ресурси, запам'ятовуючі пристрої довільно великої ємності, має у своєму розпорядженні нескінченно багато часу для стеганоаналізу і йому відомо довільну множину перехвачених стеганограм. Єдине, що невідомо зловмиснику, – використовуваний ключ стеганосистеми. Якщо у даній моделі зловмисник не в змозі встановити, міститься чи ні приховане повідомлення в контрольованому стегі, то назвемо таку стеганосистему теоретико-інформаційно стійкою до атак пасивного зловмисника або досконалою [5].

Стійкість різних стеганосистем може бути розділена на стійкість до виявлення факту передачі приховуваної інформації, стійкість до витягання приховуваної інформації, стійкість до нав'язування помилкових повідомлень за допомогою прихованого зв'язку, стійкість до відновлення секретного ключа стеганосистеми.

Очевидно, що якщо стеганосистема є стійкою до виявлення факту передачі приховуваної інформації, то логічно припустити, що вона при цьому є стійкою і до читання приховуваної інформації. Зворотне в загальному випадку неправильне. Стеганосистема може бути стійкою до читання приховуваної інформації, але факт передачі певної інформації під прикриттям контейнера може виявлятися зловмисником.

Стійкість стеганосистеми до нав'язування помилкових повідомлень за допомогою прихованого зв'язку характеризує її здатність виявляти і відкидати сформовані зловмисником повідомлення, що вводяться ним в канал передачі прихованих повідомлень з метою видачі їх за істинні, які виходять від законного відправника. Стійкість до відновлення секретного ключа стеганосистеми характеризує її здатність протистояти спробам зловмисника обчислити секретну ключову інформацію даної стеганосистеми. Якщо зловмисник здатен визначити ключ симетричної стеганосистеми, то він може однозначно виявляти факти передачі прихованих повідомлень і читати їх чи нав'язувати помилкові повідомлення без будь-яких обмежень. Таку подію можна назвати повною компрометації стеганосистеми.

Якщо зловмисник здатний вирахувати ключ вбудованого водяного знака будь-якого автора інформаційних ресурсів, то він може поставити цей водяний знак на будь-який контейнер. Тим самим зловмисник дискредитує або водяний знак даного автора, або цілком всю систему ЦВДЗн. В обох випадках ставиться під сумнів законність прав одного або всіх власників інформаційних ресурсів на те, що дійсно їм належить.

Якщо система ЦВДЗн побудована як симетрична, то декодер повинен використовувати конфіденційний ключ виявлення водяного знака. Отже, такий детектор проблематично вбудовувати в пристрої, що експлуатуються, до яких доступ зловмисника технічно складно обмежити, наприклад, в персональні програвачі DVD-дисків. Несиметрична система ЦВДЗн використовує секретний ключ вбудовування водяного знака у контейнери і відкритий ключ перевірки ЦВДЗн.

Зауважимо, що побудова несиметричних систем ЦВДЗн та інших стеганосистем викликає суттєві практичні проблеми. По-перше, несиметричні системи, як відомо з криптографії, в реалізації виявляються обчислювально складніше симетричних систем. По-друге, крім вимог до стійкості ключа стеганосистеми, висуваються жорсткі вимоги до стійкості системи ЦВДЗн до різноманітних спроб зловмисника перекручування водяного знака. Несиметричні системи побудовані на основі односпрямованих функції з потайним ходом. Принципи побудови переважної більшості відомих односпрямованих функцій з потайним ходом такі, що будь-яке завгодно мале спотворення вихідного значення цих функцій при використанні законним одержувачем потайного ходу призводить до істотного розмноженню помилок у повідомленні, що приймається. Цей недолік односпрямованих функцій характерний і для нині використовуваних несиметричних криптографічних систем. Однак там його можна компенсувати використанням додаткових заходів підвищення вірогідності переданих криптограм або цифрових підписів повідомлень. Але в стеганосистемах використання цих же способів підвищення достовірності ускладнене. По-перше, їх застосування демаскує прихований канал. По-друге, активний зловмисник в атаках на стеганосистему ЦВДЗн має великі можливості підібрати такий руйнівний вплив, при якому доступні методи підвищення вірогідності інформації можуть виявитися неефективними. Наприклад, якщо відправник використовує алгоритми завадостійкого кодування, які забезпечують захист приховуваного повідомлення від рівновірогідних розподілених помилок, то зловмисник підбирає закон розподілу пакетувальних помилок, при якому канальний декодер отримувача не здатний їх виправити і розмножує помилки при декодуванні [6].

5. Апробація результатів дослідження

Для аналізу стійкості стеганографічних систем до виявлення факту передачі секретних повідомлень розглянемо теоретико-інформаційну модель стеганосистеми з пасивним зловмисником.

Зловмисник A спостерігає повідомлення, що передаються відправником B одержувачу D. A не знає, чи містять ці повідомлення нешкідливий контейнер C або стег S з приховуваною інформацією. Будемо вважати, що B може знаходиться в одному з двох режимів: він або активний або пасивний. Коли B активий, він перетворює контейнер з вкладенням в нього секретного повідомлення M, використовуючи секретний ключ K. Отримавши стег S, D повинен бути здатний витягти з нього повідомлення M, використовуючи ключ K. Стеганосистема повинна задовольняти співвідношенням:

1. $H(S/CMK)=0$. Сформований відправником стег S однозначно визначається значеннями контейнера C, ключа K і повідомлення M.

2. $H(M)>0$. Невизначеність до моменту передачі прихованого повідомлення M і для одержувача і для зловмисника строго більше нуля.

3. $H(SM/SK)=0$. Одержувач D має однозначно відновити приховане повідомлення M з прийнятого стега S, користуючись ключем K.

Будемо вважати, що імовірнісні розподіли множин прихованих повідомлень, контейнери, стеги і ключі відомі для всіх учасників інформаційного протиборства. Додатково одержувач D знає, активна чи ні відправник B. A, спостерігаючи повідомлення, що передаються B, повинна встановити, передається каналом зв'язку приховувана інформація чи ні. Для виявлення факту використання стеганосистеми A намагається визначити, чи відповідає інформаційний потік, що передається, розподілу контейнерів або розподілу стега. Якщо A здатна встановити, що в контрольованому каналі передаються повідомлення з

розподілом стеганограм, то факт прихованої передачі інформації від B до D доведено, а використована ними стеганосистема є нестійкою.

У розглянутій моделі стеганосистеми відомо ймовірнісний розподіл порожніх контейнерів, які позначаються P_C, і ймовірнісний розподіл стеганограм, які позначаються P_S. Зловмисник у контрольованому каналі зв'язку може спостерігати множину можливих порожніх контейнерів і стеганограм. Позначимо цю множину можливих спостережень Q. Зловмисник, спостерігаючи передане повідомлення $q \in Q$, висуває дві гіпотези H_C і H_S. Якщо справедлива гіпотеза H_C, то повідомлення q породжено згідно з розподілом P_C, а якщо справедлива H_S, то q відповідає розподілу P_C. Правило рішення полягає в розбитті множини Q на дві частини так, щоб призначити одну з двох гіпотез кожному можливому повідомленню $q \in Q$. У цьому завданні розрізнення можливі два типи помилок: помилка першого типу, яка полягає у встановленні гіпотези H_s, коли вірною є H_c, і помилка другого типу, коли прийнято рішення H_c при вірній гіпотезі H_s. Ймовірність помилки першого типу позначається α, імовірність помилки другого типу – β [4].

Використовуємо відносну ентропію $D(P_c||P_s)$ між відділами P_c і P_s для оцінки стійкості стеганосистеми при пасивному зловмиснику. Стеганосистема називається є стійкою проти пасивного зловмисника, якщо $D(P_C||P_S) \leq \varepsilon$. Якщо $\varepsilon=0$, то стеганосистема є досконалою. Якщо розподіли контейнера і стега однакові, то $D(P_c||P_s)=0$, і така стеганосистема є досконалою. Це означає, що ймовірність виявлення факту передачі приховуваної інформації не змінюється від того, спостерігає зловмисник інформаційний обмін від B до D чи ні [4].

Розглянемо умови забезпечення стійкості стеганосистем. Відомо співвідношення між ентропією, відносною ентропією і розміром алфавіту $|\mathbf{X}|$ для довільних випадкових змінних S і C. Зазначимо, що контейнери C і стега S належать одному і тому ж алфавіту X. Якщо змінна S рівновірогідна і незалежно розподілена, то $H(C)+D(P_C||P_S)=\log|X|$.

Якщо змінна C є рівновірогідною і незалежно розподіленою, то виконується рівність $H(C)=\log|X|$ і тоді $D(P_C||P_S)=0$.

6. Висновки

Отже, в розглянутій моделі, якщо в якості контейнерів C використовувати випадкові послідовності і приховуване повідомлення буде описуватися також випадковими послідовностями, то сформовані стеги S не будуть мати жодних статистичних відмінностей від порожніх контейнерів, і така стеганосистема буде досконалою. Якщо приховувана інформація становить осмислені повідомлення, які описуються послідовностями з нерівномірними і залежними між собою символами, то до необхідного вигляду їх легко привести шляхом шифрування будь-яким стійким шифром.

Література

1. Кузнецов, О. О. Стеганографія [Текст]: навч. пос. / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х.: Вид. ХНЕУ, 2011. – 232 с.

2. Агрsuperновский, А. В. Стеганография, цифровые водяные знаки и стеганоанализ [Текст] / А. В. Агрsuperновский. – М.: Вузовская книга, 2009. – 220 с.

3. Грибунин, В. Г. Цифровая стеганография [Текст] / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М.: Солон-Пресс, 2009. – 265 с.

4. Хорошко, В. О. Основи комп'ютерної стеганографії : навч. посібн. для студентів і аспірантів [Текст] / В. О. Хорошко, О. Д. Азаров, М. В. Шелест та ін. – Вінниця: ВДТУ, 2003. – 143 с.

5. Конахович, Г. Ф. Компьютерная стеганография. Теория и практика [Текст] / Г. Ф. Конахович, А. Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.

6. Поліновський, В. В. Інформаційна технологія для досліджень методів стеганографії і стегоаналізу [Текст] / В. В. Поліновський // Міжвузівський збірник "Комп'ютерно-інтегровані технології: освіта, наука, виробництво". – 2011. – № 5. – С. 236–242.

References

1. Kuznetsov, O. O., Yevseiev, S. P., Korol, O. H. (2011). Stehanohrafiia : navchalnyi posibnyk. Kharkiv: Vyd. KhNEU, 232.

2. Agranovskii, A. V. (2009). Steganografiia, tsifrovie vodianie znaki i steganoanaliz. Moscow: Vuzovskaia kniga, 220.

3. Hrybunyn, V. H., Okov, Y. N., Turyntsev, Y. V. (2009). Tsyfrovaia stehanohrafyia. Kyiv: Solon-Press, 265.

4. Khoroshko, V. O., Azarov, O. D., Shelest, M. V. et al. (2003). Osnovy kompiuternoi stehanohrafii: navch. posibn. dlia studentiv i aspirantiv. Vinnytsia: VDTU, 143.

5. Konakhovych, H. F., Puzyrenko, A. Iu. (2006). Kompiuternaia stehanohrafyia. Teoryia y praktyka. Kyiv: MK-Press, 288.

6. Polinovskyi, V. V. (2011). Informatsiina tekhnolohiia dlia doslidzhen metodiv stehanohrafii i stehoanalizu. Mizhvuzivskyi zbirnyk "Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo", 5, 236–242.

Рекомендовано до публікації д-р тех. наук, професор Рудь В. Д.
Дата надходження рукопису 22.07.2015

Ліщина Наталія Миколаївна, кандидат технічних наук, доцент, кафедра комп'ютерних технологій, Луцький національний технічний університет, вул. Потебні, 56, м. Луцьк, Україна, 43018
E-mail: lischyna@gmail.com