ближенных решений / Л.А.Заде. – М. : Мир, 1976. – 165 с.

19. Паніотто В.І. Статистичний аналіз соціологічних даних / В.І.Паніотто, В.С.Максименко, Н.М.Харченко. – К. : Вид. дім "КМ Академія", 2004. – 269 с.

20. Тернер Д. Вероятность, статистика и исследование операций / Д.Тернер. – М. : Статистика, 1976. – 432 с.

21. Паклин Н. Бизнес-аналитика: от данных к знаниям / Н.Паклин, В.Орешков. – 2-е изд., испр. – СПб. : Питер, 2009. – 708 с.

22. Флейс Дж. Статистические методы для изучения таблиц долей и пропорций / Дж. Флейс. – М. : Финансы и статистика, 1989. – 319 с.

23. Ахиезер А. Критические пороги социальных систем / А.Ахиезер, Г.Гольц // Общественные науки и современность. – 1992. – № 1. – С. 45-56.

24. Седов Е.А. Информационно-энтропийные свойства социальных систем / Е.А.Седов // Общественные науки и современность. – 1993. – № 5. – С. 92-100.

25. Сороко Э.М. Золотые сечения, процессы самоорганизации и эволюции систем: Введение в общую теорию гармонии систем / Э.М.Сороко. – М. : КомКнига, 2006. – 264 с.

26. Блаттер К. Вейвлет анализ. Основы теории / К.Блаттер. – М. : Техносфера, 2004. – 280 с.

27. Чуи К. Введение в вейвлеты / К.Чуи. – М. : Мир, 2001. – 412 с.

28. Давыдов А.А. Системный подход в социологии: новые направления, теории и методы анализа социальных систем / А.А.Давыдов. – М. : КомКнига, 2005. – 328 с.

Аннотация: В статье рассмотрены четыре группы математических методов оценки состояния безопасности структурно сложных систем: эвристические, стохастические, аналитические и нелинейной динамики. Проанализированы и систематизированы математические модели определения граничных значений индикаторов безопасности этих систем.

Ключевые слова: математические методы, математические модели, нелинейная динамика, оценка состояния безопасности структурно сложных систем, граничные значения индикаторов безопасности.

Abstract: The article researches four groups mathematical methods of to assess the security status of structurally complex systems: heuristic, stochastic, analytical and nonlinear dynamics. The mathematical models for determining the boundary value of these security systems are analyzed and systematized.

Key words: mathematical methods, mathematical models, nonlinear dynamics, safety assessment of structurally complex systems, the boundary value problems of security indicator.

УДК 004.056.5 (045)

МЕЛЬНИК Сергій Володимирович
КАЩУК Владислав Іванович

МЕТОДИ ЦИФРОВОЇ СТЕГАНОГРАФІЇ: СТАН ТА НАПРЯМИ РОЗВИТКУ

Постановка проблеми. Стеганографія як один із напрямів людської діяльності має багатовікову історію. Так, слово "стеганографія" у перекладі з грецької мови означає "тайнопис", тобто процес приховування самого факту передачі або зберігання інформації шляхом її маскування у різних об'єктах (або засобах) неживої чи живої природи, що можуть мати дискретні властивості та змінюватись людиною.

Стеганографія як наука стала відома громадськості лише в останні десятиріччя, хоча методи приховування інформації разом із шифрувальною справою (криптографією) відомі ще із часів Давнього світу. Історично розвиток методів стеганографії безпосередньо пов'язаний із технологічним розвитком цивілізацій, спочатку як ремесло і мистецтво приховування інформації, а потім вже як фахової галузі знань та науки [1].

Сучасну стеганографію прийнято розділяти на класичну, комп'ютерну і цифрову. У межах класичної стеганографії розглядаються методи приховування текстової інформації, що використовували властивості самої текстової інформації, зображень, поведінки і зовнішності людини, розташування предметів, стану і порядку роботи пристроїв та систем різного типу, хімічні властивості матеріалів тощо. У свою чергу, комп'ютерна і цифрова стеганографія розглядає методи приховування будь-якої електронної інформації (текст, мова, зображення, відео, програма), що використовують технологічні можливості сучасних інформаційно-телекомунікаційних систем.

Класична стеганографія фактично є вже історією, яка надає важливі знання щодо основних принципів побудови методів стеганографії та стеганоаналізу, оцінки їх ефективності (стеганографічної стійкості), а також можливостей і ефективності їх практичного використання у межах заходів інформаційного протиборства та історичних прикладів конфліктології взагалі.

Сучасна стеганографія та її методи активно розвиваються, використовуючи новітні можливості сучасних ІТ-технологій для реалізації, по суті, класичних підходів до приховування інформації. Йдеться про використання: апаратних функцій управління накопичувачами електронної інформації; файлової структури операційних систем; форматів представлення даних (файлів); протоколів інформаційного обміну, і навіть тих, що використовуються в методах криптографічного і технічного захисту інформації.

У сучасному світі можна виокремити кілька практичних причин, що зумовлюють практичний інтерес до комп'ютерної і, насамперед, цифрової стеганографії. На наш погляд, це наявність таких практичних проблем, як:

– обмеження на використання засобів криптографічного захисту інформації в деяких країнах світу та новими технологічними можливостями для діяльності спеціальних служб в сучасних умовах;

– управління комп'ютерними (ІТ) інцидентами та комп'ютерної (ІТ) криміналістики, внаслідок широких технологічних можливостей для порушення спостережності за діями користувачів і процесів інформаційно-телекомунікаційних систем (далі – ІТС), що може призвести до реалізації загроз витоку, нав'язування, знищення та блокування інформації;

– захист прав власності на інформацію, представлену в цифровому вигляді, та розвиток технологій захисту інформації від підробки та несанкціонованого тиражування.

Спостерігається науковий інтерес до сфери стеганографії, який полягає у формалізації її методів, поняття ефективності їх побудови і використання, підходів до аналізу та оцінювання тощо.

Вважаємо, що достатньо актуальними науково-практичними питаннями у цій сфері є:

методологічні аспекти формалізації процесів протидії порушенню спостережності інформаційного обміну в ІТС;

показники ефективності та критерії оцінювання методів, засобів та заходів аудиту інформаційних потоків у глобальних та локальних мережах;

моделі забезпечення кібернетичної безпеки людини, суспільства, держави в частині протидії загрозам порушення спостережності інформаційного обміну в ІТС.

Аналіз останніх досліджень і публікацій щодо технологічних питань спостережності кіберпростору свідчить про недостатність системних досліджень цієї тематики. У розвиток вітчизняної стеганографії зробили вагомий внесок М.Є.Шелест, Г.Ф.Конахович, А.Ю.Пузиренко, В.О.Хорошко та інші учені і практики, який полягає у розробці та удо-

сконаленні моделей, методів та засобів стеганографії і стеганоаналізу, оцінюванні їх характеристик тощо. Однак, на наш погляд, доцільно також звернути увагу на питання формалізації, моделювання та оцінювання стеганографічних систем, що передбачають також комплексне використання засобів технічного і криптографічного захисту інформації, технологічний та організаційний аспект.

Метою статті є огляд можливостей методів цифрової стеганографії в контексті побудови стеганографічних систем у сучасних умовах розвитку ІТ-технологій. Визначення основних позицій застосування системного підходу до формалізації процесів забезпечення спостережності інформаційних процесів.

Виклад основного матеріалу. Цифрова стеганографія – це галузь знань та технічна наука, яка розглядає методи:

– організації прихованих каналів передачі і зберігання інформації з використанням різних цифрових об'єктів (засобів і систем зберігання і передачі електронної інформації);

– вбудовування спеціальних міток в електронну інформацію з метою захисту від підробки та несанкціонованого тиражування (цифрових водяних знаків – електронних голографічних елементів).

Методам цифрової стеганографії, способам їх програмної реалізації та оцінкам стійкості присвячено достатня кількість доступної на сьогодні літератури [2-5]. У цих працях стеганографія розглядається як один із сучасних видів захисту інформації, таких як технічний і криптографічний захист інформації, голографічний захист носіїв інформації, методи біометричної автентифікації тощо. Однак з огляду на технологічні можливості цифрової стеганографії та загальні завдання інформаційної і національної безпеки методи цифрової стеганографії доцільно розглядати передусім через призму загроз безпеці інформації у кіберпросторі, що дають змогу реалізовувати:

– канали прихованого агентурного зв'язку та середовища прихованого зберігання інформації;

– канали прихованого управління різними технічними об'єктами критичної кібернетичної інфраструктури;

– технічні канали витоку інформації з обмеженим доступом в ІТС;

– технічні канали несанкціонованого доступу до інформації з обмеженим доступом в ІТС;

– "камуфляж" шкідливого програмного забезпечення в різних програмних середовищах, наприклад, функцію запуску троянської програми під час перегляду фотографії у соціальній мережі тощо.

У цьому контексті слід звернути увагу на те, що сучасна прикладна стеганографія узагальнює такі поняття, як:

сховище (тайник) та *контейнер* (засіб зберігання чи передачі прихованої інформації);

– *тайникова операція* (порядок обміну повідомленнями через сховище);

– *сигнальна інформація* (порядок обміну повідомленнями про небезпеку чи безпеку особистого контакту; знак підтвердження або спростування факту відсилання чи отримання кореспонденції, матеріальних і технічних засобів тощо);

– *канал передачі/витоку/несанкціонованого доступу* (*стеганографічний канал* передачі/зберігання інформації шляхом використання *стеганограм,* тобто заповнених контейнерів, що містять приховану інформацію).

Як наслідок, питання цифрової стеганографії і стеганоаналізу становлять безпосередній інтерес у завданнях розвідувальної і контррозвідувальної діяльності, управління комп'ютерними (ІТ) інцидентами та комп'ютерної (ІТ) криміналістики, що стосуються передусім:

– методів приховування інформації в контейнерах, способів їх технічної реалізації, підходів до оцінювання стійкості з урахуванням можливостей їх комплексного застосування з методами криптографічного і технічного захисту інформації;

– визначення найбільш ефективних із погляду стеганографічної стійкості контейнерів, які доступні у сучасних ІТ-технологіях;

– методів аналізу потоків інформації на предмет виявлення стеганографічних каналів;

– методів відновлення, зміни та знищення прихованої інформації із стеганограм.

При цьому методи цифрової і комп'ютерної стеганографії у сукупності з методами криптографічного і технічного захисту інформації, організаційно-технічними заходами безпеки можуть звести наявність доказової бази противоправної діяльності у кіберпросторі до нуля. Наприклад, такі електронні докази, як засоби шифрування і тайнопису, що використовуються для приховування інформації, самі можуть бути приховані в операційній системі комп'ютера, прикладному програмному забезпеченні та будь-яких інших файлах на будь-яких носіях.

Відомо, що у сучасних захищених ІТС (автоматизованих системах класу 3), доступ до мережі Інтернет яких не використовується лише як захищений канал передачі даних між окремо виділеними комп'ютерами, будь-яка обрана політика безпеки не зможе забезпечити гарантований рівень захисту інформації. Відповідно, можуть мати місце комп'ютерні інциденти та виникає необхідність щодо їх адекватного управління.

Безумовно, в сучасних умовах розвитку ІТ-технологій без урахування практичних можливостей методів цифрової і комп'ютерної стеганографії у межах заходів управління інформаційною безпекою [6-8] достатньо проблематично вести мову про ефективність процесів:

– виявлення й оцінки комп'ютерних інцидентів;

– реагування на комп'ютерні інциденти, насамперед, що стосуються питання своєчасної активації адекватних засобів захисту під час моніторингу стану безпеки інформації у мережі;

– застосування превентивних захисних заходів попередження комп'ютерних інцидентів.

Слід звернути увагу на те, що без урахування практичних можливостей методів цифрової і комп'ютерної стеганографії в сучасних ІТ-технологіях також проблематично забезпечити ефективність криміналістичних досліджень комп'ютерної техніки щодо:

– виявлення та зчитування інформації у відкритому та зашифрованому вигляді;

– виявлення шкідливого програмного забезпечення та джерел зараження;

– забезпечення цілісності інформації після вилучення комп'ютерної техніки та носіїв інформації, або після проведення їх дослідження тощо.

У загальному випадку всі методи стеганографії використовують деякий надлишок в обраній для зміни інформації, за рахунок якого приховується необхідна інформація, і це не призводить до суттєвої зміни властивостей контейнера (дискретного об'єкта) та порушення його функціональності (цільового призначення). У свою чергу, методи стеганографічного аналізу використовують імовірнісно-статистичні відхилення властивостей стеганограми від контейнера (дискретного об'єкта з прихованою інформацією від його природного стану), що йому відповідає або може відповідати із деякою ймовірністю. Ефективність цих методів залежить від статистичного розподілу елементів контейнерів, імовірнісного розподілу самих контейнерів, стеганограм та ключів, якщо вони використовуються.

У зв'язку з цим становлять інтерес стеганографічні канали в тих цифрових об'єктах (електронній інформації), де елементи природно розподілені рівноімовірно та незалежно. Це суттєво із погляду стеганографічної стійкості, крім того, не викликає зайвої уваги у супротивника.

У цьому контексті слід також враховувати питання пропускної здатності стеганографічних каналів, бо цей аспект зумовлює їх практичну й економічну ефективність.

З огляду на зазначене слід зосередити увагу на:

1. Криптографічних системах загального і спеціального використання:

– системах аутентифікації за принципом "запит-відповідь" (генерується і передається випадкова послідовність – електронна інформація) – передусім інтернет-протоколи

програмного забезпечення, системи віддаленого управління різними об'єктами, системи, що використовують парольний доступ до інформаційних ресурсів;

– системах електронного цифрового підпису, що використовують алгоритми експоненціального типу, а це фактично всі відомі у світі чинні державні стандарти алгоритмів електронного цифрового підпису – особливо цікавлять платіжні системи.

2. Системах цифрового зв'язку – телефон, передача будь-якої інформації у цифровому форматі, включаючи сигнали управління та діагностики об'єктів віддаленого управління, текстові файли, електронну пошту, чати, зображення, аудіо- і відеофайли.

3. Системах зберігання електронної інформації. Наприклад, інтернет-сайтах або електронних каталогах, інформація в яких динамічно змінюється та не має оригінальних копій (сайти з аудіо-, відеоінформацією та зображеннями, найбільший інтерес становлять ті файли, що мають авторську природу, тобто не мають оригінала).

4. Системах електронних розваг, що передбачають інтенсивний обмін електронною інформацією (як правило, випадковою) в локальних та глобальних комп'ютерних мережах, наприклад, програмних іграшках тощо.

Враховуючи те, що в стеганографії визначені поняття теоретичної (абсолютної) та практичної стеганографічної стійкості, то існують методи і засоби, що дають змогу будувати стеганографічні канали з гарантованою стійкістю, класичний моніторинг яких не має сенсу. Відповідно, становить теоретичний і практичний інтерес комплексне визначення стеганографічної практичної стійкості стеганосистем, що містить у собі інтегральну оцінку:

– математичних властивостей методів стеганографії (класична постановка завдання на оцінювання стеганографічної стійкості до загроз виявлення, зчитування або знищення інформації);

– інженерних властивостей їх технічної реалізації (властивості стеганографічних засобів із погляду інженерно-стеганографічних характеристик, НСД та ПЕМВН);

– організаційно-технічних характеристик побудови та використання стеганосистем у формалізації "людина-машина" (властивості процедур управління ключами та застосування засобів стеганографії).

Як основні показники інтегральної оцінки можна розглянути максимальну ймовірність успішної атаки на стеганосистему (заходу протидії) та необхідний часовий і матеріальний ресурс.

Висновки. Таким чином, цифрова стеганографія і стеганоаналіз як галузь знань та наука є суттєвою складовою технічних завдань удосконалення методів, засобів та заходів управління інформаційною безпекою (технічних заходів попередження правопорушень у кіберпросторі), а також завдань їх розслідування та розкриття в частині комп'ютерної криміналістики.

Дослідження питань цифрової стеганографії і стеганоаналізу, а також технічних способів їх застосування у межах аналізу й оцінки заходів та засобів підготовки і реалізації можливих комп'ютерних інцидентів передбачають змістові знання сучасних ІТ-технологій, методів технічного і криптографічного захисту інформації та їх подолання, методів управління інформаційною безпекою та загальнотеоретичних підходів до моделювання та оцінювання ефективності систем захисту інформації.

Список використаних джерел

1. Мельник С.В. Світові тенденції розвитку цифрової стеганографії в контексті завдань забезпечення інформаційної безпеки держави / С.В.Мельник, С.В.Кондакова // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. – К. : Наук.-вид. відділ НА СБ України, 2010. – С. 134-138.

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

3. Грибунин В.Г. Цифровая стеганография / В.Г.Грибунин, И.Н.Оков, И.В.Туринцев. – М. : СОЛОН-Пресс, 2002. – 272 с.

4. Johnson N.F. Steganography: Seeing the Unseen / N.F.Johnson, S.Jajodia // IEEE Computer. – 1998. – № 2. – P. 26–34.

5. Sokol B. Cryptography and steganography: teaching experience / B.Sokol, V.Yarmolik // Enhanced methods in computer security, biometric and artificial intelligence systems. – Springer-Verlag, London, UK, 2005. – P. 83–92.

6. Міжнародні стандарти "Управління інформаційною безпекою": ISO/IEC 27000.

7. Міжнародний стандарт ISO/IEC TR 18044: 2004 "Менеджмент інцидентів інформаційної безпеки".

8. Міжнародний стандарт ISO/IEC TR 13335-5: 2001 "Керівництво по менеджменту безпеки мережі".

Аннотация: В статье рассматриваются методы современной стеганографии в условиях развития IT-технологий, системный подход к формализации процессов наблюдательности информационных процессов в ИТС.

Ключевые слова: стеганография, методы стеганографии, стеганоанализ, стеганографическая стойкость.

Abstract: The article deals with modern methods of steganography in the development of IT-technologies, as well as system approach to the formalization of the observation information processes in ITS.

Key words: steganography, methods of steganography, steganalysis, steganographic resistance.