УДК 004.056

МЕТОДИ СТЕГАНОГРАФІЧНОЇ ПЕРЕДАЧІ ІНФОРМАЦІЇ В РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТА ПОБУДОВІ ЛОГІКИ СИСТЕМИ ЗАХИСТУ

Ягло В.О., студентка, leramur2003@gmail.com, ХНУ ім. В.Н. Каразіна
Стяглик Н.І., к.п.н., natalia.stiahlyk@karazin.ua, завідувач кафедри інформаційних технологій та математичного моделювання, ХНУ ім. В.Н. Каразіна

Вступ. В сучасному світі, коли збільшується обсяг цифрової інформації і її повсякденне використання, питання конфіденційності та безпеки даних стає критично важливим для багатьох галузей, зокрема в інформаційних технологіях. Небажання авторів або адміністраторів дозволити доступ до цінної інформації третім особам стає тяжкою проблемою, яка потребує пошуку нових та ефективних методів захисту.

Опис проблеми конфіденційності даних в IT-сфері. Небезпека порушення конфіденційності даних в IT-сфері лежить у тому, що долучені дані можуть бути підвернені несанкціонованому доступу, викраденню або модифікації. Це може призвести до серйозних наслідків, включаючи втрату довіри користувачів, фінансові збитки, порушення законодавства та інші негативні наслідки.

Визначення стеганографії та її роль у захисті інформації. Стеганографія – це наука про приховування інформації від несанкціонованих осіб. Цей підхід до захисту даних дозволяє приховати наявність інформації, що зберігається в інших формах даних, так що навіть в основі об'єкта не видно слідів змін. Стеганографія відіграє важливу роль у забезпеченні безпеки даних, дозволяючи передавати конфіденційну інформацію надійно і безпечно.

Опис методів вбудовування даних у програмне забезпечення. Одним із методів вбудовування даних у програмне забезпечення є використання маловідомих або незначних змін в структурі файлів чи коду програми. Наприклад, можливо використовувати незначні зміни в бітах або пікселях зображень, що не будуть помічені звичайним спостереженням. Іншим методом може бути використання деяких резервних або пустих областей у файловій системі для зберігання додаткової інформації. Також, можна розглядати інший підхід, де дані розподіляються між кількома файлами чи частинами системи для покращення захисту від виявлення.

Аналіз методів захисту від виявлення стеганографії. Для захисту від виявлення стеганографії можливо використовувати різноманітні методи та підходи. Один із них – регулярна перевірка програмного забезпечення на вміст прихованої інформації шляхом виявлення незвичайних змін у структурі файлів чи коду. Додатково можна використовувати аналіз підозрілих областей для

виявлення потенційних стеганографічних даних. Також важливо розробляти ефективні методи для виявлення та вилучення стеганографії з програмного забезпечення.

Розглянемо приклади практичного використання стеганографії в розробці програмного забезпечення. Стеганографія широко використовується в різних галузях, зокрема в розробці програмного забезпечення. Наприклад, багато програм для обміну повідомленнями в месенджерах використовують методи стеганографії для захисту конфіденційної інформації. Також, розробники антивірусного програмного забезпечення використовують стеганографію для приховання внутрішніх ключів і алгоритмів, що робить їх менш вразливими до атак ззовні.

Ще одним практичним прикладом використання стеганографії є вбудовування секретної інформації в аудіо- або відеофайли. Це може бути корисним у випадку потреби у захисті інформації в трансляціях або зберіганні даних.

Огляд інструментів для реалізації стеганографії в програмному забезпеченні. Для реалізації стеганографії в програмному забезпеченні існує велика кількість інструментів і бібліотек. Наприклад, стеганографічний софт можна створювати використовуючи мови програмування, такі як Python, Java або C++. Популярні бібліотеки, такі як OpenStego, Steghide, або Invisible Secrets, надають зручний інтерфейс для роботи із стеганографією.

Стеганографія в програмному забезпеченні відкриває двері для створення потужних систем захисту даних, які можуть ефективно захищати конфіденційну інформацію від несанкціонованого доступу.

Побудова логіки захисту за допомогою стеганографії. У розробці програмного забезпечення та систем захисту важливу роль відіграє побудова логіки захисту за допомогою стеганографії. Стеганографія може бути використана для приховування конфіденційної інформації під покривними даними, такими як зображення, аудіо або відеофайли. Це дозволяє зберігати важливі дані в зашифрованому вигляді, при цьому унеможливлюється їх виявлення або злам.

Розробка алгоритмів контролю доступу до стеганографічної інформації

Одним із елементів побудови логіки захисту є розробка алгоритмів контролю доступу до стеганографічної інформації. Це означає визначення прав доступу до прихованої інформації, контроль за процесом розкриття інформації та перевірку легітимних користувачів програмного забезпечення. Застосування відповідних алгоритмів дозволяє підтримувати безпеку та конфіденційність стеганографічної інформації.

Застосування стеганографії для створення внутрішньої системи захисту. Стеганографія може бути також застосована для створення внутрішньої системи захисту. Прихована інформація може бути використана для автентифікації користувачів або контролю доступу до різних ресурсів

програмного забезпечення. Це дозволяє ускладнити процес несанкціонованого доступу та забезпечити додатковий рівень безпеки.

Загалом, стеганографія може бути ефективним інструментом у розробці програмного забезпечення та побудові логіки систем захисту. Вона дозволяє зберігати конфіденційну інформацію у безпечному вигляді, забезпечуючи високий рівень безпеки та конфіденційності даних.

Висновок. Підсумки дослідження методів стеганографії. Дослідження показують, що стеганографічні методи можуть бути ефективними у захисті конфіденційної інформації в програмному забезпеченні. Вони дозволяють приховати дані у носіях таким чином, що не викликає підозри.

Перспективи використання стеганографії у розробці програмного забезпечення та захисті даних. З врахуванням постійного розвитку технологій та зростання кількості кіберзагроз, використання стеганографії у розробці програмного забезпечення та захисті даних матиме все більше значення. Системи, які поєднують в собі стеганографічні методи та методи криптографії, будуть стати засобом ефективного захисту конфіденційної інформації.

Список використаних джерел

1. Кузнецов О. О. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.
2. Мельник С.В. Світові тенденції розвитку цифрової стеганографії в контексті завдань за-безпечення 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.
3. Хорошко В.Щ. Комп’ютерна стеганографія: навчальний посібник / В.О.Хорошко, Ю.Є.Яремчук, В.В.Карпінець – Вінниця: ВНТУ, 2017. – 155 с.