УДК 004.056 (045)
DOI: 10.18372/2310-5461.36.12231

О. К. Юдін
д-р техн. наук, проф.
Національний авіаційний університет
orcid.org/0000-0001-5098-7796
e-mail: yak333@ukr.net;

Я. А. Симониченко
аспірант
Національний авіаційний університет
orcid.org/0000-0002-9404-6610
e-mail: yaroslavsim@ukr.net;

А. А. Симониченко
Національний авіаційний університет
orcid.org/0000-0001-5317-3464
e-mail: annasim98@ukr.net;

ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНИХ МЕТОДІВ В ЗАДАЧАХ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Вступ

На сьогодні інформація відіграє дуже велику роль у житті сучасного суспільства та держави, що призвело до необхідності використання засобів відображення наявної інформації, її обробки та передавання. Тому, питання використання інформаційних технологій та забезпечення інформаційної безпеки є особливо важливим на теперішній час.

Широке впровадження інформаційних технологій та використання різних засобів обробки інформації, призначених для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства або держави, призвело до підвищення кількості методів реалізації загроз інформаційної безпеки з метою можливого порушення конфіденційності, цілісності або доступності інформації.

Зокрема, у червні 2017 р., засоби масової інформації опублікували інформацію про те, що вірус Petya.A призвів до порушення доступності інформації на комп'ютерах користувачів, під керуванням операційних систем сімейства Microsoft Windows, різних підприємств та державних установ на території України. Поширення цього вірусу виконувалась з використанням вразливості механізмів засобів захисту та реалізовувалось на базі прихованого шкідливого програмного забезпечення, у файлах оновлення спеціалізованого програмного забезпечення електронного документообігу, з метою отримання матеріальної винагороди. За офіційними даними Microsoft, унаслідок реалізації даної атаки було порушено роботу більш ніж 12 тисяч комп'ютерів на території України, що призвело до великих моральних та матеріальних збитків. Крім України, даний вірус завдав збитків ще в 64 інших країнах.

Таким чином, забезпечення інформаційної безпеки та захист інформації, під час її обробки в інформаційно-телекомунікаційних системах, від несанкціонованого доступу є актуальним питанням сьогодення, для різних підприємств та державних установ.

Постановка завдання

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» (від 23 лютого 2006 року №3475-IV) визначає, що державні інформаційні ресурси — систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень.

Для постановки завдання та подальшої уніфікації інформаційного змісту даної статті, слід навести визначення таких термінів згідно Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» (від 5 липня 1994 р. №80/94-ВР): *інформаційно-телекомунікаційна система* (далі — ІТС) — сукупність інформаційних та телекомунікаційних систем, які у процесі

обробки інформації діють як єдине ціле; *інформаційна (автоматизована) система* (далі — АС) — організаційно-технічна система, у якій реалізується технологія обробки інформації з використанням технічних і програмних засобів; *телекомунікаційна система* (далі — ТС) — сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб; *користувач інформації в системі* — фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі; *доступ до інформації в системі* — отримання користувачем можливості обробляти інформацію в системі.

Отже, під ІТС слід розуміти сукупність систем (далі — підсистеми ІТС), що виконують обробку АС та обмін ТС державними інформаційними ресурсами між підсистемами ІТС. Обмін та обробка інформації в підсистемах ІТС виконується користувачами, що отримують відповідний (санкціонований) доступ до інформації. Надання відповідного доступу здійснюється з використанням політики безпеки та правил розмежування доступу, що можуть контролювати дії користувачів відносно: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання та передавання інформації, які здійснюються в ІТС за допомогою технічних і програмних засобів.

Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» (від 5 липня 1994 року №80/94-ВР), державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, повинні оброблятися в системі із застосуванням комплексної системи захисту інформації з підтвердженою відповідністю. Під комплексною системою захисту інформації (далі — КСЗІ) розуміють взаємопов'язану сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації.

Одним з основних заходів захисту інформації в ІТС є впровадження та використання різноманітних сучасних технічних засобів захисту, що призводить до ускладнення використання відомих загроз та потребує удосконалення порушником механізмів їх реалізації. Зокрема, для підвищення ступеню захисту інформації або удосконалення механізмів реалізації загроз, можуть використовуватися стеганографічні методи приховування інформації. Для виявлення факту використання стеганографічних методів приховування інформації та можливої наявності відповідних прихованих каналів витоку інформації можуть використовуватися методи стеганографічного аналізу (стеганоаналізу) [с. 389, 1].

Метою даною статті є визначення можливості використання стеганографічних методів в задачах захисту державних інформаційних ресурсів. Під задачами захисту слід розуміти можливість виконання вимог, щодо послуг захисту інформації в ІТС, де обробляється інформація з метою реалізації комплексів засобів захисту (далі — КЗЗ) в КСЗІ або механізмів захисту в програмних або технічних засобах захисту інформації.

Виклад основного матеріалу

Згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» (від 5 липня 1994 року №80/94-ВР), *об'єктами захисту в ІТС* є інформація, що обробляється в ній, а для створення КСЗІ державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, використовуються засоби захисту інформації, які мають сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері технічного та/або криптографічного захисту інформації. Зазвичай для захисту інформаційних ресурсів у ТС використовують криптографічні засоби захисту інформації (використання засобів криптографічного перетворення, електронного цифрового підпису та ін.), а в АС — використовують технічні засоби захисту інформації (пристрої мережевого захисту, системи попередження вторгнень, спеціалізовані програмні комплекси, операційні системи та ін.).

У рамках даної роботи, розглядається сфера технічного захисту інформації (далі — ТЗІ), що обробляється в АС. Під технічним захистом інформації, слід розуміти — вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Згідно з НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу», затвердженого наказом ДСТСЗІ СБУ від 28 квітня 1999 р. №22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 №806 (далі — НД ТЗІ 1.1-002-99), прийнято розрізняти два основних напрями ТЗІ в АС — це захист АС і оброблюваної інформації від несанкціонованого доступу і захист інформації від витоку технічними каналами (оптичними, акустичними, захист від витоку каналами побічних електромагнітних випромінювань і наводів).

Постійне згадування в засобах масової інформації технології приховування повідомлення в інформаційних об'єктах (графічних файлах, відеофайлах, аудіофайлах та ін.) та вільне розповсюдження стеганографічних програмних засобів мережею Інтернет, зробили вищезазначену технологію доступною для будь-якого пересічного громадянина, що може використовуватися з метою організації захисту інформації або прихованого каналу передачі (витоку) інформації та отримання несанкціонованого доступу до неї [с. 126, 2]. Останнім часом, використання стеганографічних методів зафіксовано в такому шкідливому програмному забезпеченні [3]: Microcin; NetTraveler; Zberp; Enfal; Shamoon; KinS; ZeusVM, Triton та ін.

Зважаючи на спосіб та формат реалізації стеганографічних методів, для вирішення поставленого завдання, будемо розглядати напрямок технічного захисту інформації від несанкціонованого доступу. Оскільки, реалізація стеганографічних методів, зазвичай виконується в програмному вигляді (стеганографічні програмні засоби), що може входити до складу програмних та програмно-технічних засобів обробки інформації в АС, та реалізується із використанням цифрових інформаційних об'єктів (графічних файлах, відеофайлах, аудіофайлах та ін.), що можуть передаватися в ІТС, та стеганографічних методів.

За принципом приховування, стеганографічні методи поділяються на два основні класи [с. 126, 2]: безпосередньої заміни (використовують надлишковість ІО в просторовій (для зображення) або часовій (для звуку) області та полягають у заміні малозначущих частин контейнера елементами (бітами) прихованого повідомлення); спектральні методи (використовують спектральне представлення елементів ІО, у яке вбудовують елементи прихованого повідомлення).

Вимоги щодо оцінки спроможності АС або засобу захисту забезпечувати захист оброблюваної інформації від несанкціонованого доступу описано в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», затвердженого наказом ДСТСЗІ СБУ від 28 квітня 1999 р. №22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 №806 (далі — НД ТЗІ 2.5-004-99). Згідно з НД ТЗІ 2.5-004-99, оцінка функцій захисту інформації, що може використовуватися КЗЗ при побудові КСЗІ державних інформаційних ресурсів або оцінки механізмів захисту програмних або технічних засобів захисту інформації в процесі експертизи або сертифікації, виконуються відповідно до встановлених функціональних критеріїв. Функціональні критерії розбиті на чотири групи, кожна з яких описує вимоги до послуг, що забезпечують захист від загроз одного із чотирьох основних типів: *конфіденційність* (загрози, що відносять до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності); *цілісність* (загрози, що відносять до несанкціонованої модифікації інформації, становлять загрози цілісності); *доступність* (загрози, що відносять до порушення можливості використання оброблюваної інформації, становлять загрози доступності); *спостереженість* (ідентифікація і контроль за діями користувачів, керованість АС становлять предмет послуг спостереженості і керованості).

До критеріїв конфіденційності відносять такі послуги: довірчу конфіденційність, адміністративну конфіденційність, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні (експорті/імпорті).

До критеріїв цілісності відносять такі послуги: довірчу цілісність, адміністративну цілісність, відкат і цілісність при обміні.

До критеріїв доступності відносять такі послуги: використання ресурсів, стійкість до відмов, гарячу заміну, відновлення після збоїв.

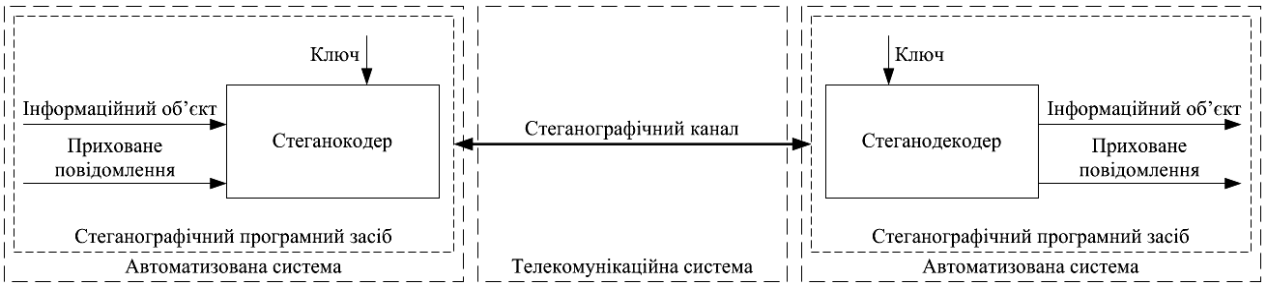
До критеріїв спостережності відносять такі послуги: реєстрацію, ідентифікацію і автентифікацію, достовірні канали, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, автентифікацію при обміні, автентифікацію відправника (невідмову від авторства), ав-тентифікацію одержувача (невідмову від одержання).

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки, цей документ містить критерії гарантій, що дозволяють оцінити коректність реалізації послуг. Критерії гарантій включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації.

Для подальшого визначення ролі стеганографічних методів в задачах захисту державних інформаційних ресурсів, розглянемо детальніше їх аспекти використання та реалізації.

Аналіз літературних джерел та ресурсів мережі Інтернет, дозволяє зробити висновок щодо сучасного використання стеганографічних методів приховування інформації для вирішення наступних ключових завдань в задачах захисту інформації: захист конфіденційної інформації від несанкціонованого доступу, захист авторського права на інтелектуальну власність із використанням цифрових водяних знаків, проходження механізмів захисту технічних засобів захисту при реалізації загроз та організація прихованих каналів витоку інформації.

Реалізація стеганографічних методів призводить до створення спеціальних стеганографічних систем (див. рисунок).



Узагальнена модель реалізації стеганографічної системи в ІТС

Під стеганографічною системою слід розуміти об'єднання методів і засобів, які використовуються для створення прихованого каналу передачі інформації. Стеганографічна система виконує вбудовування прихованого повідомленням в інформаційний об'єкт (із використанням стеганокодера), його передавання стеганографічним каналом (із використанням телекомунікаційних каналів зв'язку) та декодування приховуваного повідомлення (із використанням стеганодекодера).

У більшості стеганосистемах для вбудовування та декодування прихованого повідомлення використовується ключ, який зумовлює алгоритм, що визначає порядок внесення повідомлення в інформаційний об'єкт. Тип ключа зумовлює існування двох типів стеганосистем: з секретним ключем — використовується один ключ для вбудовування та декодування прихованого повідомлення; з відкритим ключем — для вбудовування та декодування прихованого повідомлення використовуються різні ключі [с. 24, 4]. Для узгодження дій користувачів при використанні стеганографічної системи використовуються стеганографічні протоколи таких типів: безключові системи; системи із відкритим ключем; системи із секретним ключем та змішані системи [с. 27, 4].

Однією з основних характеристик стеганографічної системи є її пропускна спроможність. Під пропускною спроможністю розуміється максимальна кількість інформації, що може бути вбудована в один елемент інформаційного об'єкта (наприклад, піксель зображення) з використанням стеганографічних методів.

Основною метою стеганографічного аналізу є моделювання стеганографічних систем та їх дослідження для отримання якісних і кількісних оцінок надійності використання стеганографічного перетворення, а також побудова методів виявлення прихованої в контейнері інформації, її модифікації або руйнування. Стеганографічна система є зламаною, якщо порушнику вдалося, принаймні, довести існування прихованого повідомлення у перехопленому контейнері. У більшості випадків виділяють кілька етапів злому стеганографічної системи [с. 34, 4]: виявлення факту присутності прихованої інформації; видобування прихованого повідомлення; модифікація (спотворення) прихованої інформації та заборона на виконання будь-якого пересилання інформації, у тому числі прихованої. Виконання злому стеганографічної системи може відбуватися із використанням атак (загроз) на основі: відомого/обраного заповненого ІО; на основі відомого/обраного прихованого повідомлення; адаптивна атака на основі обраного повідомлення; на основі відомого/обраного порожнього ІО; на основі відомої математичної моделі ІО або його частини та ін.

Зважаючи на вищезазначені сфери використання стеганографічних методів, їх реалізації та мети стеганоаналізу, можна визначити послуги захисту, при реалізації яких можуть використовуватися дані методи. До таких послуг безпеки можна віднести послуги:

– «Аналіз прихованих каналів»;
– «Конфіденційність при обміні»;
– «Автентифікація відправника».

Послуга безпеки «Аналіз прихованих каналів» має три рівня, що називаються:

- «Виявлення прихованих каналів» (із мнемонічним позначенням КК-1);
- «Контроль прихованих каналів» (КК-2);
- «Перекриття прихованих каналів» (КК-3).

Згідно з НД ТЗІ 2.5-004-99, аналіз прихованих каналів виконується з метою виявлення і усунення потоків існуючої інформації, але не контролюється іншими послугами. Рівні даної послуги ранжируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів. До реалізації послуги «Аналіз прихованих каналів», залежно від рівня, можуть висуватися вимоги відносно: аналізу прихованих каналів та їх документування; визначення максимальної пропускної здатності кожного прихованого каналу; усунення знайдених під час аналізу прихованих каналів та ін. Отже, використання методів стеганографічного аналізу, що дозволяє виявляти функціонування стеганографічної системи, виконувати вимоги даної послуги із реалі-

зацією вищезазначених механізмів атак, виявлення факту присутності прихованої інформації, його видобування, модифікації та спотворення, а також визначення її пропускної спроможності.

Послуга безпеки «Конфіденційність при обміні» має чотири рівня, що називаються:

– «Мінімальна конфіденційність при обміні» (КВ-1);
– «Базова конфіденційність при обміні» (КВ-2);
– «Повна конфіденційність при обміні» (КВ-3);
– «Абсолютна конфіденційність при обміні» (КВ-4).

Згідно з НД ТЗІ 2.5-004-99, ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. До реалізації послуги «Конфіденційність при обміні», залежно від рівня, можуть висуватися вимоги відносно політики конфіденційності: визначення множини об'єктів, до яких вона належить; визначання рівня захищеності інформації; забезпечення захисту від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається та ін. Отже, використання стеганографічних методів для реалізації документованих прихованих каналів з метою забезпечення конфіденційності інформації від несанкціонованого доступу під час її обробці в ІТС, дозволяє виконувати вимоги даної послуги із реалізацією вищезазначеної стеганографічної системи та відповідних протоколів.

Послуга безпеки «Автентифікація відправника» має два рівня, що називаються:

1. «Базова автентифікація відправника» (НА-1);
2. «Автентифікація відправника з підтвердженням» (НА-2).

Згідно з НД ТЗІ 2.5-004-99, ця послуга дозволяє забезпечити захист від відмови від авторства і однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною. До реалізації послуги «Автентифікація відправника», залежно від рівня, можуть висуватися вимоги відносно: процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем та підтвердження належності об'єкта незалежною третьою стороною; використання протоколу, що забезпечує можливість однозначного підтвердження належності об'єкта незалежною третьою стороною та ін.

Отже, використання стеганографічних методів для реалізації приховування спеціальної, невидимої для людини, мітки, що зберігається в інформаційному об'єкті та виявляється спеціальним програмним забезпеченням, а також, використання вищезазначеної стеганографічної системи та відповідних протоколів, дозволяє виконувати вимоги даної послуги.

Висновок

Під час виконання даної роботи було визначено можливість використання стеганографічних методів в задачах захисту державних інформаційних ресурсів.

Таким чином, використання стеганографічних методів надає можливості виконати вимоги, щодо послуг захисту інформації в ІТС, де обробляється інформація з метою реалізації КЗЗ в КСЗІ або механізмів захисту в програмних або технічних засобах захисту інформації. До таких послуг безпеки відносять: «Аналіз прихованих каналів», «Конфіденційність при обміні» та «Автентифікацію відправника» на різних рівнях. Реалізація вищезазначених вимог досягається при використанні механізмів стеганографічної системи, відповідних протоколів, її основних показників та методів стеганоаналізу.

ЛІТЕРАТУРА

1. **Юдін О. К.** Виявлення прихованих каналів передачі інформації на базі методів стеганоаналізу / О. К. Юдін, Я. А. Симониченко // Наукоємні технології. — 2016. — №4 (32). — С. 389–394.

2. **Юдін О. К.** Дослідження сучасних стеганографічних методів та засобів обробки цифрових зображень/О. К. Юдін, Я. А. Симониченко, А. А. Симониченко // Наукоємні технології. — 2017. — №2 (34). — С. 126–133.
DOI: 10.18372/2310-5461.34.11610.

3. Стеганография в современных кибератаках: 2017 [Електронний ресурс]. — Режим доступу: https://securelist.ru/steganography-in-contemporary-cyberattacks/79090/.

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

Юдін О. К., Симониченко Я. А., Симониченко А. А.

ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНИХ МЕТОДІВ В ЗАДАЧАХ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

У статті проведено визначення можливості використання стеганографічних методів, а саме, методів приховування інформації та стеганографічного аналізу в задачах захисту державних інформаційних ресурсів. Під час роботи було визначено можливість використання стеганографічних методів для виконання вимог послуг захисту інформації в інформаційно-телекомунікаційних системах, де обробляється інформація, з метою реалізації комплексів засобів захисту в комплексних системах захисту інформації або механізмів захисту в програмних або технічних засобах захисту інформації. Було виконано дослідження реалізації стеганографічних методів приховування інформації та стеганографічного аналізу, їх основних характеристик та сфер використання. На основі проведених досліджень були визначені послуги захисту інформації, при реалізації яких можуть використовуватися стеганографічні методи приховування інформації та стеганографічного аналізу.

Ключові слова: стеганографічні методи, стеганографічна система; стеганографічний аналіз; державні інформаційні ресурси; послуги захисту інформації.

Юдин А. К., Симониченко Я. А., Симониченко А. А.

ИСПОЛЬЗОВАНИЕ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ В ЗАДАЧАХ ЗАЩИТЫ ГОСУДАРСТВЕННЫХ ІНФОРМАЦИОННЫХ РЕСУРСОВ

В статье проведено определение возможности использования стеганографических методов, а именно, методов сокрытия информации и стеганографического анализа, в задачах защиты государственных информационных ресурсов. Во время работы была определена возможность использования стеганографических методов для выполнения требований услуг защиты информации в информационно-телекоммуникационных системах, где обрабатывается информация, с целью реализации комплексов средств защиты в комплексных системах защиты информации или механизмов защиты в программных или технических средствах защиты информации. Было выполнено исследование реализации стеганографических методов сокрытия информации и стеганографического анализа, их основных характеристик и сфер использования. На основе проведенных исследований были определены услуги защиты информации, при реализации которых могут использоваться стеганографические методы сокрытия информации и стеганографического анализа.

Ключевые слова: стеганографические методы, стеганографическая система; стеганографический анализ; государственные информационные ресурсы; услуги защиты информации.

Yudin A. K., Simonichenko Y. A., Simonichenko A. A.

USING STEGANOGRAPHIC METHODS IN PROBLEMS OF PROTECTION OF STATE-PARTICULAR INFORMATION RESOURCES

The article deals with the definition of the possibilities of using steganographic methods, namely, methods of information hiding and steganography analysis, in problems of protection of state information resources. During the work was identified the opportunity of the application of steganographic techniques to meet the requirements of protection's services of information in information telecommunication systems where information is processed, with the aim of the implementation of protection's systems in the integrated systems of information protection or protection mechanisms in the software or technical means of information protection. It was the research of the implementation of the steganographic methods of information hiding and steganographic analysis, their characteristics and applications. Based on the conducted research identified services of the information security, implementation of which can be used steganography techniques information hiding and steganographic analysis.

Keywords: steganographic methods, the steganographic system: steganographic analysis; government information resources; services information security.

Стаття надійшла до редакції 27.11.2017 р.
Прийнято до друку 29.11.2017 р.
Рецензент — д-р техн. наук, проф. Конахович Г. Ф.