законодавство та створювати більш ефективні, доцільні та ненадмірні метоти та засоби захисту таємниці. Також, комерційна таємниця є цілісною і повинно бути недопущення потрапляння секретної інформації до конкурентів чи третіх осіб, що може негативно вплинути на діяльність підприємства.

Список використаних джерел:

1. Цивільний кодекс України від 16.01.2003 № 435-IV // Відомості Верховної Ради України (ВВР). – 2003. – № № 40-44, ст. 356 [Електронний ресурс]. – Режим доступу до тексту: http://zakon3.rada.gov.ua/laws/main/435-15

2. Про перелік відомостей, що не становлять комерційної таємниці: Постанова Кабінету Міністрів України від 09.08.1993 № 611 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/611-93-%D0%BF

3. Клименко П. М. Інформація як об’єкт інтелектуальної власності, що потребує охорони // Недержавна система безпеки підприємництва як суб’єкт національної безпеки України: Зб. Матеріалів наук.-практ. конф., Київ, 16-17 травня 2001 року. – К.: Вид-во Європ. ун-ту, 2003. – С. 283-289.

Клапко О.О.

студент,
Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України

ПОРІВНЯЛЬНИЙ АНАЛІЗ СТЕГАНОГРАФІЧНИХ МЕТОДІВ

Сучасні комп’ютерні технології обробки даних істотно підвищили рівень інформаційної безпеки завдяки глибокій інтеграції криптографічних засобів в інформаційні системи. Як відомо, на відміну від криптографічного захисту інформації стеганографічні програмні засоби намагаються насамперед приховати сам факт існування конфіденційної інформації.

Стеганографічні методи, які приховують інформацію у потоках оцифрованих сигналів та реалізуються на основі комп’ютерної техніки і програмного забезпечення, становлять предмет вивчення цифрової стеганографії. Актуальність дослідження методів стеганографії невпинно зростає, адже з поширенням персональних комп’ютерів, і особливо Інтернету, можливість конфіденційно передавати інформацію привертає увагу великої кількості людей. Переважна більшість теоретичних та практичних досліджень у галузі стеганографії присвячена саме розробці нових та вдосконаленню існуючих методів приховування даних [1–5].

Цифрова стеганографія – напрям класичної стеганографії, що полягає у впровадженні додаткової інформації у цифрові об’єкти (контейнери), викликаючи при цьому деякі спотворення цих об’єктів. Ця технологія призначена для організації таємного зв’язку, що є класичним завданням стеганографії, проте останнім часом вона використовується також для захисту інтелектуальної власності [3].

Стеганографія та цифрові водяні знаки

Один з найефективніших технічних засобів захисту мультимедійної інформації і полягає у вбудовуванні в об'єкт, що захищається, невидимих міток – цифрових водяних знаків (ЦВЗ). На відміну від звичайних паперових водяних знаків ЦВЗ можуть бути не тільки видимими, але і, як правило, невидимими. Невидимі ЦВЗ аналізуються спеціальним декодером, який виносить рішення про їх коректність. ЦВЗ можуть містити деякий автентичний код, інформацію про власника або будь-яку іншу інформацію.

Основна відмінність задачі прихованої передачі даних від задачі вбудовування ЦВЗ полягає у тому, що в першому випадку порушник повинен здогадуватись про наявність прихованого повідомлення, тоді як у другому випадку його існування може не приховуватися [2].

Застосування методів стеганографії для різних завдань захисту інформації

Традиційно інтерес до стеганографічних методів проявлявся у військових і дипломатичних колах, оскільки донедавна термін «стеганографія» означав лише приховану передачу інформації. Сьогодні ж ця технологія знаходить своє застосування і в інших сферах діяльності, пов'язаних з інформаційною безпекою. Зокрема існують методи, що дають можливість впровадження ЦВЗ у файли різних форматів, заголовки IP-пакетів, у текстові повідомлення та цифрові медіадані [1].

Завдання, виконані стеграфічними методами

Області застосування стеганографії	
Захист від копіювання Електронна комерція, контроль за копіюванням (DVD), розповсюдження мультимедійної інформації (відео за запитом)	Прихована анотація документів Медичні знімки, картографія, мультимедійні бази даних
Аутентифікація Системи відеоспостереження, електронної комерції, голосової пошти, електронне конфіденційне діловодство	Прихований зв'язок Військові та розвідувальні додатки

Однією з проблем, пов'язаних з ЦВЗ, є різноманіття вимог, що ставляться перед системою залежно від завдань, які вона повинна виконувати. Наприклад, співвідношення між ступенем захищеності вбудованого повідомлення та його розміром змінюватиметься залежно від призначення стегосистеми. Для захисту авторських прав важливо, щоб водяний знак був стійкам до видалення чи спотворення, натомість обсяг інформації, яку він становить, може бути невеликим. Для прихованого зв'язку, – навпаки, кількість переданої інформації є значно більшою. Менш важливою стає стійкість до модифікацій контейнера; вона повинна бути достатньою, щоб прочитати приховану інформацію.

Отже, залежно від цілей, для яких використовується приховування даних, різними є і вимоги щодо рівня стійкості системи до модифікації контейнера. Як наслідок, для різних цілей оптимальними є різні методи стеганографії.

Список використаних джерел:

1. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – К.: Солон-Пресс, 2002. – 265 с.

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

3. Поліновський В.В. Інформаційна технологія для досліджень методів стеганографії і стегоаналізу / В.В. Поліновський // Міжвузівський збірник «Комп'ютерно-інтегровані технології: освіта, наука, виробництво». – Луцьк, 2011. – № 5. – С. 236–242.

4. Таранчук А.А. Стеганографічний метод приховування даних в області частотних перетворень зображень / А.А. Таранчук, Л.Г. Гальпер // Вісник Хмельницького національного університету. – Хмельницький, 2009. – № 2: «Технічні науки». – С. 197–201.

5. Хорошко В.А. Методи й засоби захисту інформації / В.А. Хорошко, А. А. Чекатков. – К.: Юніор, 2003. – 504 с.

Лупаїна Д.А.

студент,

Навчально-науковий інститут інформаційної безпеки

Національної академії Служби безпеки України

РОЗРАХУНКОВА ВАРТІСТЬ ОБРАНИХ ЗАХОДІВ ЗАХИСТУ

Для визначення систем та засобів з яких складається комплекс ТЗІ необхідно зрозуміти, які збитки буде нести підприємство у разі несанкціонованого ознайомлення, модифікації, знищення, копіювання, поширення інформації.

Одним із принципів, які притаманні процедурі побудови системи захисту інформації є принцип економічної доцільності.

Економічна доцільність зазначає, що витрати на розробку і реалізацію системи захисту інформації не повинні перевищувати розміри потенційного збитку, який може наступити в результаті порушення безпеки інформації, що захищається [1, с. 8-10].

Основні економічні принципи:

– технологія захисту інформації повинна вибиратися таким чином, щоб при мінімальних витратах, забезпечувати максимальний захист;

– надійність захисту повинна визначатися з міркувань оптимізації відношення «функціональність системи без захисту» / «функціональність системи із захистом» [3].

Захист інформації, яка не становить державну таємницю забезпечується досягненням необхідного рівня захисту інформації з обмеженим доступом за