**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**КАФЕДРА** **КОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Казмірчук

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.

На правах рукопису

УДК

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

**Тема**:Методи стеганоаналізу критичної інформації кіберпростору.

|  |  |
| --- | --- |
| **Автор:** | Є.О. Іванюк |
| **Науковий керівник:** к.т.н., доц. | О.С. Шматок |
| **Нормоконтролер:** | С.В. Егоров |

**Київ 2020**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Факультет:** Кібербезпеки, комп’ютерної та програмної інженерії

**Кафедра:** Комп’ютеризованих систем захисту інформації

**Освітній ступінь:** Магістр

**Спеціальність:** 125 «Кібербезпека»

**Освітньо-професійна програма**: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Казмірчук

« » 20\_\_ р.

**ЗАВДАННЯ**

**на виконання магістерської атестаційної роботи**

**магістранта Іванюк Євгеній Олексійович**

1. Тема: *Методи стеганоаналізу критичної інформації кіберпростору*.

затверджена наказом ректора від «\_\_» \_\_\_\_\_\_\_\_\_\_ 20\_\_ № \_\_\_\_\_/ст*.*

1. Термін виконання з \_\_.\_\_.20\_\_р. по \_\_.\_\_.20\_\_р*.*
2. Вихідні дані: сформувати схему дій руйнівного програмного засобу моделі «стеганографічне перетворення», в якості стегоконтейнера використати графічний файл, для виявлення стеганографічних закладок використати методи стеганоаналізу, змоделювати систему захисту інформації з використанням стеганографічних перетворень.
3. Зміст пояснювальної записки: аналіз стеганографічних методів в системі забезпечення кібербезпеки, аналіз сучасних методів стеганоаналізу та існуючих руйнівних програмних засобів, оцінка якості стеганографічної системи, розробка методики реалізації та виявлення руйнівних програмних засобів моделі «стеганографічне перетворення», організація системи захисту інформації.

**КАЛЕНДАРНИЙ ПЛАН**

**виконання магістерської роботи**

|  |  |  |  |
| --- | --- | --- | --- |
| *№ п/п* | **Етапи виконання магістерської роботи** | **Термін виконання етапів** | **Примітка** |
| 1 | Уточнення постановки задачі |  | *Виконано* |
| 2 | Аналіз літературних джерел |  | *Виконано* |
| 3 | Обґрунтування вибору рішення |  | *Виконано* |
| 4 | Збір інформації |  | *Виконано* |
| 5 | Аналіз даних та їх класифікація |  | *Виконано* |
| 6 | Аналіз стану критичної інформації кіберпростору та місця стеганографії серед сучасних методів захисту інформації |  | *Виконано* |
| 7 | Аналіз існуючих методів стеганоаналізу |  | *Виконано* |
| 8 | Розробка методики реалізації та виявлення моделі РПЗ «стеганографічне перетворення» |  | *Виконано* |
| 9 | Оформлення і друк пояснювальної записки |  | *Виконано* |
| 10 | Оформлення презентації |  | *Виконано* |
| 11 | Отримання рецензій від опонентів |  | *Виконано* |
| 12 | Підготовка до захисту в ДЕК |  | *Виконано* |

Магістрант Є. Іванюк

(підпис, дата)

Науковий керівник О. Шматок

(підпис, дата)

**РЕФЕРАТ**

Магістерська атестаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків і має 123 сторінки основного тексту, 27 рисунка. Список використаних джерел містить 25 найменування. Загальний обсяг роботи 124 сторінок.

Метою роботи є підвищення рівня захищеності інформаційної системи з використанням методів стеганоаналізу для боротьби з стеганографічними закладками.

В роботі основну увагу приділено стеганографічним перетворенням та методам стеганоаналізу та можливості їх використання для вирішення проблеми захисту інформації в комп’ютерних системах.

В роботі розроблена схема реалізації РПЗ моделі «стеганографічне перетворення» та створена модель використання методів стеганоаналізу для її виявлення.

В роботі було визначено основні етапи процедури впровадження стеганографічних закладок в інформаційну систему та було сформовано модель системи захисту інформації для боротьби з РПЗ з використанням стегоаналітичних засобів.

Розроблений метод та програмне забезпечення відносяться до галузі інформаційної безпеки і можуть бути використані для підвищення рівня захищеності.

Ключові слова: стеганографія, стеганографічне перетворення, руйнівний програмний засіб, стеганографічна система, стегоканал, стегоконтейнер, стеганоаналіз, метод заміни найменшого значущого біту.

**ЗМІСТ**

[ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ 7](#_Toc295081996)

[ВСТУП 8](#_Toc295081997)

[РОЗДІЛ 1](#_Toc295081998).[Стеганографічні методи в системі забезпечення інформаційної безпеки 10](#_Toc295081999)

[1.1. Аналіз стану критичної інформації кіберпростору 10](#_Toc295082000)

[1.2. Аналіз нормативно - правової бази забезпечення захисту інформації в автоматизованих системах](#_Toc295082001) 37

[1.3. Сучасні методи захисту інформації](#_Toc295082002) 41

[1.3.1. Організаційні методи захисту інформації 43](#_Toc295082003)

[1.3.2. Технічні засоби захисту інформації 46](#_Toc295082004)

[1.3.3. Програмні методи захисту інформації 47](#_Toc295082005)

[1.3.4. Криптографічні методи захисту 49](#_Toc295082006)

[1.3.5. Стеганографія 50](#_Toc295082007)

[1.4. Критерії вибору стеганосистеми 53](#_Toc295082008)

[1.5. Висновки по розділу 62](#_Toc295082009)

[РОЗДІЛ 2.](#_Toc295082010) [Інтегровані стеганографічні методи](#_Toc295082011) 64

[2.1. Руйнівні програмні коди серед загроз інформаційній безпеці 64](#_Toc295082012)

[2.1.1. Віруси як різновид руйнівних програмних кодів 68](#_Toc295082013)

[2.1.2. Програмні закладки 72](#_Toc295082014)

[2.2. Використання стеганографічних методів для реалізації загроз інформаційній безпеці 75](#_Toc295082015)

[2.3. Аналіз сучасних методів стеганоаналізу. Класифікація атак на системи прихованої передачі інформації 79](#_Toc295082016)

[2.4. Оцінка якості стеганографічної системи 91](#_Toc295082017)

[2.5. Висновки по розділу 95](#_Toc295082018)

[РОЗДІЛ 3.](#_Toc295082019) [Модель РПЗ «стеганографічне перетворення»: методика реалізації та виявлення](#_Toc295082020) 97

[3.1. Аналіз існуючих моделей РПЗ 97](#_Toc295082021)

[3.1.1.Класифікація РПЗ за різними ознаками. 97](#_Toc295082022)

[3.1.2.Основні методи впровадження РПЗ. 103](#_Toc295082023)

[3.1.3.Моделі взаємодії прикладної програми і програмної закладки. 104](#_Toc295082024)

[3.2. Формування моделі РПЗ «стеганографічне перетворення» 109](#_Toc295082025)

[3.3. Моделювання системи виявлення та захисту від РПЗ з використанням методів стеганоаналізу 113](#_Toc295082026)

[3.4. Організація системи захисту інформації 116](#_Toc295082027)

[3.5. Висновки по розділу 119](#_Toc295082028)

[ВИСНОВКИ 120](#_Toc295082029)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ 121](#_Toc295082030)

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

АС – автоматизована система;

ЗЗІ – засоби захисту інформації;

ІКС – інформаційна – комунікаційна система,

ІС – інформаційна система;

КС – комп’ютерна система;

КСЗІ – комплексна система захисту інформації;

НЗБ – найменший значущий біт.

ПЗ – програмний засіб;

РПЗ – руйнівний програмний засіб;

СЗІ – служба захисту інформації;

# ВСТУП

**Актуальність**.Розвиток комп'ютерних методів обробки інформації дозволив суттєво підвищити рівень забезпечення інформаційної безпеки. Значних успіхів у цьому напрямі вдалося досягнути з використанням сучасних криптографічних методів. Однак у цілому ряді завдань інформаційної безпеки їх стає недостатньо, оскільки вони не дозволяють приховати сам факт наявності або передачі інформації. Вирішувати такі проблеми стало можливим з використанням стеганографічних методів захисту інформації.

Поряд зі створенням нових стеганоалгоритмів приховування інформації не менш актуальною є розробка методів сучасного стеганоаналізу. Основне завдання стеганоаналізу – встановлення факту наявності в контейнері прихованої інформації. Крім того використання методів стеганоаналізу дозволяє боротися з такими видом загроз як стеганографічна закладка, що може включати в собі реалізацію будь-якого руйнівного програмного засобу. У ході вирішення даної задачі стеганоаналітиком використовуються різні методи аналізу.

**Метою роботи є** підвищення рівня захищеності інформаційної системи з використанням методів стеганоаналізу для боротьби з стеганографічними закладками. Для досягнення поставленої мети вирішуються такі **задачі:**

- сформувати схему дій руйнівного програмного засобу моделі «стеганографічне перетворення»,

- в якості стегоконтейнера використати графічний файл, для виявлення стеганографічних закладок використати методи стеганоаналізу,

- змоделювати систему захисту інформації з використанням стеганографічних перетворень.

**Галузь застосування**. Розроблений метод та програмне забезпечення відносяться до галузі інформаційної безпеки і можуть бути використані для підвищення рівня захищеності ІКС за рахунок використання методів стеганографічних перетворень.

**Об’єктом дослідження є** процес захисту інформації в ІКС.

**Предметом дослідження** є методи, моделі та системи стеганографії та стеганоаналізу в системі забезпечення захисту інформації.

**Метод дослідження** створення моделі реалізації та виявлення РПЗ «стеганографічне перетворення» з використанням в якості стеганоконтейнера графічних файлів.

**Новизна одержаних результатів полягає в наступному:**

* вперше на основі моделі «стеганографічне перетворення», в розробці схеми реалізації РПЗ та створення моделі з використання методів стеганоаналізу для її виявлення.

**Практичне значення отриманих результатів:**

* визначити основні етапи впровадження руйнівних програмних засобів та їх класифікацію;
* розробити модель реалізації та виявлення руйнівного програмного засобу типу «стеганографічне перетворення» на базі графічного стеганоконтейнера;
* розробити схему організації системи захисту інформації.
* **Апробація.** Основні положення роботи доповідалися та обговорювалися на конференції:

…………………………………………………….

## РОЗДІЛ 1

## Стеганографічні методи в системі забезпечення інформаційної безпеки України

## 1.1. Аналіз стану критичної інформації кіберпростору

ЗАКОН УКРАЇНИ

Про основні засади забезпечення кібербезпеки України

(Відомості Верховної Ради (ВВР), 2017, № 45, ст.403)

{Із змінами, внесеними згідно із Законом

№ 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст.241}

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

1) індикатори кіберзагроз - показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози;

2) інформація про інцидент кібербезпеки - відомості про обставини кіберінциденту, зокрема про те, які об’єкти кіберзахисту і за яких умов зазнали кібератаки, які з них успішно виявлені, нейтралізовані, яким запобігли за допомогою яких засобів кіберзахисту, у тому числі з використанням яких індикаторів кіберзагроз;

3) інцидент кібербезпеки (далі - кіберінцидент) - подія або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського фактора) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів;

4) кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об’єкти кіберзахисту;

5) кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

6) кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об’єктів;

7) кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

8) кіберзлочин (комп’ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

9) кіберзлочинність - сукупність кіберзлочинів;

10) кібероборона - сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

11) кіберпростір - середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних;

12) кіберрозвідка - діяльність, що здійснюється розвідувальними органами у кіберпросторі або з його використанням;

13) кібертероризм - терористична діяльність, що здійснюється у кіберпросторі або з його використанням;

14) кібершпигунство - шпигунство, що здійснюється у кіберпросторі або з його використанням;

15) критична інформаційна інфраструктура - сукупність об’єктів критичної інформаційної інфраструктури;

16) критично важливі об’єкти інфраструктури (далі - об’єкти критичної інфраструктури) - підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов’язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров’я людей;

17) Національна телекомунікаційна мережа - сукупність спеціальних телекомунікаційних систем (мереж), систем спеціального зв’язку, інших комунікаційних систем, які використовуються в інтересах органів державної влади та органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону, призначена для обігу (передавання, приймання, створення, оброблення, зберігання) та захисту національних інформаційних ресурсів, забезпечення захищених електронних комунікацій, надання спектра сучасних захищених інформаційно-комунікаційних (мультисервісних) послуг в інтересах здійснення управління державою у мирний час, в умовах надзвичайного стану та в особливий період, та яка є мережею (системою) подвійного призначення з використанням частини її ресурсу для надання послуг, зокрема з кіберзахисту, іншим споживачам;

18) національні електронні інформаційні ресурси (далі - національні інформаційні ресурси) - систематизовані електронні інформаційні ресурси, які містять інформацію незалежно від виду, змісту, форми, часу і місця її створення (включаючи публічну інформацію, державні інформаційні ресурси та іншу інформацію), призначену для задоволення життєво важливих суспільних потреб громадянина, особи, суспільства і держави. Під електронними інформаційними ресурсами розуміється будь-яка інформація, що створена, записана, оброблена або збережена у цифровій чи іншій нематеріальній формі за допомогою електронних, магнітних, електромагнітних, оптичних, технічних, програмних або інших засобів;

19) об’єкт критичної інформаційної інфраструктури - комунікаційна або технологічна система об’єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об’єкта критичної інфраструктури;

20) система управління технологічними процесами (далі - технологічна система) - автоматизована або автоматична система, яка є сукупністю обладнання, засобів, комплексів та систем обробки, передачі та приймання, призначена для організаційного управління та/або управління технологічними процесами (включаючи промислове, електронне, комунікаційне обладнання, інші технічні та технологічні засоби) незалежно від наявності доступу системи до мережі Інтернет та/або інших глобальних мереж передачі даних;

21) системи електронних комунікацій (далі - комунікаційні системи) - системи передавання, комутації або маршрутизації, обладнання та інші ресурси (включаючи пасивні мережеві елементи, які дають змогу передавати сигнали за допомогою проводових, радіо-, оптичних або інших електромагнітних засобів, мережі мобільного, супутникового зв’язку, електричні кабельні мережі в частині, в якій вони використовуються для цілей передачі сигналів), що забезпечують електронні комунікації (передачу електронних інформаційних ресурсів), у тому числі засоби і пристрої зв’язку, комп’ютери, інша комп’ютерна техніка, інформаційно-телекомунікаційні системи, які мають доступ до мережі Інтернет та/або інших глобальних мереж передачі даних.

Терміни "національна безпека", "національні інтереси", "загрози національній безпеці"вживаються в цьому Законі у значенні, визначеному Законом України "Про основи національної безпеки України".

Стаття 2. Принципи застосування Закону

1. Цей Закон не поширюється на:

1) відносини та послуги, пов’язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах;

2) діяльність, пов’язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;

3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов’язані з функціонуванням таких мереж і ресурсів;

4) комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем).

2. Застосування законодавства у сфері кібербезпеки та прийняття суб’єктами владних повноважень рішень на виконання норм цього Закону здійснюються з додержанням принципів:

1) мінімально необхідного регулювання, згідно з яким рішення (заходи) суб’єктів владних повноважень повинні бути необхідними і мінімально достатніми для досягнення мети і завдань, визначених цим Законом;

2) об’єктивності та правової визначеності, максимально можливого застосування національного та міжнародного права щодо повноважень і обов’язків державних органів, підприємств, установ, організацій, громадян у сфері кібербезпеки;

3) забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, та/або послуг із захисту інформації, кіберзахисту, у тому числі прав щодо невтручання у приватне життя і захисту персональних даних;

4) прозорості, згідно з яким рішення (заходи) суб’єктів владних повноважень мають бути належним чином обґрунтовані та повідомлені суб’єктам, яких вони стосуються, до набрання ними чинності (їх застосування);

5) збалансованості вимог та відповідальності, згідно з яким має бути забезпечено баланс між встановленням відповідальності за невиконання вимог кібербезпеки та кіберзахисту, а також за запровадження надмірних вимог та обмежень;

6) недискримінації, згідно з яким рішення, дії та бездіяльність суб’єктів владних повноважень не можуть призводити до юридичного або фактичного обсягу прав та обов’язків особи, який є:

відмінним від обсягу прав та обов’язків інших осіб у подібних ситуаціях, якщо тільки така відмінність не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

таким, як і обсяг прав та обов’язків інших осіб у неподібних ситуаціях, якщо така однаковість не є необхідною та мінімально достатньою для задоволення загальносуспільного інтересу;

7) еквівалентності вимог до забезпечення кібербезпеки об’єктів критичної інфраструктури, згідно з яким застосування правових норм повинно бути якомога більш рівнозначним щодо кіберзахисту комунікаційних та технологічних систем об’єктів критичної інфраструктури, що належать до одного сектору економіки та/або які здійснюють аналогічні функції.

Зазначені принципи застосовуються без переваги будь-якого з них з урахуванням мети і завдань цього Закону.

Стаття 3. Правові основи забезпечення кібербезпеки України

1. Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, цей та інші закони України, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов’язковість яких надана Верховною Радою України, укази Президента України, акти Кабінету Міністрів України, а також інші нормативно-правові акти, що приймаються на виконання законів України.

2. Якщо міжнародним договором України, згоду на обов’язковість якого надано Верховною Радою України, передбачено інші правила, ніж встановлені цим Законом, застосовуються положення міжнародного договору України.

Стаття 4. Об’єкти кібербезпеки та кіберзахисту

1. Об’єктами кібербезпеки є:

1) конституційні права і свободи людини і громадянина;

2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища;

3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність;

4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави;

5) об’єкти критичної інфраструктури.

2. Об’єктами кіберзахисту є:

1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону;

2) об’єкти критичної інформаційної інфраструктури;

3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу.

3. Порядок формування переліку об’єктів критичної інформаційної інфраструктури, перелік таких об’єктів та порядок їх внесення до державного реєстру об’єктів критичної інформаційної інфраструктури, а також порядок формування та забезпечення функціонування державного реєстру об’єктів критичної інформаційної інфраструктури затверджуються Кабінетом Міністрів України.

Повноваження щодо формування та забезпечення функціонування реєстру об’єктів критичної інформаційної інфраструктури у банківській системі України покладаються на Національний банк України.

Стаття 5. Суб’єкти забезпечення кібербезпеки

1. Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.

2. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб’єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

3. Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури (крім об’єктів критичної інфраструктури у банківській системі України).

4. Суб’єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є:

1) міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб’єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) підприємства, установи та організації, віднесені до об’єктів критичної інфраструктури;

8) суб’єкти господарювання, громадяни України та об’єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов’язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

5. Суб’єкти забезпечення кібербезпеки у межах своєї компетенції:

1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях;

2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків;

3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз;

4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту;

5) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об’єктах та об’єктах, що належать до сфери їх управління;

6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору.

Стаття 6. Об’єкти критичної інфраструктури

1. До об’єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації незалежно від форми власності, які:

1) провадять діяльність та надають послуги в галузях енергетики, хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, у банківському та фінансовому секторах;

2) надають послуги у сферах життєзабезпечення населення, зокрема у сферах централізованого водопостачання, водовідведення, постачання електричної енергії і газу, виробництва продуктів харчування, сільського господарства, охорони здоров’я;

3) є комунальними, аварійними та рятувальними службами, службами екстреної допомоги населенню;

4) включені до переліку підприємств, що мають стратегічне значення для економіки і безпеки держави;

5) є об’єктами потенційно небезпечних технологій і виробництв.

2. Критерії та порядок віднесення об’єктів до об’єктів критичної інфраструктури, перелік таких об’єктів, загальні вимоги до їх кіберзахисту, у тому числі щодо застосування індикаторів кіберзагроз, та вимоги до проведення незалежного аудиту інформаційної безпеки затверджуються Кабінетом Міністрів України, а в банківській системі України - Національним банком України.

3. Вимоги і порядок проведення незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури встановлюються відповідними нормативно-правовими актами з аудиту інформаційної безпеки, що затверджуються Кабінетом Міністрів України.

Розроблення нормативно-правових актів з незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури здійснюється на основі міжнародних стандартів, стандартів Європейського Союзу та НАТО з обов’язковим залученням представників основних суб’єктів національної системи кібербезпеки, наукових установ, незалежних аудиторів та експертів у сфері кібербезпеки, громадських організацій.

4. Відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об’єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог законодавства, за невідкладне інформування урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об’єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об’єктів критичної інфраструктури.

5. Обмін інформацією про інциденти кібербезпеки, що містить персональні дані, здійснюється з дотриманням вимог Закону України "Про захист персональних даних".

Стаття 7. Принципи забезпечення кібербезпеки

1. Забезпечення кібербезпеки в Україні ґрунтується на принципах:

1) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом;

2) забезпечення національних інтересів України;

3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі;

4) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері;

5) пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам, реалізації невід’ємного права держави на самозахист відповідно до норм міжнародного права у разі вчинення агресивних дій у кіберпросторі;

6) пріоритетності запобіжних заходів;

7) невідворотності покарання за вчинення кіберзлочинів;

8) пріоритетного розвитку та підтримки вітчизняного наукового, науково-технічного та виробничого потенціалу;

9) міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних, воєнних, інших протиправних цілях;

10) забезпечення демократичного цивільного контролю за утвореними відповідно до законів України військовими формуваннями та правоохоронними органами, що провадять діяльність у сфері кібербезпеки.

Стаття 8. Національна система кібербезпеки

1. Національна система кібербезпеки є сукупністю суб’єктів забезпечення кібербезпеки та взаємопов’язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об’єктів критичної інформаційної інфраструктури.

2. Основними суб’єктами національної системи кібербезпеки є Державна служба спеціального зв’язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України, які відповідно до Конституції і законів України виконують в установленому порядку такі основні завдання:

1) Державна служба спеціального зв’язку та захисту інформації України забезпечує формування та реалізацію державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту об’єктів критичної інформаційної інфраструктури, здійснює державний контроль у цих сферах; координує діяльність інших суб’єктів забезпечення кібербезпеки щодо кіберзахисту; забезпечує створення та функціонування Національної телекомунікаційної мережі, впровадження організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об’єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації (переатестації); координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об’єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту, урядової команди реагування на комп’ютерні надзвичайні події України CERT-UA;

2) Національна поліція України забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі;

3) Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об’єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки;

4) Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі (кібероборони); здійснюють військову співпрацю з НАТО та іншими суб’єктами оборонної сфери щодо забезпечення безпеки кіберпростору та спільного захисту від кіберзагроз; впроваджують заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури в умовах надзвичайного і воєнного стану;

5) розвідувальні органи України здійснюють розвідувальну діяльність щодо загроз національній безпеці України у кіберпросторі, інших подій і обставин, що стосуються сфери кібербезпеки;

6) Національний банк України визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб’єктів переказу коштів, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об’єктах критичної інфраструктури у банківській системі України.

3. Функціонування національної системи кібербезпеки забезпечується шляхом:

1) вироблення і оперативної адаптації державної політики у сфері кібербезпеки, спрямованої на розвиток кіберпростору, досягнення сумісності з відповідними стандартами Європейського Союзу та НАТО;

2) створення нормативно-правової та термінологічної бази у сфері кібербезпеки, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної безпеки та кібербезпеки відповідно до міжнародних стандартів, зокрема стандартів Європейського Союзу та НАТО;

3) встановлення обов’язкових вимог інформаційної безпеки об’єктів критичної інформаційної інфраструктури, у тому числі під час їх створення, введення в експлуатацію, експлуатації та модернізації з урахуванням міжнародних стандартів та специфіки галузі, до якої належать відповідні об’єкти критичної інформаційної інфраструктури;

4) формування конкурентного середовища у сфері електронних комунікацій, надання послуг із захисту інформації та кіберзахисту;

5) залучення експертного потенціалу наукових установ, професійних та громадських об’єднань до підготовки проектів концептуальних документів у сфері кібербезпеки;

6) проведення навчань щодо дій у разі надзвичайних ситуацій та інцидентів у кіберпросторі;

7) функціонування системи аудиту інформаційної безпеки, запровадження кращих світових практик і міжнародних стандартів з питань кібербезпеки та кіберзахисту;

8) розвитку мережі команд реагування на комп’ютерні надзвичайні події;

9) розвитку та вдосконалення системи технічного і криптографічного захисту інформації;

10) забезпечення дотримання вимог законодавства щодо захисту державних інформаційних ресурсів та інформації;

11) створення та забезпечення функціонування Національної телекомунікаційної мережі;

12) обміну інформацією про інциденти кібербезпеки між суб’єктами забезпечення кібербезпеки у порядку, визначеному законодавством;

13) впровадження єдиної (універсальної) системи індикаторів кіберзагроз з урахуванням міжнародних стандартів з питань кібербезпеки та кіберзахисту;

14) підготовки фахівців освітньо-кваліфікаційних рівнів бакалавра і магістра за державним замовленням в обсязі, необхідному для задоволення потреб державного сектору економіки, а також за небюджетні кошти, у тому числі для підвищення кваліфікації та проведення обов’язкової періодичної атестації (переатестації) персоналу, відповідального за забезпечення кібербезпеки об’єктів критичної інфраструктури, з урахуванням міжнародних стандартів;

15) впровадження організаційно-технічної моделі національної системи кібербезпеки як комплексу заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливості комунікаційних систем;

16) встановлення вимог (правил, настанов) щодо безпечного використання мережі Інтернет та надання електронних послуг державними органами;

17) державно-приватної взаємодії у запобіганні кіберзагрозам об’єктам критичної інфраструктури, реагуванні на кібератаки та кіберінциденти, усуненні їх наслідків, зокрема в умовах кризових ситуацій, надзвичайного і воєнного стану, в особливий період;

18) періодичного проведення огляду національної системи кібербезпеки, розроблення індикаторів стану кібербезпеки;

19) стратегічного планування та програмно-цільового забезпечення у сфері розвитку електронних комунікацій, інформаційних технологій, захисту інформації та кіберзахисту;

20) розвитку міжнародного співробітництва у сфері кібербезпеки, підтримки міжнародних ініціатив у сфері кібербезпеки, що відповідають національним інтересам України, поглиблення співпраці України з Європейським Союзом та НАТО з метою посилення спроможності України у сфері кібербезпеки, участі у заходах із зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;

21) здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидії кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності у кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях;

22) здійснення воєнно-політичних, військово-технічних та інших заходів для розширення можливостей Воєнної організації держави, сектору безпеки і оборони з використанням кіберпростору, створення і розвитку сил, засобів та інструментів можливої відповіді на агресію у кіберпросторі, яка може застосовуватися як засіб стримування воєнних конфліктів та загроз з використанням кіберпростору;

23) обмеження участі у заходах із забезпечення інформаційної безпеки та кібербезпеки будь-яких суб’єктів господарювання, які перебувають під контролем держави, визнаної Верховною Радою України державою-агресором, або держав та осіб, стосовно яких діють спеціальні економічні та інші обмежувальні заходи (санкції), прийняті на національному або міжнародному рівні внаслідок агресії щодо України, а також обмеження використання продукції, технологій та послуг таких суб’єктів для забезпечення технічного та криптографічного захисту державних інформаційних ресурсів, посилення державного контролю в цій сфері;

24) розвитку системи контррозвідувального забезпечення кібербезпеки, призначеної для запобігання, своєчасного виявлення та протидії зовнішнім і внутрішнім загрозам безпеці України з використанням кіберпростору; усунення умов, що їм сприяють, та причин їх виникнення;

25) проведення розвідувальних заходів із виявлення та протидії загрозам національній безпеці України у кіберпросторі, виявлення інших подій і обставин, що стосуються сфери кібербезпеки.

4. Порядок функціонування Національної телекомунікаційної мережі, критерії, правила та вимоги щодо надання послуг, їх тарифікації для користувачів бюджетної сфери, відшкодування витрат державного бюджету на утримання Національної телекомунікаційної мережі затверджуються Кабінетом Міністрів України.

5. Впровадження організаційно-технічної моделі кібербезпеки як складової національної системи кібербезпеки здійснюється Державним центром кіберзахисту, який забезпечує створення та функціонування основних складових системи захищеного доступу державних органів до мережі Інтернет, системи антивірусного захисту національних інформаційних ресурсів, аудиту інформаційної безпеки та стану кіберзахисту об’єктів критичної інформаційної інфраструктури, системи виявлення вразливостей і реагування на кіберінциденти та кібератаки щодо об’єктів кіберзахисту, системи взаємодії команд реагування на комп’ютерні надзвичайні події, а також у взаємодії з іншими суб’єктами забезпечення кібербезпеки розробляє сценарії реагування на кіберзагрози, заходи щодо протидії таким загрозам, програми та методики проведення кібернавчань.

Стаття 9. Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA

1. Завданнями CERT-UA є:

1) накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

2) надання власникам об’єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об’єктів;

3) організація та проведення практичних семінарів з питань кіберзахисту для суб’єктів національної системи кібербезпеки та власників об’єктів кіберзахисту;

4) підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

5) взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

6) взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

7) взаємодія з українськими командами реагування на комп’ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, які провадять діяльність, пов’язану із забезпеченням безпеки кіберпростору;

8) опрацювання отриманої від громадян інформації про кіберінциденти щодо об’єктів кіберзахисту;

9) сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам.

2. Забезпечення функціонування CERT-UA здійснює Державна служба спеціального зв’язку та захисту інформації України у межах штатної чисельності та виділених обсягів фінансування.

Стаття 10. Державно-приватна взаємодія у сфері кібербезпеки

1. Державно-приватна взаємодія у сфері кібербезпеки здійснюється шляхом:

1) створення системи своєчасного виявлення, запобігання та нейтралізації кіберзагроз, у тому числі із залученням волонтерських організацій;

2) підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і вмінь, необхідних для підтримки цілей кібербезпеки, реалізації державних і громадських проектів з підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту;

3) обміну інформацією між державними органами, приватним сектором і громадянами щодо кіберзагроз об’єктам критичної інфраструктури, інших кіберзагроз, кібератак та кіберінцидентів;

4) партнерства та координації команд реагування на комп’ютерні надзвичайні події;

5) залучення експертного потенціалу, наукових установ, професійних об’єднань та громадських організацій до підготовки ключових галузевих проектів та нормативних документів у сфері кібербезпеки;

6) надання консультативної та практичної допомоги з питань реагування на кібератаки;

7) формування ініціатив та створення авторитетних консультаційних пунктів для громадян, представників промисловості та бізнесу з метою забезпечення безпеки в мережі Інтернет;

8) запровадження механізму громадського контролю ефективності заходів із забезпечення кібербезпеки;

9) періодичного проведення національного саміту з професійними постачальниками бізнес-послуг, включаючи страховиків, аудиторів, юристів, визначення їхньої ролі у сприянні кращому управлінню ризиками у сфері кібербезпеки;

10) створення системи підготовки кадрів та підвищення компетентності фахівців різних сфер діяльності з питань кібербезпеки;

11) тісної взаємодії з фізичними особами, громадськими та волонтерськими організаціями, ІТ-компаніями з метою виконання заходів кібероборони в кіберпросторі.

2. Державно-приватна взаємодія у сфері кібербезпеки застосовується з урахуванням встановлених законодавством особливостей правового режиму щодо окремих об’єктів та окремих видів діяльності.

Стаття 11. Сприяння суб’єктам забезпечення кібербезпеки України

Державні органи та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та об’єднання громадян зобов’язані сприяти суб’єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об’єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків.

Стаття 12. Відповідальність за порушення законодавства у сфері кібербезпеки

Особи, винні у порушенні законодавства у сферах національної безпеки, електронних комунікацій та захисту інформації, якщо кіберпростір є місцем та/або способом здійснення злочину, іншого винного діяння, відповідальність за яке передбачена цивільним, адміністративним, кримінальним законодавством, несуть відповідальність згідно із законом.

Стаття 13. Фінансове забезпечення заходів кібербезпеки

Джерелами фінансування робіт і заходів із забезпечення кібербезпеки та кіберзахисту є кошти державного і місцевих бюджетів, власні кошти суб’єктів господарювання, кредити банків, кошти міжнародної технічної допомоги та інші джерела, не заборонені законодавством.

Стаття 14. Міжнародне співробітництво у сфері кібербезпеки

1. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з міжнародною кіберзлочинністю.

2. Україна відповідно до міжнародних договорів, згода на обов’язковість яких надана Верховною Радою України, може брати участь у спільних заходах із забезпечення кібербезпеки, зокрема у проведенні спільних навчань суб’єктів сектору безпеки і оборони в рамках заходів колективної оборони з дотриманням вимог законів України "Про порядок направлення підрозділів Збройних Сил України до інших держав" та "Про порядок допуску та умови перебування підрозділів збройних сил інших держав на території України".

3. Відповідно до законодавства України у сфері зовнішніх зносин суб’єкти забезпечення кібербезпеки у межах своїх повноважень можуть здійснювати міжнародну співпрацю у сфері кібербезпеки безпосередньо на двосторонній або багатосторонній основі.

4. Інформацію з питань, пов’язаних із боротьбою з міжнародною кіберзлочинністю, Україна надає іноземній державі на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов’язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору.

Стаття 15. Контроль за законністю заходів із забезпечення кібербезпеки України

1. Контроль за дотриманням законодавства при здійсненні заходів із забезпечення кібербезпеки здійснюється Верховною Радою України в порядку, визначеному Конституцією України.

Парламентський контроль за дотриманням законодавства про захист персональних даних та доступ до публічної інформації у сфері кібербезпеки здійснюється Уповноваженим Верховної Ради України з прав людини.

2. Контроль за діяльністю із забезпечення кібербезпеки суб’єктів сектору безпеки і оборони, інших державних органів здійснюється Президентом України та Кабінетом Міністрів України в порядку, визначеному Конституцією і законами України.

3. Незалежний аудит діяльності основних суб’єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави проводиться щороку згідно з міжнародними стандартами аудиту.

Звіти про результати проведення незалежного аудиту діяльності основних суб’єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, щодо ефективності системи забезпечення кібербезпеки держави за попередній рік подаються Президентові України, Верховній Раді України та Кабінету Міністрів України у сорокап’ятиденний строк після закінчення календарного року.

Комітет Верховної Ради України, до предмета відання якого належать питання національної безпеки і оборони, та Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв’язку, на своїх засіданнях розглядають звіти основних суб’єктів національної кібербезпеки, визначених частиною другою статті 8 цього Закону, про результати незалежного аудиту їхньої діяльності щодо ефективності системи забезпечення кібербезпеки держави.

Основні суб’єкти національної кібербезпеки, визначені частиною другою статті 8 цього Закону, подають один раз на рік звіти про стан виконання ними заходів з питань забезпечення кібербезпеки держави, віднесених до їх компетенції, які мають містити, зокрема, інформацію про результати проведення незалежного аудиту їхньої діяльності.

За результатами розгляду звітів основних суб’єктів національної кібербезпеки Комітет Верховної Ради України, до предмета відання якого належать питання інформатизації та зв’язку, може порушити питання про розгляд цих питань Верховною Радою України.

ПРИКІНЦЕВІ ТА ПЕРЕХІДНІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності через шість місяців з дня його опублікування.

2. Внести зміни до таких законів України:

1) статтю 7 Закону України "Про Національний банк України" (Відомості Верховної Ради України, 1999 р., № 29, ст. 238 із наступними змінами) доповнити пунктами 32 і 33 такого змісту:

"32) визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки у банківській системі України та для суб’єктів переказу коштів, здійснює контроль за їх виконанням; утворює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту у банківській системі України;

33) забезпечує формування та ведення переліку об’єктів критичної інфраструктури, а також реєстру об’єктів критичної інформаційної інфраструктури у банківській системі України, визначає критерії та порядок віднесення об’єктів у банківській системі України до об’єктів критичної інфраструктури та об’єктів критичної інформаційної інфраструктури, забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки у банківській системі України";

2) у Законі України "Про оборону України" (Відомості Верховної Ради України, 2000 р., № 49, ст. 420; 2011 р., № 4, ст. 27; 2015 р., № 16, ст. 110; 2016 р., № 33, ст. 564):

а) статтю 3 після абзацу дев’ятнадцятого доповнити новим абзацом такого змісту:

"здійснення заходів з кібероборони (активного кіберзахисту) для захисту суверенітету держави та забезпечення її обороноздатності, запобігання збройному конфлікту та відсічі збройній агресії".

У зв’язку з цим абзац двадцятий вважати абзацом двадцять першим;

б) друге речення частини другої статті 4 доповнити словами "у тому числі проведення спеціальних операцій (розвідувальних, інформаційно-психологічних тощо) у кіберпросторі";

3) у Законі України "Про розвідувальні органи України" (Відомості Верховної Ради України, 2001 р., № 19, ст. 94; 2006 р., № 14, ст. 116; 2016 р., № 33, ст. 564 із наступними змінами):

а) абзац другий статті 1 після слів "за межами України" доповнити словами "у тому числі у кіберпросторі";

б) абзац шостий статті 4 після слів "національній безпеці України" доповнити словами "у тому числі у кіберпросторі";

{Підпункт 4 пункту 2 розділу втратив чинність на підставі Закону № 2469-VIII від 21.06.2018}

5) абзац шостий статті 3 Закону України "Про Службу зовнішньої розвідки України" (Відомості Верховної Ради України, 2006 р., № 8, ст. 94) після слів "національній безпеці України" доповнити словами "у тому числі у кіберпросторі";

6) у Законі України "Про Державну службу спеціального зв’язку та захисту інформації України" (Відомості Верховної Ради України, 2014 р., № 25, ст. 890, № 29, ст. 946):

а) частину першу статті 2 та абзац другий частини першої статті 3 після слів "криптографічного та технічного захисту інформації" доповнити словом "кіберзахисту";

б) у частині першій статті 14:

пункт 39 після слів "забезпечення функціонування" доповнити словом "урядової";

доповнити пунктами 85-92 такого змісту:

"85) формування та реалізація державної політики щодо захисту у кіберпросторі державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, кіберзахисту критичної інформаційної інфраструктури, здійснення державного контролю у цих сферах;

86) координація діяльності суб’єктів забезпечення кібербезпеки щодо кіберзахисту;

87) забезпечення створення та функціонування Національної телекомунікаційної мережі;

88) впровадження організаційно-технічної моделі кіберзахисту, здійснення організаційно-технічних заходів із запобігання, виявлення та реагування на кіберінциденти і кібератаки та усунення їх наслідків;

89) інформування про кіберзагрози та відповідні методи захисту від них;

90) забезпечення впровадження системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури, встановлення вимог до аудиторів інформаційної безпеки, їх атестації (переатестації);

91) координація, організація та проведення аудиту захищеності комунікаційних і технологічних систем об’єктів критичної інфраструктури на вразливість;

92) забезпечення функціонування Державного центру кіберзахисту".

3. Кабінету Міністрів України у тримісячний строк з дня набрання чинності цим Законом:

забезпечити прийняття нормативно-правових актів, необхідних для реалізації цього Закону;

привести свої нормативно-правові акти у відповідність із цим Законом;

забезпечити перегляд і скасування міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів, що суперечать цьому Закону.

Характерною ознакою сучасного етапу економічного та науково-технічного прогресу є стрімкий розвиток інформаційних технологій, їх якнайширше використання як у повсякденному житті, так і в управлінні державою. Інформація і інформаційні технології все більше визначають розвиток суспільства та слугують новими джерелами національної могутності. Становлення інформаційного суспільства радикально змінює політичну, екологічну та соціальну сфери життєдіяльності людства. У цих умовах формування інформаційного суспільства змінює предмет праці на інформацію і знання. У свою чергу основою глобалізації стають інтеграція інформаційних систем різних держав до єдиної загальносвітової інформаційної системи, формування єдиного інформаційного простору, створення глобальних інформаційно-телекомунікаційних тенет, інтенсивне впровадження нових інформаційних технологій в усі галузі суспільного життя, включаючи і державне управління [10].

Інформаційний суверенітет та інформаційна безпека гарантуються і забезпечуються Конституцією України, Законом України "Про Інформаційний суверенітет та інформаційну безпеку України", Законами України “Про інформацію”, “Про друковані засоби масової інформації (пресу) в Україні”, “Про телебачення і радіомовлення”, “Про авторське право та суміжні права”, “Про державну таємницю”, “Про захист інформації в автоматизованих системах”. “Про національний архівний фонд та архівні установи”, “Про охорону і використання пам'яток історії та культури”, “Про інформаційні агентства”, “Про зв'язок”, “Про рекламу”, “Про видавничу справу”, “Про професійних творчих працівників та творчі спілки”, “Про державну підтримку засобів масової інформації та соціальний захист журналістів”, “Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації”, “Про кінематографію”, “«Про Національну раду України з питань телебачення і радіомовлення”, “Про систему Суспільного телебачення і радіомовлення України’, Основами законодавства України про культуру, іншими законодавчими актами, а також міжнародними договорами і конвенціями в галузі свободи слова та інформаційної діяльності, ратифікованими Україною.

У Законі «Про основи національної безпеки України» вперше дано офіційну оцінку значущості й системної сутності інформаційної безпеки як невід'ємної складової національної безпеки України [12].



Рис.1.1. Основні елементи системи забезпечення інформаційної безпеки

У п. 2.8. Стратегії національної безпеки, присвяченому стану інформаційної безпеки в нашій державі, зазначено:

* + - * посилюється негативний зовнішній вплив на інформаційний простір України, що загрожує розмиванням суспільних цінностей і національної ідентичності;
      * недостатніми залишаються обсяги вироблення конкурентоспроможного національного інформаційного продукту;
      * наближається до критичного стан безпеки інформаційно-комп'ютерних систем у галузі державного управління, фінансової і банківської сфери, енергетики, транспорту, внутрішніх та міжнародних комунікацій тощо.

Ще в одному офіційному документі – «Рекомендаціях парламентських слухань з питань розвитку інформаційного суспільства в Україні» ідеться, що стан розбудови інформаційного суспільства в Україні порівняно зі світовими тенденціями є недостатнім і не відповідає потенціалу та можливостям України, зокрема:

* + - * відсутні національна стратегія розвитку інформаційного суспільства в Україні та план дій щодо її реалізації;
      * немає координації зусиль державного і приватного секторів для ефективного використання наявних ресурсів;
      * ефективність використання фінансових, матеріальних, кадрових ресурсів, спрямованих на виконання Національної програми інформатизації, впровадження інформаційно-комунікаційних технологій у соціально-економічну сферу, зокрема в сільське господарство, є низькою;
      * є відставання у впровадженні технологій електронного бізнесу, електронних бірж та аукціонів, електронних депозитаріїв, використанні безготівкових розрахунків за товари та послуги тощо;
      * рівень інформатизації окремих галузей економіки, деяких регіонів країни є низьким;
      * розвиток нормативно-правової бази інформаційної сфери є недостатнім;
      * створення національної інформаційної інфраструктури для надання органами державної влади та органами місцевого самоврядування юридичним і фізичним особам інформаційних послуг з використанням Інтернету відбувається повільно;
      * рівень комп'ютерної грамотності населення є недостатнім, впровадження нових методів навчання із застосуванням сучасних інформаційно-комунікаційних технологій – повільним;
      * рівень інформаційної представленості України в інтернет-просторі є низьким, а присутність в Інтернеті україномовних інформаційних ресурсів – недостатньою;
      * рівень державної підтримки виробництва засобів інформатизації, програмних засобів і впровадження інформаційно-комунікаційних технологій не забезпечує всіх потреб економіки й суспільного життя;
      * спостерігаються нерівномірність забезпечення можливості доступу населення до комп'ютерних і телекомунікаційних засобів, поглиблення «інформаційної нерівності» між окремими регіонами, галузями економіки та різними верствами населення;
      * не вирішуються в повному обсязі питання захисту авторських прав на програмну продукцію, відсутні системні державні рішення, спрямовані на створення національних структур (центрів, технополісів і технопарків) з розробки конкурентоспроможного програмного забезпечення.

І це незважаючи на те, що за минулі роки відбулася досить серйозна трансформація інформаційної організації держави. Організаційно-правові засади у сфері інформаційної безпеки, що діють сьогодні в Україні, загалом створюють необхідні передумови для реалізації відповідної державної політики. Проте новий виток технологічних успіхів в інформатиці поряд із прогресивними можливостями, що відкриваються, народжує й нові загрози безпеці.

На жаль, пріоритети державної політики визначаються не деклараціями, навіть якщо вони закріплені в нормативно-правових актах, а їх реальним ресурсним забезпеченням: фінансовим, організаційним, кадровим та ін.. Відсутність чітко визначених і підкріплених ресурсами пріоритетів розвитку інформаційної сфери не дозволяє зменшити технологічне відставання України від розвинутих держав.

Стан інформаційного простору України характеризується наявністю протиріччя між потребами суспільства в розширенні вільного обміну інформацією і необхідністю окремих обмежень на її поширення. Необхідно відзначити, що порушенню інформаційної безпеки сприяє безсистемність захисту інформації і слабка координація дій по захисту інформації в загальнодержавному масштабі.

Рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, бо найчастіше реалізація інформаційних загроз - це нанесення шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо.

На сучасному етапі в Україні немає реальних гарантів інформаційної безпеки країни, відсутній комплекс нормативно-правових актів щодо захисту інформаційних ресурсів та інформаційної інфраструктури. Процес інформатизації має стихійний, некерований характер, з переважним ухилом у бік використання засобів інформатизації іноземного виробництва.

Безсистемність процесів формування інформаційної інфраструктури України обумовлює складність вирішення проблеми інформаційної безпеки, захисту інформаційних ресурсів. Специфіка цих проблем полягає в тому, що об’єктивно достатній рівень захищеності інформаційної інфраструктури та інформаційних ресурсів може бути досягнутий тільки у результаті чіткого визначення об’єктів інформаційної безпеки України, забезпечення надійного функціонування державних та суспільних інститутів для реалізації практичних заходів забезпечення інформаційної безпеки.

Основною метою забезпечення інформаційної безпеки країни є:

* захист національних інтересів в умовах все більшої глобалізації багатьох інформаційних процесів, формування світових інформаційних мереж, прагнення окремих розвинутих країн до домінування в інформаційній сфері;
* безперебійне забезпечення органів державної влади та управління, підприємств і громадян країни повною й своєчасною інформацією, необхідною для їх діяльності;
* запобігання порушень цілісності, збереження і незаконного використання інформаційних ресурсів;
* забезпечення практичної реалізації прав громадян, організацій і держави на отримання, розповсюдження та використовування інформації.

Для досягнення мети забезпечення інформаційної безпеки держави важливо правильно визначати об'єкти інформаційної безпеки. До таких об'єктів відносяться:

* інформаційні ресурси, що містять конфіденційну інформацію (секретну, обмеженого доступу або ж комерційну таємницю), а також загальнодоступну відкриту інформацію та наукові знання;
* інформаційна інфраструктура суспільства (мережі зв'язку та інформаційних комунікацій, центри аналізу та обробки даних, системи й засоби захисту інформації);
* система формування, розповсюдження та використовування інформаційних ресурсів в країні;
* система формування суспільної свідомості, що базується на засобах масової інформації;
* права громадян, юридичних осіб і держави на отримання, розповсюдження й використання інформації, а також захист конфіденційної інформації та інтелектуальної власності.

Негативні тенденції розвитку інформаційного простору України, недосконалість системи забезпечення інформаційної безпеки, кризовий стан вітчизняної економіки створюють передумови для ескалації загроз інформаційній безпеці України.

Джерелами загроз для інформаційної безпеки країни можуть бути зовнішні та внутрішні фактори.

До числа джерел зовнішніх загроз належить зарахувати такі:

* політика окремих країн, що направлена на домінування в інформаційній сфері та протидіюча доступу України до новітніх інформаційних технологій і рівноправної участі в міжнародному розподілі праці з виробництва засобів інформатики та інформаційних продуктів, на створення технологічної залежності України від інших країн в інформаційній сфері;
* розробка окремими державами концепцій "інформаційної війни", які передбачають створення та використання засобів небезпечного впливу на інформаційну сферу інших країн з метою порушення її нормального функціонування й несанкціонованого доступу до інформаційних ресурсів;
* діяльність іноземних розвідувальних і спеціальних служб, а також економічних і політичних структур в інформаційній сфері, направлена проти національних інтересів країни;
* злочинна діяльність міжнародних терористичних груп, організацій і окремих осіб в інформаційній сфері;
* розгортання окремими країнами світу "культурної експансії" щодо інших країн, і особливо проти України, що проявляється, зокрема, в прагненні скоротити використання української мови як засобу спілкування й таким чином зменшити український інформаційний простір.
* істотне відставання України від провідних країн світу за рівнем інформатизаціїсуспільства, що обмежує можливості країни відносно рівноправного входження в світовий інформаційний простір та Modern Information Technologies in the Sphere of Set.

Внутрішні загрози

Якщо говорити про джерела внутрішніх загроз для інформаційної безпеки нашої країни, то тут найважливішими є такі:

* + 1. В області геополітики та міжнародної співпраці їх результатом може стати втрата нашою країною свого міжнародного авторитету держави в області науки, освіти і високих технологій, а також втрата лідерства в певних напрямах розвитку науково-технічного прогресу. Внаслідок цього можуть скоротитися можливості впливу країни на розвиток світових геополітичних процесів, її рівноправної участі в міжнародному розподілі праці та використанні міжнародного інформаційного ринку продуктів і послуг, буде ускладнено ухвалення найважливіших політичних, економічних та інших рішень, в яких визначальне значення має міжнародний авторитет держави.
    2. В області соціально-економічного розвитку країни проявлятиметься тенденція до зниження темпів науково-технічного прогресу й переходу до використання високоефективних передових технологій, що призведе до уповільнення розвитку економіки, зниження якості та рівня життя людей, підвищення рівня соціальної напруженості в суспільстві.
    3. В області державного управління може відбутися дискредитація органів державної влади й місцевого самоврядування, створення штучних труднощів у забезпеченні їх нормального функціонування, а також дисбаланс інтересів людини, суспільства та держави, що може спровокувати соціальні, національні чи релігійні конфлікти в суспільстві, страйки й масове безладдя.
    4. В області розвитку культури, освіти та духовної сфери суспільства результатом впливу інформаційних загроз може стати втрата культурної спадщини Й національних традицій, розповсюдження чужої ідеології і моральних цінностей, прояв бездуховності та аморальності, втрата національної самосвідомості.
    5. В області обороноздатності та національної безпеки країни такими наслідками можуть бути:
* порушення системи управління військами, озброєнням і військовою технікою;
* зниження технологічного рівня розвитку оборонної промисловості;
* зниження морального духу особового складу збройних сил і працівників підприємств оборонного комплексу.
* - технологічне відставання вітчизняної електронної промисловості від розвинутих країн світу в області виробництва інформаційної та телекомунікаційної техніки, що змушує імпортувати ці засоби з-за кордону і на їх основі створювати свою національну інформаційну інфраструктуру, а це робить її уразливою з боку країн Заходу;
* недостатня координація діяльності органів державної влади країни щодо формування та реалізації єдиної державної політики забезпечення інформаційної безпеки України як найважливішої частини її національної безпеки;
* зниження рівня загальної освіти громадян України, що затрудняє підготовку фахівців необхідної кваліфікації, а також користувачів для роботи в інформаційній сфері;
* посилення організованої злочинності в країні та зростання кількості комп'ютерних злочинів, що знижує рівень захищеності інтересів громадян, організацій і держави в інформаційній сфері.

Усі перераховані вище можливі наслідки є досить серйозними для життя та діяльності кожного громадянина країни, а не тільки для еліти чи політичного керівництва. Саме тому проблема забезпечення інформаційної безпеки людини й суспільства повинна стати в сучасних умовах справою кожного. А для цього вона повинна бути, в першу чергу, чітко сформульована та доведена до свідомості широких мас населення через систему освіти й засоби масової інформації.

При подальшому розгортанні глобального процесу інформатизації, неминучої глобалізації морового співтовариства та переході розвинутих країн до інформаційного способу життя, значення даної проблеми відчуватиметься все сильніше й сильніше.

Основними задачами держави та суспільства по запобіганню, відбиттю та нейтралізації зовнішніх і внутрішніх загроз інформаційної безпеки є:

1)створення законодавчої бази забезпечення інформаційної безпеки, що формує правову основу для протидії інформаційним загрозам. Така база є зараз в багатьох країнах світу. Формується вона і в Україні. Ведеться робота зі створення механізмів практичної реалізації цих законів, готуються інші законопроекти, регулюючі суспільні відносини в інформаційній сфері;

2)проведення спеціальних заходів для забезпечення інформаційної безпеки в органах державної влади країни та місцевого самоврядування, створення захищеної інформаційно-телекомунікаційної системи органів державної влади, здатної протистояти зовнішнім і внутрішнім інформаційним загрозам;

3)створення та запровадження національної інформаційної інфраструктури,вітчизняних високоефективних засобів і систем захисту інформаційних ресурсів, а також методів забезпечення надійного й безперебійного функціонування органів державного управління та підприємств фінансової, економічної й суспільно-політичної сфери;

4) створення та практичне запровадження ефективних засобів, методів і систем захисту національних інформаційних ресурсів країни від руйнувань і несанкціонованого доступу, підвищення надійності та безпеки їх зберігання;

5) розвиток вітчизняної промисловості для виробництва в необхідних об'ємах сучасних засобів інформаційної техніки, що використовуються для створення й розвитку національної інформаційної інфраструктури, забезпечення діяльності оборонного комплексу, органів державного управління та найважливіших підприємств фінансової і ділової сфери.

Вирішення цієї проблеми крім економічних зусиль потребує також відповідної орієнтації системи освіти, науки й громадської думки в країні з тим, щоб зробити працю в цій області престижною та соціально привабливою. Тільки так можна забезпечити притік до цієї сфери людських ресурсів та підготовку необхідної кількості фахівців і науковців, отримання від цього відповідних економічних і соціально-політичних вигод;

Динаміка розвитку та використання інформаційних технологій, на жаль, розширює й можливості здійснення злочинів.

Варто зазначити, що дотепер в міжнародних актах і в національному законодавстві відсутні чітко сформульовані поняття киберзлочинності, кібербезпеки і кібертероризму. Необхідність забезпечення національної безпеки від цих загроз на основі узгодженості дій вимагає від міжнародного інформаційного співтовариства вироблення єдиного правового механізму врегулювання протидії використанню інформаційних технологій із злочинною метою.

Вплив перерахованих вище зовнішніх і внутрішніх загроз на інформаційну сферу країни може призвести до негативних наслідків для майбутнього нашої країни.

6)розробка та планомірне проведення спеціальних організаційно-правових і виховних заходів, направлених на запобігання інформаційних загроз в духовній сфері життя суспільства, формування суспільної свідомості населення країни в напрямку активної протидії цим загрозам.

До таких заходів, перш за все, повинні відноситися:

* проведення відкритої та активної пропаганди державної ідеології суспільства, яка була б зрозумілою й прийнятною для більшості населення та враховувала культурні, національні й історичні традиції розвитку країни;
* розробка, та здійснення цивілізованих форм впливу на ЗМІ з метою їх орієнтації на поширення в суспільстві духовних цінностей, що відповідають національній меті країни, вихованню патріотизму й громадянського обов'язку щодо захисту її інтересів [24].

Аналіз стану інформаційної безпеки України показує, що до основних проблем забезпечення інформаційної безпеки належать проблеми загальносистемного характеру, пов’язані з відсутністю наукового обґрунтування і практичної апробації політики і методології державної системи інформаційної безпеки. За характером це правові та нормативно-правові, науково-технічні, (економічні, організаційні, кадрові проблеми тощо).

Отже, інформаційна безпека України залежить від вирішення проблем формування і керування процесами суспільної свідомості, виробництва та репродукції інформаційних ресурсів і доступу до них, створення цивілізованого ринку інформаційних продуктів та послуг, реалізації прав громадян на інформацію.

## 1.2. Аналіз нормативно - правової бази забезпечення захисту інформації в автоматизованих системах

Проблема забезпечення безпеки автоматизованих систем (АС) - одна з найбільш важливих і складних проблем в області автоматизованої обробки інформації.

Оскільки компонентами АС є апаратні засоби, програмне забезпечення, що обробляється інформація, лінії зв'язку, персонал та документація, збиток автоматизованій системі - поняття досить широке. Крім того, шкодою вважається не тільки явне пошкодження будь-якого з компонентів, а й приведення компонентів системи з ладу, а також різного роду витоку інформації, зміна певних фізичних і логічних характеристик АС.

У цьому зв'язку визначення можливої шкоди АС є складним завданням, що залежить від багатьох умов. Можна з упевненістю сказати, що скрізь, де використовують АС, існує потенційна загроза нанесення шкоди (прямого чи непрямого) законним власникам і законним користувачам цих АС.

З іншого боку, заслуговує на увагу питання про вартість самої інформації. У світовій практиці прийнято вважати, що інформація коштує рівно стільки, скільки коштує збиток від її втрати в поєднанні з витратами на її відновлення.

Питання безпеки АС можна умовно розділити на наступні групи:

* • Питання забезпечення фізичної безпеки компонентів АС. Сюди належать питання захисту АС від пожежі, затоплення, інших стихійних лих, збоїв живлення, крадіжки, пошкодження і т.д.
* Питання забезпечення логічної безпеки компонентів АС. Сюди належать питання захисту АС від несанкціонованого доступу, від навмисних і ненавмисних помилок у дії людей і програм, які можуть призвести до збитку і т.д.
* Питання забезпечення соціальної безпеки АС. Сюди належать питання розробки законодавства, що регулює застосування АС і визначає порядок розслідування та покарання порушень безпеки АЕС.

Можливо, це здасться комусь не настільки важливим, але багато фахівців вважають, що чималу роль відіграють питання вироблення у користувачів АС певної дисципліни, а також формування певних етичних норм, обов'язкових для персоналу АС. До них слід віднести будь-які умисні або ненавмисні дії, які:

* порушують нормальну роботу АС;
* викликають додаткові витрати ресурсів (машинного часу, смуги передачі тощо);
* порушують цілісність зберігається і оброблюваної інформації;
* порушують інтереси законних користувачів;
* викликають незаплановані витрати ресурсів на ведення додаткового контролю, відновлення працездатності систем, знищення наслідків порушення безпеки систем і т.д.

З теоретичної точки зору, всі загрози АС, можна віднести до одного з наступних чотирьох типів.

Переривання. При перериванні компонент системи втрачається (наприклад, внаслідок викрадення), стає недоступним (наприклад, в результаті блокування - фізичної або логічного), або втрачає працездатність.

Перехоплення. Зловмисник отримує доступ до АС. Прикладами перехоплення є: незаконне копіювання програм і даних; несанкціоноване читання даних з лінії зв'язку комп'ютерної мережі і т.д.

Модифікація. Зловмисник не тільки отримує доступ до компонента, але й маніпулює над ним.

Підробка. Зловмисник може додати деякий фальшивий процес у систему для виконання потрібних йому, що не враховуються системою, дій, або підробленої запису у файли системи або інших користувачів.

Під захистом інформації в АС розуміється сукупність заходів, методів і засобів, які забезпечують вирішення наступних основних завдань:

* перевірка цілісності інформації;
* виключення несанкціонованого доступу до ресурсів АС і зберігаються в ній програмам і даним;
* виключення несанкціонованого використання зберігаються в АС програм (тобто захист програм від копіювання).

Існуюча в Україні нормативна база ще не досягла необхідного розвитку в області захисту інформації в АС. Так, наприклад, з величезного списку стандартів і нормативних документів України можна виділити лише деякі, які можуть бути використані при проектуванні захищених АС [5, 13-16].

Тому, при проведенні даного роду робіт, фахівці використовують також міжнародні (ISO) і міждержавні (ГОСТи, затверджені до 1992 року, включно) стандарти.

Згідно з одним із таких стандартів [2] АС являє собою систему, що складається з персоналу та комплексу засобів автоматизації його діяльності, реалізовує інформаційну технологію виконання установлених функцій.

Залежно від виду діяльності виділяють наступні види АС: автоматизовані системи управління (АСУ), системи автоматизованого проектування (САПР), автоматизовані системи наукових досліджень (АСНІ) і ін.

Залежно від виду керованого об'єкта (процесу) АСУ ділять на АСУ технологічними процесами (АСУТП), АСУ підприємствами (АСУП) і т.д.

У нашому випадку АС являє собою середовище обробки інформації, і також інформаційних ресурсів в інформаційно-телекомунікаційній системі. Тому надалі будемо використовувати поняття автоматизована інформаційна система.

Закон України «Про інформацію» [6] трактує поняття «інформація» в наступному вигляді: «під інформацією розуміється документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому середовищі».

У свою чергу, захист інформації в АС - діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації і АС в цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків у результаті реалізації загроз [5].

Для забезпечення захисту інформації в АС створюється служба захисту інформації (СЗІ). Згідно з Положенням [15] метою створення СЗІ є організаційне забезпечення завдань керування комплексною системою захисту інформації (КСЗІ) в АС та здійснення контролю за її функціонуванням. На СЗІ покладається виконання робіт з визначення вимог з захисту інформації в АС, проектування, розроблення і модернізації КСЗІ, а також з експлуатації, обслуговування, підтримки працездатності КСЗІ, контролю за станом захищеності інформації в АС.

Правову основу для створення і діяльності СЗІ становлять Закон України “Про захист інформації в автоматизованих системах ”, Положення про технічний захист інформації в Україні, Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах.

СЗІ у своїй діяльності керується Конституцією України, законами України, нормативно-правовими актами Президента України і Кабінету Міністрів України, іншими нормативно-правовими актами з питань захисту інформації, державними і галузевими стандартами, розпорядчими та іншими документами організації, а також цим положенням.

СЗІ здійснює діяльність відповідно до “Плану захисту інформації в автоматизованій системі ”, календарних, перспективних та інших планів робіт, затверджених керівником (заступником керівника) організації.

*Завданнями СЗІ є:*

* захист законних прав щодо безпеки інформації організації, окремих її структурних підрозділів, персоналу в процесі інформаційної діяльності та взаємодії між собою, а також у взаємовідносинах з зовнішніми вітчизняними і закордонними організаціями;
* дослідження технології обробки інформації в АС з метою виявлення можливих каналів витоку та інших загроз для безпеки інформації, формування моделі загроз, розроблення політики безпеки інформації, визначення заходів, спрямованих на її реалізацію;
* організація та координація робіт, пов’язаних з захистом інформації в АС,необхідність захисту якої визначається її власником або чинним законодавством, підтримка необхідного рівня захищеності інформації, ресурсів і технологій;
* розроблення проектів нормативних і розпорядчих документів, чинних у межах організації, згідно з якими повинен забезпечуватися захист інформації в АС;
* організація робіт зі створення і використання КСЗІ на всіх етапах життєвого циклу АС;
* участь в організації професійної підготовки і підвищенні кваліфікації персоналу та користувачів АС з питань захисту інформації;
* формування у персоналу і користувачів розуміння необхідності виконання вимог нормативно-правових актів, нормативних і розпорядчих документів, що стосуються сфери захисту інформації;
* організація забезпечення виконання персоналом і користувачами вимог
* нормативно-правових актів, нормативних і розпорядчих документів з захисту інформації в АС та проведення контрольних перевірок їх виконання.

## 1.3. Сучасні методи захисту інформації

Способи ЗІ залежать від типу інформації, форми її зберігання, обробки і передачі, типу носія інформації, а також передбачуваного способу нападу і наслідків його за впливом на інформацію (копіювання, спотворення, знищення).

Досвід застосування систем ЗІ (СЗІ) показує, що ефективною може бути лише комплексна система захисту інформації (КСЗІ), що поєднує такі заходи:

1. Законодавчі. Використання законодавчих актів, що регламентують права та обов'язки фізичних і юридичних осіб, а також держави в області ЗІ.
2. Морально-етичні. Створення і підтримка на об'єкті такої моральної атмосфери, в якій порушення регламентованих правил поведінки оцінювалося б більшістю співробітників різко негативно.
3. Фізичні. Створення фізичних перешкод для доступу сторонніх осіб до інформації, що охороняється.
4. Адміністративні. Організація відповідного режиму секретності, пропускного і внутрішнього режиму.
5. Технічні. Застосування електронних та інших пристроїв для ЗІ.
6. Криптографічні та стеганографічні. Застосування шифрування і кодування для приховування оброблюваної та переданої інформації від несанкціонованого доступу.
7. Програмні. Застосування програмних засобів розмежування доступу.

Обґрунтований вибір необхідного рівня захисту інформації є системоутворюючим завданням, оскільки як заниження, так і завищення рівня неминуче веде до втрат. При цьому останнім часом роль даного питання різко зросла у зв'язку з тим, що, по-перше, тепер до числа тих, що потребують захисту крім військових, державних і відомчих, включені також секрети промислові, комерційні і навіть особисті, а по-друге, сама інформація все більше стає товаром. Таким чином, для оцінки інформації необхідні показники двох видів:

* + характеризують інформацію як ресурс, що забезпечує діяльність товариства;
  + характеризують інформацію як об'єкт праці.

Показники першого виду носять прагматичний характер. До них відносять важливість, значимість з точки зору тих завдань, для вирішення яких використовується оцінювана інформація, повнота інформації для інформаційного забезпечення вирішуваних завдань; адекватність, тобто відповідність поточному стану відповідних об'єктів або процесів; релевантність інформації і її толерантність.

Показники другого виду повинні характеризувати інформацію як об'єкт праці, над якими здійснюються деякі процедури в процесі її переробки з метою інформаційного забезпечення вирішуваних завдань. До них відносяться: ефективність кодування інформації та її обсяг. Методи визначення цих показників досить повно розроблені в теорії інформації.

Всі сучасні методи захисту можна розділити на організаційні, технічні, криптографічні та програмні.

Засоби захисту у свою чергу можна розділити на постійно діючі та ті, що вмикаються при виявленні спробі нападу. За активністю вони діляться на пасивні, напівактивні й активні. За рівнем забезпечення ЗІ засоби захисту поділяються на 4 класи: системи слабкого захисту (1 клас), системи сильного захисту, системи дуже сильного захисту, системи особливого захисту.

### 1.3.1. Організаційні методи захисту інформації

Закони та нормативні акти виконуються тільки в тому випадку, якщо вони підкріплюються організаторською діяльністю відповідних структур, що створюються в державі, при відомствах, установах і організаціях. При розгляді питань безпеки інформації така діяльність відноситься до організаційних методів захисту інформації. Організаційні методи захисту інформації включають заходи, заходи та дії, які повинні здійснювати посадові особи в процесі створення і експлуатації КС для забезпечення заданого рівня безпеки інформації.

Організаційні методи захисту інформації тісно пов'язані з правовим регулюванням у сфері безпеки інформації. Відповідно до законів і нормативних актів в міністерствах, відомствах, на підприємствах (незалежно від форм власності) для захисту інформації створюються спеціальні служби безпеки (на практиці вони можуть називатися і інакше). Ці служби підпорядковуються, як правило, керівництву установи. Керівники служб організовують створення та функціонування систем захисту інформації.

Організаційний захист включає в себе регламентацію:

1)Формування та організації діяльності служби безпеки, забезпечення діяльності цих служб нормативно-методичними документами з організації захисту інформації.

2)Складання і регулярного оновлення складу інформації, що захищається компанією, складання і ведення переліку захищуваних паперових і електронних документів.

3)Дозвільної системи розмежування доступу персоналу до інформації, що захищається.

4)Методів відбору персоналу для роботи з інформацією, яка захищається, методики навчання та інструктування співробітників.

5)Напрямів і методів виховної роботи з персоналом, контролю дотримання співробітниками порядку захисту інформації.

6)Технології захисту, обробки та зберігання паперових і електронних документів.

7)Порядку захисту цінної інформації компанії від випадкових або навмисних несанкціонованих дій персоналу.

8)Ведення всіх видів аналітичної роботи.

9)Порядку захисту інформації при проведенні нарад, засідань, переговорів, прийому відвідувачів, роботі з представниками ЗМІ.

10)Обладнання та атестації приміщень і робочих зон, виділених для роботи з конфіденційною інформацією.

11)пропускного режиму на території, в будівлі, приміщеннях, ідентифікації транспорту і персоналу компанії.

12)Системи охорони території.

13)Дій персоналу в екстремальних ситуаціях.

14) Організаційних питань придбання, встановлення і експлуатації технічних засобів захисту інформації та охорони.

15)Роботи з управління системою захисту інформації.

16)Критеріїв і порядку проведення оціночних заходів зі встановлення ступеня ефективності системи захисту інформації.

Система організаційних заходів із захисту інформації представляють собою комплекс заходів, що включають чотири основні компоненти:

* + Вивчення обстановки на об'єкті;
  + Розробку програми захисту;
  + Діяльність з проведення зазначеної програми в життя;
  + Контроль за її дієвістю та виконанням встановлених правил.

Виділяють наступні організаційні заходи:

* + Ознайомлення зі співробітниками, їх вивчення, навчання правилам роботи з конфіденційною інформацією, ознайомлення з заходами відповідальності за порушення правил захисту інформації та ін;
  + Організація надійної охорони приміщень і території проходження лінії зв'язку;
  + Організація, зберігання і використання документів і носіїв конфіденційної інформації, включаючи порядок обліку, видачі, виконання і повернення;
  + Створення штатних організаційних структур щодо захисту цінної інформації або призначення відповідального за захист інформації на конкретних етапах її обробки і передачі;
  + Створення особливого порядку взаємовідносин зі сторонніми організаціями та партнерами;
  + Організація конфіденційного діловодства.

Організаційні заходи відіграють істотну роль у створенні надійного механізму захисту інформації, так як можливості несанкціонованого використання конфіденційних відомостей в значній мірі обумовлюються не технічними аспектами, а зловмисними діями, недбальством, недбалістю і халатністю користувачів або персоналу захисту. Впливу цих аспектів практично неможливо уникнути за допомогою технічних засобів. Для цього необхідна сукупність організаційно-правових та організаційно-технічних заходів, які виключали б (або, принаймні, зводили б до мінімуму) можливість виникнення небезпеки для конфіденційної інформації [19].

### 1.3.2. Технічні засоби захисту інформації

Технічними називаються такі засоби захисту інформації, в яких основна захисна функція реалізується технічним пристроєм (комплексом або системою).

Безперечними достоїнствами технічних засобів захисту інформації (ТСЗІ) є:

* досить висока надійність;
* досить широке коло завдань;
* можливість створення комплексних систем ЗИ (КСЗІ);
* гнучке реагування на спроби несанкціонованого впливу;
* традиційність використовуваних методів здійснення захисних функцій.

Основні недоліки ТСЗІ полягають у наступному:

* висока вартість багатьох засобів;
* необхідність регулярного проведення регламентних робіт і контролю;
* можливість видачі фіктивних тривог.

Системну класифікацію ТСЗІ зручно провести за такою сукупністю критеріїв:

* здійсненне функція захисту;
* ступінь складності пристрою;
* спряженість із засобами Вт

Наведені значення критеріїв інтерпретуються наступним чином.

* Спряженість із засобами Вт
* Автономні - засоби, що виконують свої захисні функції незалежно від функціонування засобів ОТ, тобто повністю автономно.
* Парні - кошти, виконані у вигляді самостійних пристроїв, але виконують захисні функції в сполученні (спільно) з основними засобами Вт
* Вбудовані - кошти, які конструктивно включені до складу апаратури Вт
* Виконувана функція захисту.
* Зовнішній захист - захист від дії дестабілізуючих факторів, що виявляються за межами зони ресурсів.
* Розпізнавання - специфічна група засобів, призначених для впізнання людей з різних індивідуальних характеристик.
* Внутрішній захист - захист від дії дестабілізуючих факторів, що виявляються безпосередньо в засобах обробки інформації.
* Ступінь складності пристрою.
* Прості пристрої - нескладні прилади і пристосування, що виконують окремі процедури захисту.
* Складні пристрої - комбіновані агрегати, що складаються з деякої кількості простих пристроїв, здатні до здійснення складних процедур захисту.
* Системи - закінчені технічні об'єкти, здатні здійснювати деяку комбіновану процедуру захисту, що має самостійне значення.

### 1.3.3. Програмні методи захисту інформації

Програмними ЗЗІ називаються спеціальні програми, що входять до складу програмного забезпечення АС для вирішення в них (самостійно або разом з іншими засобами) завдань захисту. Програмні ЗЗІ є неодмінною і найважливішою частиною механізму захисту сучасних АС. Така їх роль визначається наступними перевагами: універсальністю, гнучкістю, простий реалізацією, надійністю, можливістю модифікації та розвитку.

При цьому під універсальністю розуміється можливість вирішення програмними ЗЗІ великої кількості завдань захисту.

Під надійністю розуміється висока програмна стійкість при великій тривалості безперервної роботи та задоволення високим вимогам і достовірності керуючих впливів при наявності різних дестабілізуючих факторів. Програмні можливості зміни і розвитку програмних ЗЗІ визначаються самою їх природою.

Істотним недоліком програмних ЗЗІ є можливість їх реалізації тільки в тих структурних елементах АС, де є процесор, хоча функції захисту можуть реалізовуватися, здійснюючи безпеку інших структурних елементів. Крім того, програмним ЗЗІ притаманні такі недоліки:

* необхідність використання часу роботи процесора, що веде до збільшення часу відгуку на запити і, як наслідок, до зменшення ефективності її роботи;
* зменшення обсягів оперативної пам'яті (ОП) і пам'яті на зовнішніх запам'ятовуючих пристроях (ПВЗУ), доступної для використання функціональними завданнями;
* можливість випадкового або навмисного зміни, внаслідок чого програми можуть не тільки втратити здатність виконувати функції захисту, але і стати додатковими джерелами загрози безпеці;
* обмеженість через жорстку орієнтації на архітектуру певних типів ЕОМ (навіть у рамках одного класу) - залежність програм від особливостей базової системи введення / виводу, таблиці векторів переривання і т.п.

Для організаційної побудови програмних ЗЗІ найбільш характерною є тенденція розробки комплексних програм, що виконують цілий ряд захисних функцій, причому найчастіше в число цих функцій входить упізнання користувачів, розмежування доступу до масивів даних, заборона доступу до деяких областях ВП і т.п. Переваги таких програм очевидні: кожна з них забезпечує рішення деякого числа важливих завдань захисту. Але їм притаманні і суттєві недоліки, що зумовлюють необхідність критичної оцінки сформованої практики розробки та використання програмних засобів захисту. Перший і головний недолік полягає в стихійності розвитку програм захисту, що, з одного боку, не дає гарантій повноти наявних коштів, а з іншого - не виключає дублювання одних і тих же завдань захисту. Другим істотним недоліком є жорстка фіксація в кожному з комплексів програм захисних функцій. Нарешті, можна виділити ще один великий недолік - орієнтація переважної більшості наявних програмних засобів на конкретне середовище застосування (тип ЕОМ і операційного середовища).

Звідси випливають три принципово важливі вимоги до формування програмних ЗЗІ: функціональна повнота, гнучкість і уніфікованість використання.

Що стосується першої вимоги, то, як неважко переконатися, наведений вище перелік програмних засобів складений саме з таким розрахунком, щоб максимально повно охопити всі класи задач захисту.

Задоволення іншим двом вимогам залежить від форм і способів представлення програм захисту. Аналіз показав, що найбільш повно вимогам гнучкості та уніфікованості задовольняє наступна сукупність принципів: наскрізна модульна будова, повна структуризація, подання на машинно-незалежній мові.

Принцип наскрізного модульної побудови полягає в тому, що кожна з програм будь-якого рівня (обсягу) повинна представлятися у вигляді системи можливих модулів, причому кожен модуль будь-якого рівня повинен бути повністю автономним і мати стандартні вхід і вихід, що забезпечують комплексування з будь-якими іншими модулями. Неважко побачити, що ці умови можуть бути забезпечені, якщо програмні комплекси будуть розроблятися за принципом "зверху вниз", тобто відповідно до принципу повної структуризації.

Подання на машинно-незалежній мові зумовлює, що подання програмних модулів повинно бути таким, щоб їх з мінімальними зусиллями можна було включити до складу програмного забезпечення будь-якої АС. В даний час є алгоритмічні мови високого рівня, які повністю відповідають цим вимогам.

Загальноприйнятої класифікації програмних ЗЗІ в даний час не існує. Однак при описі програм захисту зазвичай дотримуються розподілу їх за функціональною ознакою, тобто за наявністю виконуваних функцій захисту. При цьому в міру розвитку форм і способів використання обчислювальної техніки функції програмного захисту розширюються.

### 1.3.4. Криптографічні методи захисту

Криптографія (від грецького kryptos — прихований і graphein — писати) — наука про математичні методи забезпечення конфіденційності (неможливості прочитання інформації стороннім) і автентичності (цілісності і справжності авторства) інформації. Розвинулась з практичної потреби передавати важливі відомості найнадійнішим чином. Для математичного аналізу криптографія використовує інструментарій абстрактної алгебри. [20]

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів. Відомо більш десятка перевірених алгоритмів шифрування, які при використанні ключа достатньої довжини і коректної реалізації алгоритму, роблять шифрований текст недоступним для криптоаналізу. Широко використовуються такі алгоритми шифрування як Twofish, IDEA, RC4 та ін.

У багатьох країнах прийняті національні стандарти шифрування. У 2001 році в США прийнятий стандарт симетричного шифрування AES на основі алгоритму Rijndael з довжиною ключа 128, 192 і 256 біт. Алгоритм AES прийшов на зміну колишньому алгоритмові DES, який тепер рекомендовано використовувати тільки в режимі Triple-DES (3DES).

Тривалий час під криптографією розумілось лише шифрування — процес перетворення звичайної інформації (відкритого тексту) в незрозуміле «сміття» (тобто, шифротекст). Дешифрування — це обернений процес відтворення інформації із шифротексту. Шифром називається пара алгоритмів шифрування/дешифрування. Дія шифру керується як алгоритмами, та і в кожному випадку ключем.

Ключ — це секретний параметр (в ідеалі, відомий лише двом сторонам) для окремого контексту під час передачі повідомлення. Ключі мають велику важливість, оскільки без змінних ключів алгоритми шифрування легко зламуються і непридатні для використання в більшості випадків. Історично склалось так, що шифри часто використовуються для шифрування та дешифрування, без виконання додаткових процедур, таких як аутенифікація або перевірка цілісності.

Криптографія може бути стійкою, а може бути і слабкою, як описано в приведеному прикладі. Криптографічна стійкість виміряється тим, скільки знадобиться часу і ресурсів, щоб із шифротекста відновити вихідний відкритий текст. Результатом стійкої криптографії є шифротекст, що винятково складно зламати без володіння визначеними інструментами по дешифруванню [9].

### 1.3.5. Стеганографія

Надійний захист інформації від несанкціонованого доступу є актуальної, але не вирішеною в повному обсязі проблемою .Один із перспективних напрямків захисту інформації сформували сучасні методи стеганографії. Слово стеганографія в перекладі з грецької буквально означає тайнопис (steganos - таємниця, секрет; graphy - запис).

Стеганографія являє собою сукупність методів, що ґрунтуються на різних принципах, які забезпечують приховування самого факту існування секретної інформації в тому чи іншому середовищі, а також засобів реалізації цих методів. До неї можна віднести величезне безліч секретних засобів зв'язку, таких як невидиме чорнило, мікрофотознімки, умовне розташування знаків, таємні (приховані) канали, засоби зв'язку з плаваючими частотами, голографія і т.д.

В даний час розвиваються методи комп'ютерної стеганографії - самостійного наукового напрямку інформаційної безпеки, що вивчає проблеми створення компонентів приховується у відкритому інформаційному середовищі, яка може бути сформована обчислювальними системами та мережами. Особливістю стеганографічного підходу є те, що він не передбачає прямого оголошення факту існування інформації, що захищається. Це дозволяє в рамках традиційно існуючих інформаційних потоків або інформаційного середовища вирішувати деякі важливі завдання захисту інформації ряду прикладних областей.

Основним визначальним моментом в стеганографії є стеганографічні перетворення. До недавнього часу стеганографія, як наука, в основному вивчала окремі методи приховування інформації і способи їх технічної реалізації. Різноманітність принципів, закладених в стеганографічних методах, по суті гальмувало розвиток стеганографії як окремої наукової дисципліни і не дозволило їй сформуватися в вигляді деякої науки зі своїми теоретичними положеннями і єдиною концептуальною системою, яка забезпечила б формальне отримання якісних і кількісних оцінок стеганометодів. У цьому історія розвитку стеганографії різко відрізняється від розвитку криптографії.

До кінця XIX століття стеганографія та криптографія розвивалися в рамках єдиної науки про тайнопис. Після формулювання голландським офіцером Кірхгоффсом (A. Kerckhoffs) знаменитого правила про те, що стійкість криптографічного алгоритму повинна визначається виключно стійкістю ключа, криптографія як окрема наука відокремилась від стеганографії. За останні десятиліття криптологія з сукупності спеціальних методів перетворилася на наукомістку дисципліну, основану на фундаментальних дослідженнях з теорії ймовірності, математичної статистики, чисел, алгебраїчних полів, що дозволило їй вирішити ряд важливих для практичного застосування завдань. Наприклад, визначення стійкості зашифрованих повідомлень по відношенню до можливих засобів криптоаналізу, а також цілий ряд інших завдань, вирішення яких дозволяє отримувати досить чіткі кількісні характеристики засобів криптографічного захисту інформації.

В основі багатьох підходів до вирішення завдань стеганографії лежить спільна з криптографією методична база, закладена Шенноном (CE Shannon) в теорії тайнопису. Проте до цих пір теоретичні основи стеганографії залишаються практично неопрацьованими.

Спостережуваний в даний час інтерес до стеганографії, як сукупності методів приховування інформації, виник у великій мірі завдяки інтенсивному впровадженню і широкому розповсюдженню засобів обчислювальної техніки в усі сфери діяльності людини. У рамках обчислювальних мереж виникли досить широкі можливості по оперативному обміну різною інформацією у вигляді текстів, програм, звуку, зображень між будь-якими учасниками мережевих сеансів незалежно від їхнього територіального розміщення. Це дозволяє активно застосовувати всі переваги, які дають стеганографічні методи захисту.

Стеганографічні методи знаходять все більше застосування в оборонній та комерційній сферах діяльності в силу їхньої легкої адаптованості при вирішенні завдань захисту інформації, а також відсутності явно виражених ознак засобів захисту, використання яких може бути обмежено або заборонено (як, наприклад, криптографічних засобів захисту).

Сьогодні стеганографічні технології активно використовуються для вирішення наступних основних завдань:

* захисту інформації з обмеженим доступом від несанкціонованого доступу;
* захисту авторських прав на деякі види інтелектуальної власності;
* подолання систем моніторингу та управління мережевими ресурсами;
* камуфляжу програмного забезпечення;
* створення прихованих каналів витоку чутливої інформації від законного користувача.

Використання стеганографічних систем є найбільш ефективною при вирішенні проблеми захисту інформації з обмеженим доступом. Так, наприклад, тільки одна секунда оцифрованого звуку з частотою дискретизації 44100 Гц і рівнем відліку 8 біт в стереорежимі дозволяє приховати за рахунок заміни молодших розрядів на приховуване повідомлення близько 10 Кбайт інформації. При цьому зміна значень відліків становить менше 1%. Така зміна практично не виявляється при прослуховуванні файлу більшістю людей.

Крім прихованої передачі повідомлень, стеганографія є одним із самих перспективних напрямків для аутентифікації і маркування авторської продукції з метою захисту авторських прав на цифрові об'єкти від піратського копіювання. На комп'ютерні графічні зображення, аудіо продукцію, літературні твори (програми в тому числі) наноситься спеціальна позначка, яка залишається невидимою для очей, але розпізнається спеціальним програмним забезпеченням. Мітка містить приховану інформацію, що підтверджує авторство. Прихована інформація покликана забезпечити захист інтелектуальної власності. Як впроваджуваної інформації можна використовувати дані про автора, дату і місце народження твору, номери документів, що підтверджують авторство, дату пріоритету і т.п. Такі спеціальні відомості можуть розглядатися в якості доказів при розгляді спорів про авторство або для доказу нелегального копіювання.

## 1.4. Критерії вибору стеганосистеми

Оскільки стеганографія займає свою нішу в забезпеченні безпеки, вона потребує уваги та систематизації існуючих досягнень. Приховування повідомлення методами стеганографії значно знижує ймовірність виявлення самого факту передачі повідомлення. А якщо це повідомлення до того ж зашифровано, то воно має ще один, додатковий, рівень захисту.

В даний час у зв'язку з бурхливим розвитком обчислювальної техніки і нових каналів передачі інформації з'явилися нові стеганографічні методи, в основі яких лежать особливості подання інформації в комп'ютерних файлах, обчислювальних мережах і т.п. Це дає нам можливість говорити про необхідність більш ретельного вивчення напрямку - комп'ютерної стеганографії.

Основним визначальним моментом в стеганографії є стеганографічне перетворення. До недавнього часу стеганографія, як наука, в основному вивчала окремі методи приховування інформації і способи їх технічної реалізації. Різноманітність принципів, закладених в стеганографічних методах, по суті гальмувало розвиток стеганографії як окремої наукової дисципліни і не дозволило їй сформуватися у вигляді деякої науки зі своїми теоретичними положеннями і єдиною концептуальною системою, яка забезпечила б формальне отримання якісних і кількісних оцінок стеганометодів.

Сучасний інтерес до стеганографії, як сукупності методів приховування інформації, виник у великій мірі завдяки інтенсивному впровадженню і широкому розповсюдженню засобів обчислювальної техніки в усі сфери діяльності людини. У рамках обчислювальних мереж виникли досить широкі можливості з оперативного обміну різною інформацією у вигляді текстів, програм, звука, зображень між будь-якими учасниками мережевих сеансів незалежно від їх територіального розміщення. Це дозволяє активно застосовувати всі переваги, які дають стеганографічні методи захисту.

Стеганографічні методи знаходять все більше застосування в оборонній та комерційній сферах діяльності в силу їхньої легкої адаптованості при вирішенні завдань захисту інформації, а також відсутності явно виражених ознак засобів захисту, використання яких може бути обмежено або заборонено (як, наприклад, криптографічних засобів захисту).

Проаналізувавши існуючі на даному етапі методи прихованої передачі інформації можна запропонувати новий підхід для класифікації методів комп’ютерної стеганографії. Доповнивши та скомпонувавши всі методи розглянуті вище, можна згрупувати їх за ознаками: вибір контейнера, призначення, наявність ключа, а також спосіб приховування даних. Схематично це матиме такий вигляд:



Рис.1.2. Авторський спосіб класифікації стеганографічних методів

А тепер більш детальніше зупинимося на кожній з ознак. Вибір контейнера можна розділила за п’ятьма напрямами:

* по формату:
  1. спеціальне форматування текстових файлів;
  2. використання зарезервованих для розширення полів комп’ютерних форматів даних;
  3. використання надлишковості аудіо та візуальної інформації.

Серед властивостей звукових даних, що впливають на забезпечення приховування конфіденційної інформації і, відповідно, на забезпечення її безпеки методами з використанням шумових біт, можна виділити наступні:

* + - неоднорідність послідовностей відліків;
    - наявність певних залежностей між бітами в відліках;
    - наявність певних залежностей між самими відліками;
    - різна ймовірність умовних розподілів в послідовності відліків;
    - наявність довгих серій однакових біт;

Про наявність кореляції між НЗБ і старшими бітами. Ці властивості в різною мірою спостерігаються у більшості звукових файлів і можуть бути використані при побудові різних статистичних критеріїв, визначальним є факт приховування інформації в молодших значущих розрядах. Ось чому подібні методи комп'ютерної стеганографії стали застосовуватися на практиці все рідше. У той же час, прогрес, досягнутий в області розробки пристроїв передачі мовних сигналів з використанням засобів обчислювальної техніки, відкриває нові можливості для прихованої передачі конфіденційної інформації в аналогових і цифрових аудиосигналах і мові на основі використання динамічно розвиваючихся технологій мультимедіа, комп'ютерної та стільникової телефонії.

При використанні надлишковості візуальної інформації в основному мають справу з кольоровими матрицями. Розглядають будь-яке зображення як масив пікселів, які мають глибину кольору 24 біти, по 8 бітів на кожен кольоровий канал RGB.

* + - за способом вилучення інформації:
      1. з оригіналом;
      2. без оригіналу;
      3. по фрагменту оригіналу.
* за розміром контейнери бувають:
  1. потоковими – до них відносяться контейнери, розмір який наперед невідомий і може змінюватись під час приховування інформації.
  2. фіксованими – до них належать контейнери розмір яких наперед відомий і незмінний.

Оскільки контейнер відомий заздалегідь, є час оцінити його ефективність стосовно до обраного алгоритму приховування інформації. З іншого боку, контейнери фіксованої довжини мають обмежений обсяг і іноді вбудоване повідомлення може не поміститися у файл-контейнер.

Інший недолік полягає в тому, що відстані між приховують бітами рівномірно розподілені між найбільш коротким і найдовшим заданими відстанями, в той час як справжній випадковий шум буде мати експоненційний розподіл довжин інтервалу. Звичайно, можна згенерувати псевдовипадкові експоненціально розподілені числа, але цей шлях зазвичай занадто трудомісткий.

Однак на практиці частіше за все використовуються саме контейнери фіксованої довжини, як найбільш поширені і доступні.

* по способу вибору контейнера:
  1. В сурогатних методах стеганографії повністю відсутня можливість вибору контейнера і для приховування повідомлення вибирається перший ліпший контейнер;
  2. В селективних методах КС передбачується, що приховане повідомлення повинне відображати спеціальні статистичні характеристики шуму контейнера. Для цього генерують велику кількість альтернативних контейнерів з послідуючим вибором найбільш оптимального з них для конкретного повідомлення;
  3. В конструюючих методах стеганографії контейнер генерується самою стеганосистемою;
* по способу організації контейнери, подібно завадостійким кодам, можуть бути
  1. систематичними, в яких можна вказати конкретні місця стеганограми, де знаходяться інформаційні біти контейнера, а де шумові біти, призначені для приховування інформації.
  2. несистематичні, в яких все навпаки.

За наявністю ключа стеганосистеми поділяються на:

* ключові;
* без ключові;
* змішані.

Для функціонування безключових стеганосистем, крім алгоритму стеганографічного перетворення, немає необхідності в додаткових даних, на подобі стеганоключа.

Ключові стеганосистеми поділяються на системи з секретним та відкритим ключами. Для систем з наявністю секретного ключа необхідна наявність безпечного (захищеного) каналу обміну стеганоключами. Стеганографічні системи з відкритим ключем не мають необхідності в додатковому каналі ключового обміну. Для їх функціонування необхідно мати два стеганоключа: один секретний, який необхідно тримати в таємниці, а інший – відкритий, який може зберігатися в доступному для всіх місці.

На практиці перевага надається без ключовим стеганосистемам, хоча останні можуть бути розкриті в тому випадку, якщо порушник дізнається про метод стеганоперетворення, який при цьому був використаний. У зв’язку з цим в безключових системах часто використовують особливості криптографічних систем з відкритим і/або секретним ключем.

За призначенням стеганографічні методи можна розділити на такі області використаня:

* захист від копіювання (електронна комерція, контроль за тиражуванням (DVD), розповсюдження мультимедійної інформації…);
* прихована анотація документів (медичні знімки, картографія, мультимедійні бази даних…);
* аутентифікація (системи відео спостереження, електронної комерції, голосової пошти, електронне конфіденційне діловедення…);
* прихований зв'язок (використання в воєнних розвідувальних цілях, а також у тих випадках, коли використовувати криптографію заборонено…).

Використання стеганографічних систем є найбільш ефективною при вирішенні проблеми захисту інформації з обмеженим доступом. Так, наприклад, тільки одна секунда оцифрованого звуку з частотою дискретизації 44100 Гц і рівнем відліку 8 біт в стереорежимі дозволяє приховати за рахунок заміни молодших розрядів на приховуване повідомлення близько 10 Кбайт інформації. При цьому зміна значень відліків становить менше 1%. Така зміна практично не виявляється при прослуховування файлу більшістю людей.

Крім прихованої передачі повідомлень, стеганографія є одним з найбільш перспективних напрямів для аутентифікації і маркування авторської продукції з метою захисту авторських прав на цифрові об'єкти від піратського копіювання. На комп’ютерні графічні зображення, аудіо продукцію, літературні твори (програми в тому числі) наноситься спеціальна позначка, яка залишається невидимою для очей, але розпізнається спеціальним програмним забезпеченням. Мітка містить приховану інформацію, що підтверджує авторство. Прихована інформація покликана забезпечити захист інтелектуальної власності. В якості прихованої інформації можна використовувати дані про автора, дату і місце народження твору, номера документів, що підтверджують авторство, дату пріоритету і т.п. Такі спеціальні відомості можуть розглядатися в якості доказів при розгляді суперечок про авторство або для доказу нелегального копіювання.

Як і будь-які інші інструменти, стеганографічні методи вимагають до себе бережного ставлення, так як вони можуть бути використані як з метою захисту, так і в протиправних цілях.

Наприклад, наприкінці 2001 року під пильною увагою преси виявилися відомості про те, що один з найнебезпечніших терористів світу Осам Бен Ладен і члени його угруповання широко використовують Інтернет для передачі повідомлень по організації терористичних акцій. Уряди деяких країн роблять кроки з метою приборкання такої загрози, намагаючись ввести обмеження на поширення програм, пов'язаних з криптографічними і стеганографічними методами. Однак стеганографічні методи успішно застосовуються для протидії системам моніторинрингу та управління мережевими ресурсами промислового шпигунства. З їх допомогою можна протистояти спробам контролю над інформаційним простором при проходженні інформації через сервери управління локальних або глобальних обчислювальних мереж.

Нерідко методи стеганографії використовують для камуфляжу програмного забезпечення. У тих випадках, коли використання програм незареєстрованими користувачами є небажаним, воно може бути закамуфльоване під стантартні універсальні програмні продукти (наприклад, текстові редактори) або приховане у файлах мультимедіа (наприклад, у звуковому супроводі комп'ютерних ігор).

І, нарешті, стеганографічний підхід використовується при створенні прихованого каналу витоку чутливої інформації від санкціонованих користувачів.

По принципу приховування методи комп’ютерної стеганографії діляться на два основні класи: безпосередньої заміни і спектральні методи. Якщо перша, використовуючи надлишок інформаційного середовища в просторовій або часовій області, заключається в заміні малозначущої частини контейнера бітами секретного повідомлення, то інші для приховування даних використовують спектральне представлення елементів середовища, в яке вбудовують приховувані дані.

За стійкістю можна виділити робастні, крихкі та напівкрихкі стегосистеми. Пояснити таку класифікацію можна за допомогою цифрових водяних знаків.

Під робастністю розуміється стійкість ЦВЗ до різного роду впливів на стего. Робастності ЦВЗ присвячено більшість досліджень.

Крихкі ЦВЗ руйнуються при незначній модифікації заповненого контейнера. Вони використовуються для підтвердження сигналів. Відмінність від засобів електронного цифрового підпису полягає в тому, що крихкі ЦВЗ все ж допускають деяку модифікацію контенту. Це важливо для захисту мультимедійної інформації, так як законний користувач може, наприклад, побажати стиснути зображення. Інша відмінність полягає в тому, що крихкі ЦВЗ повинні не тільки відобразити факт модифікації контейнера, але також вид і місце розташування цієї зміни.

Напівкрихкі ЦВЗ стійкі по відношенню до одних дій і нестійкі по відношенню до інших. Майже всі ЦВЗ можуть бути віднесені до цього типу. Однак напівкрихкі ЦВЗ спеціально проектуються так, щоб бути нестійкими по відношенню до певного роду операцій.

Така класифікація найбільш широко відображає систему методів прихованої передачі інформації. Можливо хтось заперечить такий підхід і висловить своє заперечення такому підходу, адже в приведеній класифікації включається також класифікація стеганографічних систем, що є дещо суперечливим фактом. Проте це використано з такої точки зору, що будь-який стеганографічний метод направлений на створення системи прихованої передачі інформації. Тому буде неправильно розглядати початковий етап – вибір контейнера під час класифікації даних методів, а водночас не надавати значення уже готовому продукту – стеганографічній системі.

Цей спосіб класифікації не вказує на самі методи, тут немає жодної конкретної назви того чи іншого методу, проте тут відображені всі основні властивості, які необхідно враховувати при вирішенні тієї чи іншої задачі. Також з подальшим розвитком комп’ютерних технологій дану структуру можна доповнювати та розширювати відповідно до вимог, які необхідно забезпечити.

Тепер розглянемо критерії, що стосуються стеганографічного алгоритму (способу вбудовування секретних даних у контейнер) [21].

Робастність – стійкість стеганографічного контейнера до зовнішнього впливу (тобто збереження стегоданих після модифікації стегоконтейнера). Цей критерій є критичним для захисту авторства за допомогою ЦВЗ, оскільки зловмисники намагатимуться знищити вбудовані ЦВЗ, виконавши певні перетворення над контейнером.

Таємність – стійкість до виявлення стегоданих та їх видобування зі стегоконтейнера. Цей критерій є критичним для прихованої комунікації. Виконаємо декомпозицію критерію таємності:

1. стійкість до виявленняфакту існування стегоданих – залежить від того, чи змінюються певні характеристики контейнера після вбудовування у нього стегоданих:
   * властивості контейнера (наприклад, розмір);
   * аудіовізуальні характеристики контейнера (після вбудовування стегоданих можлива втрата якості зображення, підвищення кількості шумів тощо);
   * структура, ключові елементи та статистичні характеристики контейнера (зміни цих характеристик часто неочевидні, але їх можна виявити, виконавши аналіз стегаконтейнера за допомогою спеціальних засобів);
2. стійкість до отримання стеганоданих:

* шифрування стеганоданих (під час попереднього шифрування даних, якщо зловмиснику вдасться видобути стегодані, він не зможе розшифрувати їх через відсутність у нього секретного ключа);
* складність розподілу стеганоданих у контейнері.

Ємність – максимальна кількість інформації, яка може бути вбудована в контейнер певного розміру. Зазвичай ємність контейнера визначають з урахуванням обмежень таємності та робастності. Існує два альтернативні визначення поняття стеганографічної ємності.

Зазначимо, що, залежно від шкали, оцінки бувають: а) бінарними(оцінюють значеннями «є» і «немає», залежно від того, чи притаманний об’єкт критерію стеганографічному засобу, чи ні); б)градуйованими(оцінка може набувати певного числового значення у визначеному діапазоні).

Критерії, що стосуються контейнерів і стегоданих, оцінюють бінарними оцінками, алгоритму – переважно градуйованими. Формування єдиної градуйованої шкали оцінювання цих критеріїв виходить за межі цієї роботи.

## 1.5. Висновки по розділу

В даному розділі дипломної роботи був проаналізований сучасний стан інформаційної безпеки нашої держави та місце стеганографії серед сучасних методів захисту.

Визначено, що рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, бо найчастіше реалізація інформаційних загроз - це нанесення шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо.

На сучасному етапі в Україні немає реальних гарантів інформаційної безпеки країни, відсутній комплекс нормативно-правових актів щодо захисту інформаційних ресурсів та інформаційної інфраструктури. Процес інформатизації має стихійний, некерований характер, з переважним ухилом у бік використання засобів інформатизації іноземного виробництва.

В розділі зазначено, що використання стеганографічних методів дозволяє створити додатковий рівень захисту, а для вибору параметрів стеганографічної системи необхідний комплексний підхід, що дозволить застосовувати такий вид захисту найбільш оптимально та ефективно.

# РОЗДІЛ 2

## Інтегровані стеганографічні методи

## 2.1. Руйнівні програмні коди серед загроз інформаційній безпеці

Під загрозою безпеці інформації розуміються події або дії, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів.

Якщо виходити з класичного розгляду кібернетичної моделі будь-керованої системи, впливи на неї можуть носити випадковий характер. Тому серед загроз безпеці інформації слід виділяти як один з видів загрози випадкові, чи ненавмисні. Їх джерелом можуть бути вихід з ладу апаратних засобів, неправильні дії працівників ІС або її користувачів, ненавмисні помилки в програмному забезпеченні і т.д. Такі загрози теж слід тримати на увазі, так як збиток від них може бути значним.

Розрізняють такі види навмисних загроз:

Пасивні загрози спрямовані в основному на несанкціоноване використання інформаційних ресурсів ІС, не здійснюючи при цьому впливу на її функціонування. Наприклад, несанкціонований доступ до баз даних, прослуховування каналів зв'язку і т.д.

Активні загрози мають на меті порушення нормального функціонування ІС шляхом цілеспрямованого впливу на її компоненти. До активних загроз відносяться, наприклад, виведення з ладу комп'ютера чи його операційної системи, спотворення відомостей в БД, руйнування ПЗ комп'ютерів, порушення роботи ліній зв'язку і т.д. Джерелом активних загроз можуть бути дії зломщиків, шкідливі програми і т.п.

Умисні загрози поділяються також на внутрішні (що виникають всередині керованої організації) і зовнішні.

Внутрішні загрози найчастіше визначаються соціальною напруженістю і важким моральним кліматом.

Зовнішні загрози можуть визначатися зловмисними діями конкурентів, економічними умовами та іншими причинами (наприклад, стихійними лихами). За даними зарубіжних джерел, отримало широке поширення промислове шпигунство - що завдає шкоди власнику комерційної таємниці незаконні збір, привласнення і передача відомостей, що становлять комерційну таємницю, не уповноваженою на це особою.

Загрози безпеці інформації та програмного забезпечення КС виникають як у процесі їх експлуатації, так і при створенні цих систем, що особливо характерно для процесу розробки ПЗ, баз даних та інших інформаційних компонентів КС.

При вирішенні проблеми підвищення рівня захищеності інформаційних ресурсів КС необхідно виходити з того, що найбільш імовірним інформаційним об'єктом впливу буде виступати програмне забезпечення, яке складає основу комплексу засобів отримання, семантичної переробки, розподілу та зберігання даних, використовуваних при експлуатації критичних систем.

В даний час одним з найбільш небезпечних засобів інформаційного впливу на комп'ютерні системи є програми - віруси чи комп'ютерні віруси.

Під комп'ютерним вірусом слід розуміти програми, здатні розмножуватися, прикріплятися до інших програм, передаватися по телекомунікаційних каналах. В якості основних засобів зловмисних (деструктивного) впливу на КС необхідно, поряд з комп'ютерними вірусами, розглядати алгоритмічні та програмні закладки.

Під алгоритмічної закладкою будемо розуміти умисне завуальоване спотворення будь-якої частини алгоритму розв'язання задачі, або побудова його таким чином, що в результаті кінцевої програмної реалізації цього алгоритму в складі програмного компонента або комплексу програм, останні будуть мати обмеження на виконання необхідних функцій, заданих специфікацією, або зовсім їх не виконувати за певних умов протікання обчислювального процесу, що задається семантикою оброблюваних програмою даних. Крім того, можлива поява у програмного компонента функцій, не передбачених прямо або побічно специфікацією, і які можуть бути виконані при строго визначених умовах протікання обчислювального процесу.

Під програмною закладкою будемо розуміти сукупність операторів і (або) операндів, навмисно в завуальованій формі включається до складу виконуваного коду програмного компонента на будь-якому етапі його розробки. Програмна закладка реалізує певний несанкціонований алгоритм з метою обмеження або блокування виконання програмним компонентом необхідних функцій за певних умов протікання обчислювального процесу, що задається семантикою оброблюваних програмним компонентом даних, або з метою постачання програмного компонента не передбаченими специфікацією функціями, які можуть бути виконані при строго визначених умовах протікання обчислювального процесу.

Дії алгоритмічних і програмних закладок умовно можна розділити на три класи: зміна функціонування обчислювальної системи (мережі), несанкціоноване зчитування інформації і несанкціонована модифікація інформації, аж до її знищення. В останньому випадку під інформацією розуміються як дані, так і коди програм. Слід зазначити, що вказані класи впливів можуть перетинатися.

У першому класі впливів виділимо наступні:

* зменшення швидкості роботи обчислювальної системи (мережі);
* часткове або повне блокування роботи системи (мережі);
* імітація фізичних (апаратурних) збоїв роботи обчислювальних засобів і периферійних пристроїв;
* переадресація повідомлень;
* обхід програмно-апаратних засобів криптографічного перетворення інформації;
* забезпечення доступу в систему з непередбачених периферійних пристроїв.

Несанкціоноване зчитування інформації, здійснюване в автоматизованих системах, направлено на:

* зчитування паролів і їх ототожнення з конкретними користувачами;
* отримання секретної інформації;
* ідентифікацію інформації, запитуваної користувачами;
* підміну паролів з метою доступу до інформації;
* контроль активності абонентів мережі для отримання непрямої інформації про взаємодію користувачів і характер інформації, якою обмінюються абоненти мережі.

Несанкціонована модифікація інформації є найбільш небезпечним різновидом впливів програмних закладок, оскільки призводить до найбільш небезпечних наслідків. У цьому класі впливів можна виділити наступні:

* руйнування даних, і кодів виконуваних програм внесення тонких, важко виявляються змін в інформаційні масиви;
* впровадження програмних закладок в інші програми і підпрограми (вірусний механізм впливів);
* спотворення або знищення власної інформації сервера і тим самим порушення роботи мережі;
* модифікація пакетів повідомлень.

З викладеного випливає висновок про те, що алгоритмічні і програмні закладки мають широкий спектр впливів на інформацію, оброблювану обчислювальними засобами в КС.

Отже, при контролі технологічної безпеки програмного забезпечення необхідно враховувати його призначення і склад апаратних засобів та загальносистемного програмного забезпечення програмно-апаратне середовище) КС.

З точки зору часу внесення програмних закладок у програми можна розділити на дві категорії: апріорні та апостеріорнi, тобто закладки, внесені при розробці ПЗ (або «вроджені») і закладки, внесені при випробуваннях, експлуатації або модернізації ПЗ (або «придбані») відповідно. Хоча останній різновид закладок і відноситься більше до проблеми забезпечення експлуатаційної, а не технологічної безпеки ПЗ, проте методи тестування програмних комплексів, імовірнісні методи розрахунку наявності програмних дефектів і методи оцінювання рівня безпеки ПЗ можуть значною мірою перетинатися і доповнювати один одного. Тим більше що дія програмної закладки після того як вона була внесена в ПЗ або на етапі розробки, або на наступних етапах життєвого циклу ПЗ, практично не буде нічим не відрізнятися.

Таким чином, розглянуті програмні засоби деструктивного впливу за своєю природою носять, як правило, руйнівний, шкідливий характер, а наслідки їх активізації та застосування можуть призвести до значного або навіть непоправного збитку в тих областях людської діяльності, де застосування комп'ютерних систем є життєво необхідним. У зв'язку з цим такі шкідливі програми будемо називати руйнують програмними засобами (РПЗ), а їх узагальнена класифікація може виглядати наступним чином:

* комп'ютерні віруси - програми, здатні розмножуватися, прикріплятися до інших програм, передаватися по лініях зв'язку і мереж передачі даних, проникати в електронні телефонні станції та системи управління і виводити їх з ладу;
* програмні закладки - програмні компоненти, заздалегідь впроваджувані в комп'ютерні системи, які за сигналом або у встановлений час приводяться в дію, знищуючи або спотворюючи інформацію, або дезорганізуючи роботу програмно-технічних засобів;
* способи і засоби, що дозволяють впроваджувати комп'ютерні віруси та програмні закладки в комп'ютерні системи і керувати ними на відстані [7].

### 2.1.1. Віруси як різновид руйнівних програмних кодів

Шкідливі програми класифікуються наступним чином: Логічні бомби, як випливає з назви, використовуються для спотворення або знищення інформації, рідше з їх допомогою відбуваються крадіжка чи шахрайство. Маніпуляціями з логічними бомбами зазвичай займаються чимось незадоволені службовці, які збираються покинути цю організацію, але це можуть бути і консультанти, службовці з певними політичними переконаннями і т.п. [20]

Реальний приклад логічної бомби: програміст, передбачаючи своє звільнення, вносить до програми розрахунку заробітної плати певні зміни, які починають діяти, коли його прізвище зникне з набору даних про персонал фірми.

Троянський кінь - програма, що виконує на додаток до основних, тобто запроектованих і документованих дій, дії додаткові, не описані в документації. Аналогія з давньогрецьким троянським конем виправдана - і в тому і в іншому випадку не викликає підозри, що оболонці таїться загроза. Троянський кінь являє собою додатковий блок команд, тим чи іншим чином вставлений у вихідну нешкідливу програму, яка потім передається (дарується, продається, підміняється) користувачам ІС. Цей блок команд може спрацьовувати при настанні деякої умови (дати, часу, по команді ззовні і так далі). Запуск такої програми наражає на небезпеку як особисті файли, так і всю ІС в цілому. Троянський кінь діє здебільшого в межах повноважень одного користувача, але в інтересах іншого користувача або взагалі сторонньої людини, особу якого встановити часом неможливо. Найбільш небезпечні дії троянський кінь може виконувати, якщо запустивший його користувач володіє розширеним набором привілеїв. У такому випадку зловмисник, що склав і впровадив троянського коня, і сам цими привілеями не володіє, може виконувати несанкціоновані привілейовані функції чужими руками.

Вірус - програма, яка може заражати інші програми шляхом включення в них модифікованої копії, що володіє здатністю до подальшого розмноження.

Вважається, що вірус характеризується двома основними особливостями:

1) здатністю до саморозмноження;

2) здатністю до втручання в обчислювальний процес (тобто до отримання можливості управління).

Наявність цих властивостей, як бачимо, є аналогом паразитування в живій природі, яке властиво біологічним вірусам. В останні роки проблема боротьби з вірусами стала досить актуальною, тому дуже багато хто займається нею. Використовуються різні організаційні заходи, нові антивірусні програми, ведеться пропаганда всіх цих заходів. Останнім часом вдавалося більш-менш обмежити масштаби заражень і руйнувань. Однак, як і в живій природі, повний успіх у цій боротьбі не досягнутий.

Резидентні віруси. Під терміном "резидентність" (DOS'овскій термін TSR - Terminate and Stay Resident) розуміється спроможність вірусів залишати свої копії в системній пам'яті, перехоплювати деякі події (наприклад, звернення до файлів або дисків) і викликати при цьому процедури зараження виявлених об'єктів (файлів і секторів). Таким чином, резидентні віруси активні не тільки в момент роботи інфікованої програми, але і після того, як програма закінчила свою роботу. Резидентні копії таких вірусів залишаються життєздатними аж до чергового перезавантаження, навіть якщо на диску знищені всі інфіковані файли. Часто від таких вірусів неможливо позбутися відновленням всіх копій файлів з дистрибутивних дисків або backup-копій. Резидентна копія вірусу залишається активною і заражає новостворювані файли. Це властиво і для завантажувальних вірусів - форматування диску при наявності в пам'яті резидентного вірусу не завжди виліковує диск, оскільки резидентні віруси заражають диск повторно після того, як він був відформатований.

Нерезидентні віруси. Нерезидентні віруси, навпаки, активні досить нетривалий час - тільки в момент запуску інфікованої програми. Для свого поширення вони шукають на диску незаражені файли і записуються в них. Після того, як код вірусу передає керування програмі-носію, вплив вірусу на роботу операційної системи зводиться до нуля аж до чергового запуску будь-якої зараженої програми. Тому файли, заражені нерезидентними вірусами значно простіше видалити з диску і при цьому не дозволити вірусу заразити їх повторно.

Стелс-віруси. Стелс-віруси тими або іншими способами приховують факт своєї присутності в системі. Використання СТЕЛС-алгоритмів дозволяє вірусам цілком або частково сховати себе в системі. Найбільш поширеним стелс-алгоритмом є перехоплення запитів OC на читання / запис заражених об'єктів. Стелс-віруси при цьому або тимчасово лікують їх, або «підставляють» замість себе незаражені ділянки інформації. У випадку макро-вірусів найбільш популярний спосіб - заборона викликів меню перегляду макросів. Відомі стелс-віруси всіх типів, за винятком Windows-вірусів - завантажувальні віруси, файлові DOS-віруси і навіть макро-віруси. Поява стелс-вірусів, що заражають файли Windows, є швидше за все справою часу.

Поліморфік-віруси. Самошифрування і поліморфічність використовуються практично всіма типами вірусів для того, щоб максимально ускладнити процедуру детектування вірусу. Поліморфік - віруси (polymorphic) – їх досить важко виявити, адже вони не мають сигнатур, тобто не містять жодної постійної ділянки коду. У більшості випадків два зразки того самого поліморфік-вірусу не будуть мати жодного збігу. Це досягається шифруванням основного тіла вірусу і модифікаціями програми-розшифровувача. До поліморфік-вірусів відносяться ті з них, детектування яких неможливо (або вкрай важко) здійснити за допомогою так званих вірусних масок - ділянок постійного коду, специфічних для конкретного вірусу. Досягається це двома основними способами - шифруванням основного коду вірусу з непостійним ключем та об’єднанням з набором команд розшифровувача або зміною самого виконуваного коду вірусу. Поліморфізм різного ступеня складності зустрічається у вірусах всіх типів - від завантажувальних і файлових DOS-вірусів до Windows-вірусів.

Черв’як - програма, що поширюється через мережу і не залишає своєї копії на магнітному носії. Черв'як використовує механізми підтримки мережі для визначення вузла, який може бути заражений. Зате з допомогою тих же механізмів передає своє тіло або його частину на цей вузол і або активізується, або чекає для цього відповідних умов. Найбільш відомий представник цього класу - вірус Морріса (черв’як Морріса), що вразив мережу Internet в 1988 р. В якості середовища поширення черв’яка є мережа, всі користувачі якої вважаються дружніми і довіряють один одному, а захисні механізми відсутні. Найкращий спосіб захисту від черв’яка - прийняття запобіжних заходів проти несанкціонованого доступу до мережі.

Загарбник паролів - це програми, спеціально призначені для крадіжки паролів. При спробі звернення користувача до терміналу системи на екран виводиться інформація, необхідна для закінчення сеансу роботи. Намагаючись організувати вхід, користувач вводить ім'я і пароль, які пересилаються власнику програми-загарбника, після чого виводиться повідомлення про помилку, а введення і керування повертаються до операційної системи. Користувач, який думає, що допустив помилку при наборі пароля, повторює вхід і отримує доступ до системи. Однак його ім'я і пароль вже відомі власнику програми-загарбника. Перехоплення пароля можливе і іншими способами. Для запобігання цієї загрози перед входом в систему необхідно переконатися, що ви вводите ім'я та пароль саме системній програмі введення, а не якій-небудь іншій. Крім того, необхідно неухильно дотримуватися правил використання паролів і роботи з системою. Більшість порушень відбувається не через хитромудрі атаки, а через елементарну недбалість. Дотримання спеціально розроблених правил використання паролів - необхідна умова надійного захисту [11, 22].

### 2.1.2. Програмні закладки

До руйнівних програмних кодів також відносять програмні закладки. Програмними закладками називаються своєрідні програми, що використовують вірусну технологію прихованого впровадження, поширення та активізації Однак, на відміну від вірусів, які просто знищують інформацію, програмні закладки, перш за все, призначені для її несанкціонованого прихованого отримання. Типова програмна закладка може, наприклад, зберігати введення з клавіатури інформації (в тому числі і паролі) у кількох зарезервованих для цього секторах, а потім пересилати накопичені дані по мережі на комп'ютер зловмисника.

Програмні закладки можна класифікувати за методом і місцем їх впровадження та застосування (тобто за способом впровадження в систему).

1. Дані, асоційовані з програмно-апаратним середовищем.
2. Дані, асоційовані з програмами первинного завантаження.
3. Дані, асоційовані із завантаженням драйверів, командного інтерпретатора, мережевих драйверів, тобто із завантаженням операційного середовища.
4. Дані, асоційовані з прикладним програмним забезпеченням загального призначення (вбудовані клавіатурні та екранні драйвери, програми тестування ПЕОМ, утиліти і оболонки).
5. Використовувані модулі, що містять тільки код закладки (як правило, впроваджувані в пакетні файли типу BAT).
6. Модулі-імітатори, що збігаються з деякими програмами, що вимагають введення конфіденційної інформації (за зовнішнім виглядом).
7. Дані, що маскуються під програмні засоби оптимізаційного призначення (архіватори, прискорювачі і т.д.).
8. Дані, що маскуються під програмні засоби ігрового і розважального призначення (як правило, використовуються для первинного впровадження закладок типу "дослідник").

Для того щоб закладення змогла виконати будь-які функції, вона повинна отримати управління, тобто процесор повинен почати виконувати інструкції (команди), що відносяться до коду закладки. Це можливо тільки при одночасному виконанні двох умов:

* + закладка повинна знаходитися в оперативній пам'яті до початку роботи програми, яка є метою впливу закладки, отже, вона повинна бути завантажена раніше або одночасно з цією програмою;
  + закладка повинна активізуватися по деякому загальному, як для закладання, так і для програми, події, тобто при виконанні ряду умов в апаратно-програмному середовищі управління повинно бути передано на програму-закладку.

Це досягається шляхом аналізу й обробки закладкою загальних для закладення і прикладної програми дій (як правило, переривань). Причому вибираються переривання, які напевно використовуються прикладною програмою або операційною системою. В якості таких переривань можна виділити:

* переривання від системного таймера;
* переривання від зовнішніх пристроїв;
* переривання від клавіатури;
* переривання при роботі з диском;
* переривання операційного середовища (у тому числі переривання для роботи з файлами і запуску виконуваних модулів).

В іншому разі активізації коду закладки не відбудеться, і він не зможе здійснити будь-якого впливу на роботу програми ЗІ.

Крім того, можливі випадки, коли при запуску програми (у цьому випадку активуючою подією є запуск програми) закладка руйнує деяку частину коду програми, вже завантаженої в оперативну пам'ять, і, можливо, систему контролю цілісності коду або контролю інших подій і на цьому закінчує свою роботу.

Таким чином, можна виділити наступні типи закладок.

1) Резидентні - знаходиться в пам'яті постійно з деякого моменту часу до закінчення сеансу роботи ПЕОМ (виключення живлення або перевантаження).

Закладка може бути завантажена в пам'ять при початковому завантаженні ПЕОМ, завантаженні операційної середовища або запуску деякої програми (яка за традицією називається вірусоносієм), а також запущена окремо.

2) Нерезидентна - починає роботу з аналогічної події, але закінчують її самостійно по закінченню деякого проміжку часу або деякої події, при цьому вивантажуючи себе з пам'яті повністю. Несанкціонований запис закладкою може відбуватися:

* в масив даних, який не збігається з користувацькою інформацією (розкрадання інформації);
* в масив даних, що співпадає з користувацької інформацією та її підмножини (спотворення, знищення або нав'язування інформації закладкою).

Отже, можна розглядати три основні групи деструктивних функцій, які можуть виконуватися закладками:

* збереження фрагментів інформації, що виникає при роботі користувача, прикладних програм, введенні / виводі даних, на локальному або мережевому диску;
* руйнування функцій самоконтролю або зміна алгоритмів функціонування прикладних програм;
* нав'язування деякого режиму роботи (наприклад, при знищенні інформації
* - блокування запису на диск без знищення інформації), або нав'язування сторонньої інформації замість корисної інформації при записі останньої на диск [23].

## 2.2. Використання стеганографічних методів для реалізації загроз інформаційній безпеці

Комп'ютерна стеганографія це частина стеганографії, яка займається питаннями реалізації стегосистем з використанням комп'ютерної техніки.

Оскільки цифрова інформація звичайно передається у вигляді файлів, то в комп'ютерній стегосистемі використовуються поняття файл-контейнер і файл-повідомлення. Для того, щоб сторонні не запідозрили факт передачі повідомлення, файл-повідомлення особливим чином (за допомогою стегоключа) "змішують" з файлом-контейнером. При цьому, як і прийнято в "класичній" стеганографії, файл-контейнер має виглядати цілком безневинно, а підмішування секретної інформації не повинно змінювати його основних властивостей.

Стеганографічні методи широко застосовують для вирішення цілої низки корисних завдань захисту інформації, але тим не менш, не дуже складні комп'ютерні стегосистеми вже реально застосовуються зловмисниками (зокрема, "вірусописцями").

Відомий, наприклад, вірус, що має кодову назву "W32/Perrun". Нерезидентний Win32-вірус. Є додатком Windows (PE EXE-файл), має розмір близько 12K (упакований UPX, розмір розпакованого файлу - близько 18K), написаний на Visual Basic.

Основною особливістю вірусу є те, що він поширюється через JPEG-файли (графічні файли, один з найбільш популярних форматів зберігання графічної інформації - фотографій, картинок, і іншого).

При запуску вірус шукає \*. JPG-файли в поточному каталозі і дописує до них свій EXE-код (в результаті JPG-файли ніби складаються з двох частин: верхня частина є звичайними даними в форматі JPEG, нижня частина є Win32 PE EXE-файлом).

Уражені JPG-файли містять рядок "alco" в самому кінці файлу. По цьому рядку вірус визначає вже уражені файли і таким чином уникає повторного дописування до них свого EXE-коду.

Потім вірус зчитує з свого тіла додатковий EXE-файл. Цей файл є компонентою вірусу, розміром 5.6K, також написаний на Visual Basic і упакований UPX. Ця компонента записується в поточний каталог у вигляді файлу "extrk.exe" і реєструється в ключі системного реєстру "jpegfile":

HKCR \ jpegfile \ shell \ open \ command

default =% CurrentDir% \ extrk.exe% 1

У результаті файл-компонента "extrk.exe" асоціюється з JPEG-файлами і запускається на виконання при відкритті кожного JPEG-файлу.

При запуску компоненту вірусу зчитує основний EXE-код вірусу з JPEG-файлу, записує його в поточний каталог з ім'ям X. EXE і запускає на виконання.



Рис.2.1. Схема алгоритму роботи вірусу "W32/Perrun"

Таким чином стартує основний код вірусу, які виконує дії, описані вище. У результаті в зараженій системі вірус здатний поширюватися через JPEG-файли.

Потім вірус намагається відобразити JPEG-зображення з ураженого файлу за допомогою стандартної бібліотеки Windows SHIMGVW.DLL ("Shell Image View Control"). Вірус відкриває цю бібліотеку на ім'я C:\WINDOWS\SYSTEM\SHIMGVW.DLL. Якщо цей файл відсутній, або Windows встановлена в каталозі з іншим ім'ям, то вірус не в змозі відобразити картинку з ураженого JPEG-файлу (при цьому з'являється стандартне повідомлення про помилку) [1].

З точки зору стеганографії (втім, і з точки зору вірусології) це дуже примітивний вірус. Але він показує метод, як впровадити в систему програму - закладку великого обсягу. Потрібно зробити цю програму двокомпонентною. Стартова частина, яка тільки шукає основне тіло програми в інших файлах, може бути дуже маленькою, що полегшує її впровадження. Обсяг же основної частини програми може бути дуже великим, і при цьому ризик її виявлення може бути зведений до мінімуму.

Більш складний механізм маскування реалізований творцем вірусу Win95.CIH.Цей вірус впроваджується в \*. exe файл, використовуючи особливості формату PE (Portable Executable), прийнятого в системі Windows починаючи з Windows 95. У Windows виконуваний файл \*. exe може містити не тільки код, але й численні додаткові дані.

Це піктограми, різні службові дані та додаткова інформація, наприклад, про експортовані та імпортовані функції. Кожен вид даних, що містяться у файлі формату РЕ, це окремий об'єкт. Для зберігання всіх об'єктів файл формату РЕ розбивається на ряд секцій фіксованого розміру. Кожен об'єкт починається з нової секції. Якщо об'єкт не займає всього обсягу секції, то ця частина секції не використовується. Тому у файлі формату РЕ завжди достатньо вільного місця (рис.2.2).

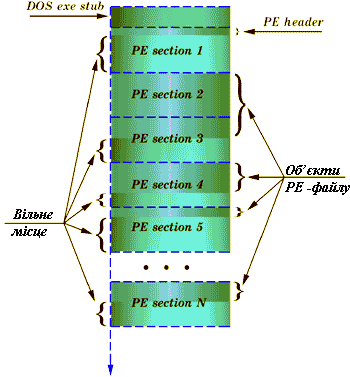


Рис.2.2. Структура РЕ-файлу

Більше всього вільного місця в першій секції, в яку записується тільки заголовок файлу (PE header). У ці вільні місця можна заховати досить багато інформації, і при цьому розмір файлу не зміниться і працездатність файлу не порушиться.

Описані вище приклади показують можливість максимально приховати процес впровадження програми - закладки в комп'ютер. Результат роботи впровадженої програми - це знайдені їй файли. Файли можуть бути різних форматів і іноді дуже великого обсягу. Для їх прихованої передачі застосовуються більш досконалі методи комп'ютерної стеганографії, засновані на надмірності аудіо-, фото-та відеоінформації. Дійсно, молодші цифрові розряди таких файлів містять мало корисної інформації, і їх зміна дуже слабо впливає на якість вихідного файлу. Тому можна використовувати молодші розряди для передачі прихованої інформації без видимого спотворення вихідного файлу. До того ж ці файли самі по собі мають великий обсяг, тому в них легше вбудувати великий обсяг інформації, що приховується [18].

## 2.3. Аналіз сучасних методів стеганоаналізу. Класифікація атак на системи прихованої передачі інформації

Як відомо, порушник може бути пасивним, активним і зловмисним. Залежно від цього він може створювати різні загрози.

Пасивний порушник може лише виявити факт наявності стегоканала і (можливо) читати повідомлення. Чи зможе він прочитати повідомлення після його виявлення залежить від стійкості системи шифрування, і це питання, як правило, не розглядається в стеганографії. Якщо у порушника є можливість виявити факт наявності прихованого каналу передачі повідомлень, то стегосистеми зазвичай вважається нестійкою. Здійснення виявлення стегоканала є найбільш трудомістким завданням, а захист від виявлення вважається основним завданням стеганографії, за визначенням.

Діапазон дій активного порушника значно ширше. Приховане повідомлення може бути їм видалено або зруйновано. У цьому випадку відправник і, можливо, одержувач дізнаються про факт втручання. У більшості випадків це суперечить інтересам порушника (наприклад, з юридичних мотивів). Інша справа - видалення або руйнування цифрового водяного знака, які можуть розглядатися як основні загрози в цій області.

Дії зловмисної порушника найбільш небезпечні. Він здатний не тільки руйнувати, але і створювати помилкові стего. Історія протистояння розвідки і контррозвідки знає чимало прикладів, коли реалізація цієї загрози призводила до катастрофічних наслідків. Ця загроза актуальна і по відношенню до систем ЦВЗ. Маючи здатність створювати водяні знаки, порушник може створювати копії захищеного контенту, створювати помилкові оригінали і т.д. У багатьох випадках порушник може створювати помилкові стего без знання ключа.

Для здійснення тієї чи іншої загрози порушник застосовує атаки.

Найбільш проста атака - суб'єктивна. Порушник уважно розглядає зображення (слухає аудіозапис), намагаючись визначити "на око", чи є в ньому приховане повідомлення. Ясно, що подібна атака може бути проведена лише проти абсолютно незахищених стегосистем. Тим не менш, вона, напевно, найбільш поширена на практиці, принаймні, на початковому етапі розкриття стегосистеми. Первинний аналіз також може включати в себе наступні заходи:

1) Первинне сортування стего за зовнішніми ознаками.

2) Виділення стего з відомим алгоритмом вбудовування.

3) Визначення використаних стегоалгоритмів.

4) Перевірка достатності обсягу матеріалу для стегоаналізу.

5) Перевірка можливості проведення аналізу по окремих випадків.

6) Аналітична розробка стегоматеріалів. Розробка методів розкриття стегосистеми.

7) Виділення стего з відомими алгоритмами вбудовування, але невідомими ключами і т.д.

Нехай ми маємо двох абонентів: Алісу та Боба, а також порушника Віллі. Тоді за аналогією з криптоаналізом в стегоаналізі можна виділити наступні типи атак.

* Атака на основі відомого заповненого контейнера. У цьому випадку у порушника є одне або кілька стего. В останньому випадку передбачається, що вбудовування прихованої інформації здійснювалося Алісою одним і тим же способом. Завдання Віллі може складатися у виявленні факту наявності стегоканала (основна), а також у його добуванні або визначенні ключа. Знаючи ключ, порушник отримає можливість аналізу інших стегоповідомлень.
* Атака на основі відомого вбудованого повідомлення. Цей тип атаки в більшій мірі характерний для систем захисту інтелектуальної власності, коли в якості водяного знака використовується відомий логотип фірми. Завданням аналізу є отримання ключа. Якщо відповідний прихованим повідомленням заповнений контейнер невідомий, то завдання вкрай важко вирішити.
* Атака на основі обраного прихованого повідомлення. У цьому випадку Віллі має можливість пропонувати Алісі для передачі свої повідомлення і аналізувати отримані стего.
* Адаптивна атака на основі обраного прихованого повідомлення. Ця атака є окремим випадком попередньої. У даному випадку Віллі має можливість вибирати повідомлення для нав'язування Алісі адаптивно, в залежності від результатів аналізу попередніх стего.
* Атака на основі обраного заповненого контейнера. Цей тип атаки більше характерний для систем ЦВЗ. Стегоаналітик має детектор стего у вигляді «чорного ящика» і декілька стег. Аналізуючи детектовані приховані повідомлення, порушник намагається розкрити ключ.

У Віллі може бути можливість застосувати ще три атаки, які не мають прямих аналогій в криптоаналізі.

* Атака на основі відомого порожнього контейнера. Якщо він відомий Віллі, то шляхом порівняння його з передбачуваним стего він завжди може встановити факт наявності стегоканала. Незважаючи на тривіальність цього випадку, в ряді робіт наводиться його інформаційно-теоретичне обґрунтування. Набагато цікавіший сценарій, коли контейнер відомий приблизно, з деякою похибкою (як це може мати місце при додаванні до нього шуму).
* Атака на основі обраного порожнього контейнера. У цьому випадку Віллі здатний змусити Алісу користуватися запропонованим їй контейнером. Наприклад, запропонований контейнер може мати великі однорідні області (однотонні зображення), і тоді буде важко забезпечити секретність впровадження.
* Атака на основі відомої математичної моделі контейнера або його частини. При цьому атакуючий намагається визначити відмінність підозрілого повідомлення від відомої йому моделі. Наприклад припустимо, що біти всередині відліку зображення корельовані. Тоді відсутність такої кореляції може служити сигналом про наявний прихованому повідомленні. Завдання приховування повідомлення полягає в тому, щоб не порушити статистики контейнера. Той хто приховує і атакуючий можуть користуватися різними моделями сигналів, тоді в інформаційно-приховуваному протиборстві переможе той, що має кращу модель.

Розглянуті вище атаки мають одну особливість: вони не змінюють стегоповідомлення, які посилає Аліса, а також не спрямовані на протидію роботи декодера Боба. У цьому полягає їхня позитивна сторона: дії Віллі навряд чи здатні насторожити Алісу і Боба.

Порівняння стійкості стегосистем спричинено зазвичай по відношенню до деяких стандартних тестів. В якості одного з них є атака, заснована на застосуванні алгоритму стиснення JPEG (досить неефективна атака). Набагато більше уявлення про достоїнства того або іншого стегоалгоритма можна отримати, комплексно використовуючи різні атаки. Загальнодоступна в Інтернеті програма Stirmark дозволяє більш повно аналізувати стійкість стегоалгоритмів. За твердженням творців програми на сьогоднішній день не існує загальновідомого стегоалгоритма, стійкого до їх комплексним атакам [3].

Всі методи стеганоаналізу, розроблені для забезпечення інформаційної безпеки в комп'ютерних мережах, можна розбити на три типи згідно з завданням, яке вони вирішують:

* Методи знищення прихованої інформації - найпростіший тип методів. Метою методів даного типу є повне або часткове знищення інформації, прихованої в контейнері, при цьому передбачається, що метод відкриття і факт наявності повідомлення в контейнері не відомі. Застосування даних методів в комп'ютерних мережах повинно захистити від можливості організації прихованих каналів на базі переданого по мережі трафіка, з урахуванням найбільшої кількості можливих типів контейнерів і методів приховування.
* Методи визначення факту наявності прихованої інформації призначені для пошуку контейнерів, що містять приховану інформацію. Методи даного типу для кожного контейнера перевіряють факт наявності інформації, прихованої за допомогою кожного з відомих методів приховування, після чого на основі отриманих результатів проводиться знищення прихованої інформації. Такі методи являються більш сильним інструментом в руках адміністратора безпеки, ніж попередні, але в той же час вони вимагають великих обчислювальних ресурсів.
* Методи добування прихованої інформації є найбільш складними в розробці. Перш за все, це пов'язано з тим, що більшість існуючих методів приховування зашифровують повідомлення перед приховуванням, внаслідок чого витяг повідомлення розбивається на два етапи: вилучення прихованих даних і дешифрування вихідного повідомлення.

Також залежно від використовуваних вихідних даних їх можна розділити на дві основні групи:

1) Методи, призначені для роботи з конкретними заздалегідь відомими стеганографічними алгоритмами.

2) Методи, призначені для будь-яких алгоритмів стеганографії. Стеганоаналіз даними методами не вимагає знання використаного стеганографічного алгоритму, алгоритму шифрування, стиснення, ключа і довжини повідомлення. Відомі методи цієї групи зазвичай побудовані на алгоритмах, що вимагають попереднього «випробування» на серіях із заповнених та порожніх контейнерів. Методи обох груп побудовані з урахуванням припущення про недоступність вихідного порожнього контейнера, який був використаний для впровадження інформації в досліджуваний стеганоконтейнер.

До першої групи відносять сигнатурні і схемні методи аналізу.

Суть *сигнатурних методів* полягає в синтаксичному аналізі поданої на вхід розпізнавального пристрою послідовності термінальних символів, визначальних для досліджуваного контейнера. У разі виявлення приналежності пред'явленої на вхід розпізнавального пристрою ланцюжка термінальних символів мови, що описує ту чи іншу стеганосистему, приймається рішення про її використання для приховування інформації. В якості термінальних символів зазвичай беруть всі або частину стандартних символів ASCII - латинські букви, цифри та спеціальні символи.

До переваг цих методів належить можливість отримання результату, який однозначно характеризує застосовану для приховування даних стеганосистему.

Основним недоліком є невелике (менше 10%) число стеганопрограмм, що залишають в контейнерах свої сигнатури.

*Схемні методи* застосовуються для перевірки гіпотез про наявність стеганографічного вкладення з апріорно відомою стеганосистемою. У літературі наведено опис застосування статистичного методу Хі-квадрат для перевірки гіпотези про наявність даних, прихованих стеганопрограмами Jsteg, Jpeg Hide & Seek і OutGuess. При цьому використовуються знання про розподіл статистики за даними контейнерів, які притаманні саме для результатів роботи зазначених програм.

Перевагою методів даного класу є відносно низька ймовірність виникнення помилок, а також той факт, що за позитивного результату аналізу аналітик ідентифікує стеганосистему, що не залишає «слідів» (сигнатур) в контейнері, що дозволяє зробити спробу вилучення прихованої інформації.

У другу групу входять візуальні і статистичні методи.

Візуальні методи базуються на здатності зорової системи людини аналізувати зорові образи і виявляти суттєві відмінності в зіставлюваних зображеннях.

*Метод візуального аналізу* є найпростішим способом аналізу графічних файлів, оскільки для цього достатньо просто подивитися на перехоплене зображення. Тим не менш, цей метод аналізу вже здатний встановити деякі обмеження на обсяг приховуваних даних. Так, для повнокольорових реалістичних зображень у форматі BMP непомітними для людського ока будуть спотворення менше 3%. У випадку з JPEG візуально визначити присутність прихованої інформації неможливо. Якщо в результаті приховування в зображенні виникають незначні спотворення, то їх можна пояснити застосуванням процедури стиснення.

*Метод візуального аналізу бітових зрізів*. Основна ідея методу полягає в порівнянні зображення в цілому з зображеннями його бітових зрізів. За допомогою програми зображення переглядають по шарах - двійковими зрізами. Враховуючи те, що інтенсивність кожного кольору визначається рівно одним байтом, всього необхідно переглянути 8 таких зрізів. Для кожного з трьох кольорів перший зріз – це зображення, побудоване наймолодшими бітами, другий зріз - зображення, побудоване другими бітами і т.д. Отримане зображення бітового зрізу переглядають і візуально порівнюють з аналізованим зображенням.

Для методу візуального аналізу бітових зрізів велике значення має те, як саме здійснюється запис інформації, що приховується. Якщо вона записується в підряд ідучі біти або рівномірно розподіляє біти сполучення (на основі генератора псевдовипадкових чисел) по всьому зображенню, то факт приховування може бути встановлений з великою ймовірністю. Також візуально можна визначити наявність вбудованої інформації у випадку запису повідомлення із заповненням. Оскільки ймовірністні характеристики повідомлення не збігаються з імовірнісними характеристиками молодших біт порожнього контейнера, то при перегляді бітового зрізу з вбудованими даними буде чітко видно межу між заповненою і не зміненою частиною. Для того щоб імовірнісні характеристики співпадали, під час запису інфорції із заповненням, повідомлення необхідно зашифровувати.

У випадку з JPEG-файлами даний метод аналізу малопридатний, так як зміна будь-якого коефіцієнта перетворення призводить до зміни безлічі пікселів зображення. Впровадження повідомлення в молодші біти дискретних косинусних коефіцієнтів незначно змінить кожен з 256 пікселів, що візуально непомітно.

*Статистичні методи* базуються на понятті «природного» контейнера. Суть методів полягає в оцінюванні ймовірності існування стеганографічного вкладення з невідомою стеганосистемою на основі критерію оцінки близькості досліджуваного контейнера до «природного». До достоїнств цієї групи методів належить необмежена область використання, що досить суттєво як при перевірці гіпотези про наявність стеганографічного вкладення з невідомою стеганосистемою, так і при розробці схемних методів стеганоаналіза.

Основним недоліком методів цього класу є сааме припущення про існування «природного» контейнера. Розглянемо ряд статистичних методів, що застосовуються на практиці.

*Метод оцінки числа переходів значень молодших біт у сусідніх елементах зображення.* У методі використовується знання, що між молодшими бітами сусідніх елементів і між ними і рештою бітами природних контейнерів є кореляційні зв'язки. При аналізі графічних файлів формату BMP в якості елементів аналізованої послідовності вибираються найменш значущі біти кольвих складових поруч стоячих пікселів зображення. При дослідженні файлів формату JPEG - молодші біти сусідніх дискретних косинусних коефіцієнтів, відмінних від 0 і 1.

Залежність між бітами у відповідних розрядах елементів контейнера має марківський характер. При цьому параметри прояву визначаються номером розряду. Під «переходом» розуміють перехід значення i-го елемента після послідовності в значення i +1 елемента послідовності x, i = 1,2 ,..., n -1, n - довжина послідовності. Так як послідовності є двійковими, то аналізують чотири види переходів: з 0 в 0, з 0 в 1, з 1 в 0 і з 1 в 1. За отриманими результатами будується гістограма. Для кожного розряду перший стовпець гістограми показує кількість переходів в потоці НЗБ з 0 в 0, другий стовпчик - з 0 в 1, третій стовпець - з 1 в 0, четвертий стовпець - з 1 в 1.

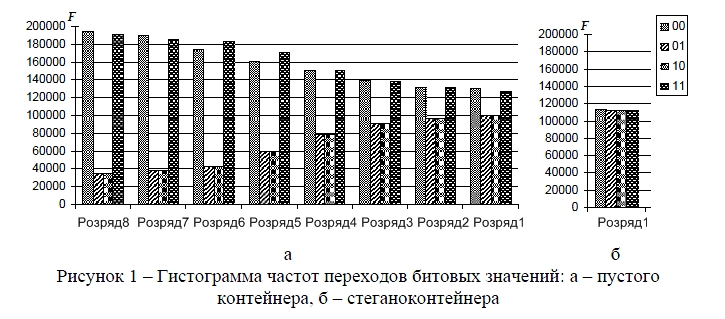


Рис.2.3. Гістограма частот переходів бітових значень: а – пустого контейнера, б – стеганоконтейнера

Для порожнього контейнера і контейнера, що містить вбудовану інформацію, кількість переходів в потоці НЗБ буде різною. Розподіл НЗБ стеганоконтейнера має, як правило, випадковий характер. Відповідно кількість переходів в потоці НЗБ для всіх станів буде приблизно однаковою, що не властиво порожньому контейнеру (рис.2.3. а, б).

*Метод оцінки частот появи k-бітових серій в потоці НЗБ елементів контейнера*. Метод дозволяє оцінити рівномірність розподілу елементів в досліджуваній послідовності на основі аналізу частоти появи нулів і одиниць, і серій, що складаються з k біт. У бітовому представленні досліджуваної послідовності x підраховується, скільки разів зустрічаються нулі й одиниці (k=1), серії-двійки (00, 01, 10, 11: k=2), серії-трійки (000, 001, 010, 011, 100, 101, 110, 111: k=3) і т.д. На основі результатів будується гістограма.

Для JPEG-зображень гістограма будується за значеннями частот появи бітових серій в потоці НЗБ дискретних косинусних коефіцієнтів, відмінних від - 1, 0, 1.0

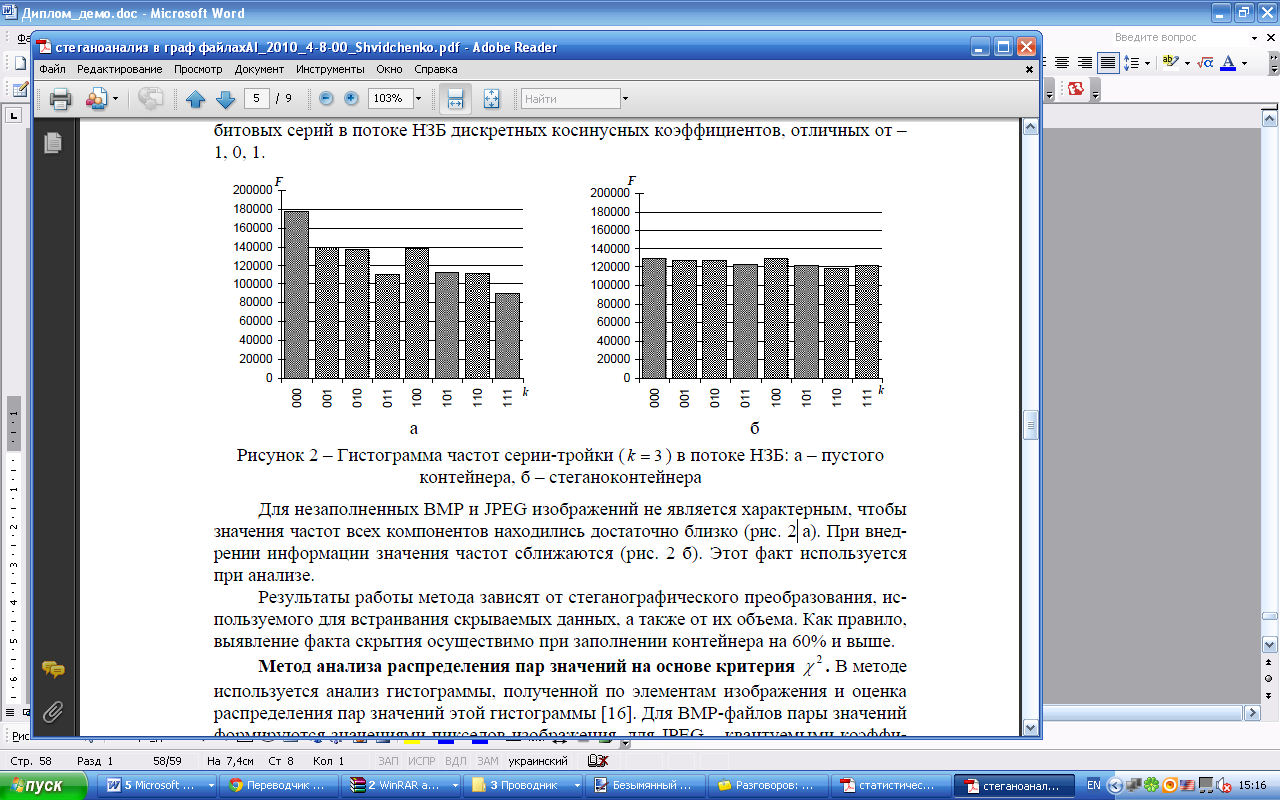


Рис.2.4 Гістограма частот серії-трійки (k=3) в потоці НЗБ: а – пустого контейнера, б – стеганоконтейнера

Для незаповнених BMP і JPEG зображень не є характерним, щоб значення частот всіх компонентів перебували досить близько (рис. 2.4. а). При вбудовуванні інформації значення частот зближуються (рис. 2.4. б). Цей факт використовується при аналізі.

Результати роботи методу залежать від стеганографічного перетворення, що викотовується для вбудовування приховуваних даних, а також від їх обсягу. Як правило, виявлення факту приховування здійсненно при заповненні контейнера на 60% і вище.

*Метод аналізу розподілу пар значень на основі критерію χ2*. У методі використовується аналіз гістограми, отриманої за елементами зображення і оцінка розподілу пар значень цієї гістограми. Для BMP-файлів пари значень формуються значеннями пікселів зображення, для JPEG - квантованого коефіцієнту дискретного косинусного перетворення, які відрізняються за молодшими бітами. Молодші біти зображень не є випадковими. Частоти двох сусідніх елементів контейнера повинні знаходитися достатньо далеко від значення частоти середнього арифметичного цих елементів. У «порожньому» зображенні ситуація, коли частоти елементів зі значеннями 2N і 2N +1 близькі за значенням, зустрічається достатньо рідко. При вбудовуванні інформації дані частоти зближуються або стають рівними. Ідея атаки хі-квадрат полягає в пошуку цих близьких значень і підрахунку ймовірності розміщення на основі того, як близько розташовуються значення частот парних і непарних елементів аналізованого контейнера. Особливістю алгоритму є послідовний аналіз всього зображення і, відповідно, накопичення частот елементів.

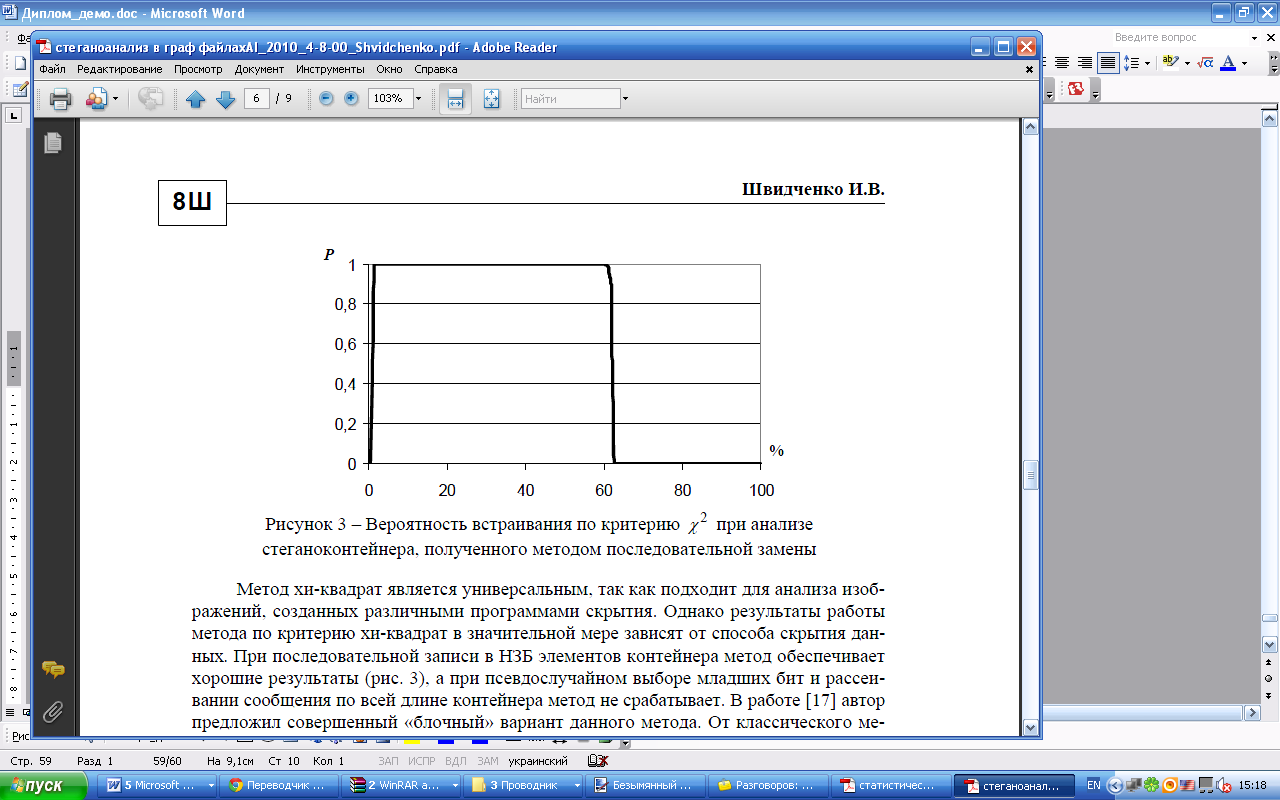


Рис.2.5.Ймовірність вбудовування по критерію хі-квадрат при аналізі стеганоконтейнера, отриманого методом послідовної заміни

Метод хі-квадрат є універсальним, так як підходить для аналізу зображень, створених різними програмами приховування. Однак результати роботи методу за критерієм хі-квадрат значною мірою залежать від способу приховування даних. При послідовному записі в НЗБ елементів контейнера метод забезпечує хороші результати (рис. 2.5.), а при псевдовипадковому виборі молодших біт і розташуванні повідомлення по всій довжині контейнера метод не спрацьовує. У роботі [4] автор запропонував досконалий «блоковий» варіант даного методу. Від класичного методу він відрізняється тим, що аналізоване зображення розбивається на блоки визначеного розміру, які можуть як перетинатися, так і не перетинатися, і для кожного з цих блоків розраховуються свої набори частот елементів і свої ймовірності приховування. Крім того, існує можливість вибору окремих областей зображення для їх подальшого аналізу. Такий підхід дозволяє виявляти наявність інформації, прихованої псевдовипадковим чином.

*Метод аналізу гістограм, побудованих по частотах елементів зображення.* Метод дозволяє оцінити рівномірність розподілу елементів аналізованого зображення, а також визначити частоту появи конкретного елемента. Якщо розкид частот появи елементів в колірних складових BMP-зображення прямує до нуля, то контейнер містить приховані дані. В іншому випадку контейнер вважається порожнім.

Для зображень в JPEG-форматі будується гістограма частот квантова них дискретних косинусних коефіцієнтів. Експериментально виявлено, що огинаюча гістограми порожнього зображення має більш гладкий характер (рис. 2.6. а) в порівнянні з гістограмами зображень, що містять стеганографічної вкладення (рис.2.6. б). Звичайно, в залежності від характеру і ступеня стиснення зображення, гістограми можуть змінюватися - у них можуть з'являтися скачки і провали, але важливо те, що приховування змінює загальний вигляд гістограм. Більшість стеганографічних програм, що працюють з JPEG, приховують дані в молодші біти дискретних коефіцієнтів, відмінних від 0 і 1. Як наслідок, частоти 0-х і 1-х DCT не змінюються, в той час як всі інші частоти або зменшуються, або збільшуються в залежності від алгоритму вбудовування. При значних обсягах прихованої інформації гістограми часто набувають ступінчастий характер, що нетипово для звичайних JPEG-зображень.

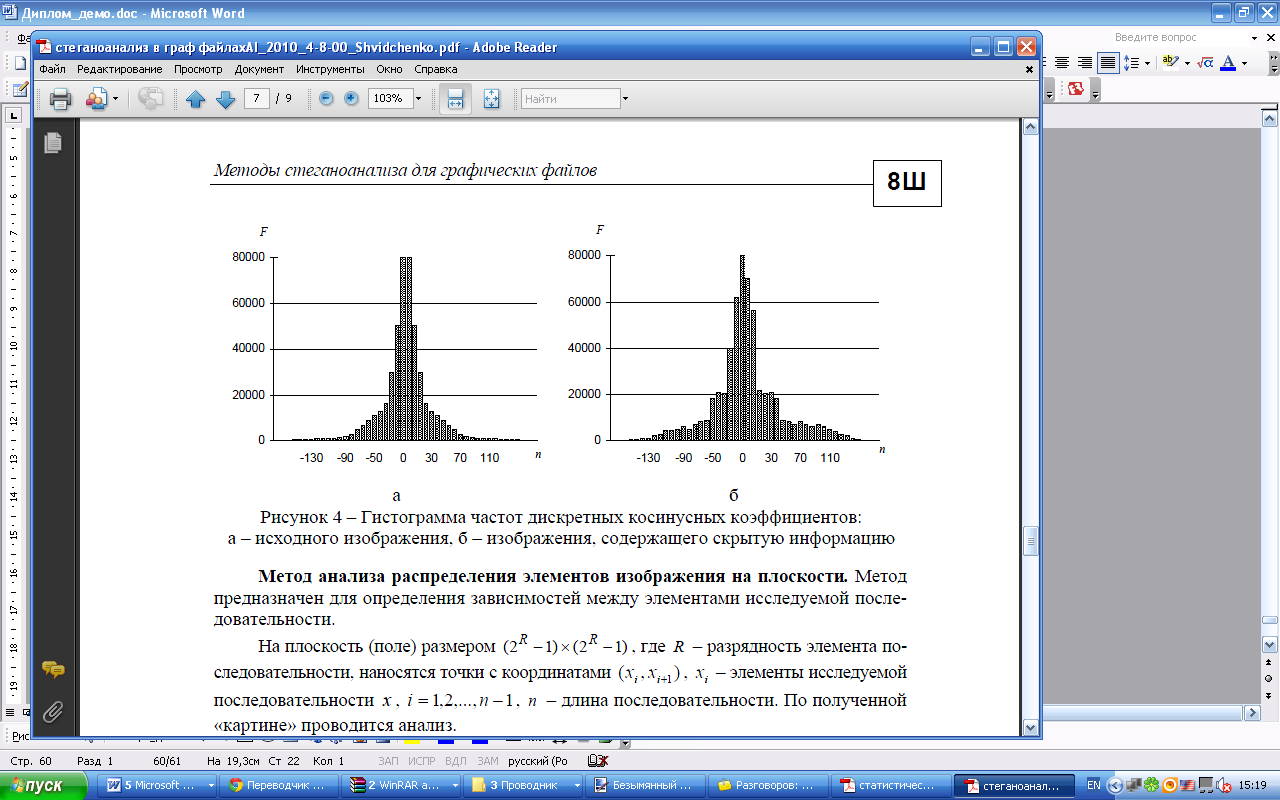


Рис.2.6.Гістограма частот дискретних косинус них коефіцієнтів: а – вихідного зображення, б – зображення, що містить приховану інформацію

*Метод аналізу розподілу елементів зображення на площині.* Метод призначений для визначення залежностей між елементами досліджуваної послідовності.

На площину (поле) розміром (2R -1) × (2R -1), де R – розрядність елемента послідовності, наносяться точки з координатами (хі, хі+1), хі- елементи досліджуваної послідовності x, i=1,2,...,n-1,n – довжина послідовності. За отриманою «картиною» проводиться аналіз.

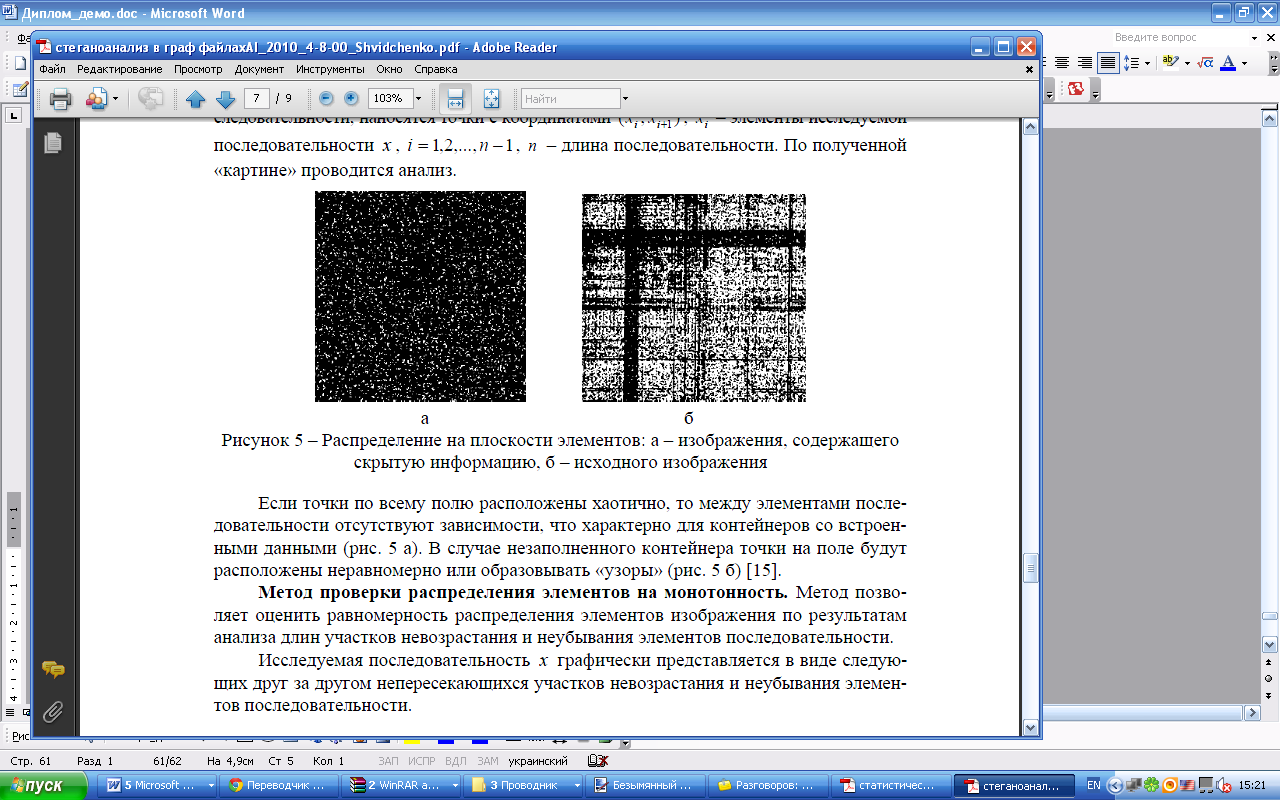


Рис.2.7. Розподілення на площині елементів: а – зображення, яке містить приховану інформацію, б – початкове зображення

Якщо точки по всьому полю розташовані хаотично, то між елементами послідовності відсутня залежність, що характерно для контейнерів з будованими даними (рис.2.7. а). У випадку незаповненого контейнера точки на полі будуть розташовані нерівномірно або утворювати «візерунки» (рис.2.7. б).

*Метод перевірки розподілу елементів на монотонність.* Метод дозволяє оцінити рівномірність розподілу елементів зображення за результатами аналізу довжин ділянок не зростання і не спадання елементів послідовності. Досліджувана послідовність x графічно представляється у вигляді слідуючих одна за одною непересікаючих ділянок незростання і неспадання елементів послідовності.

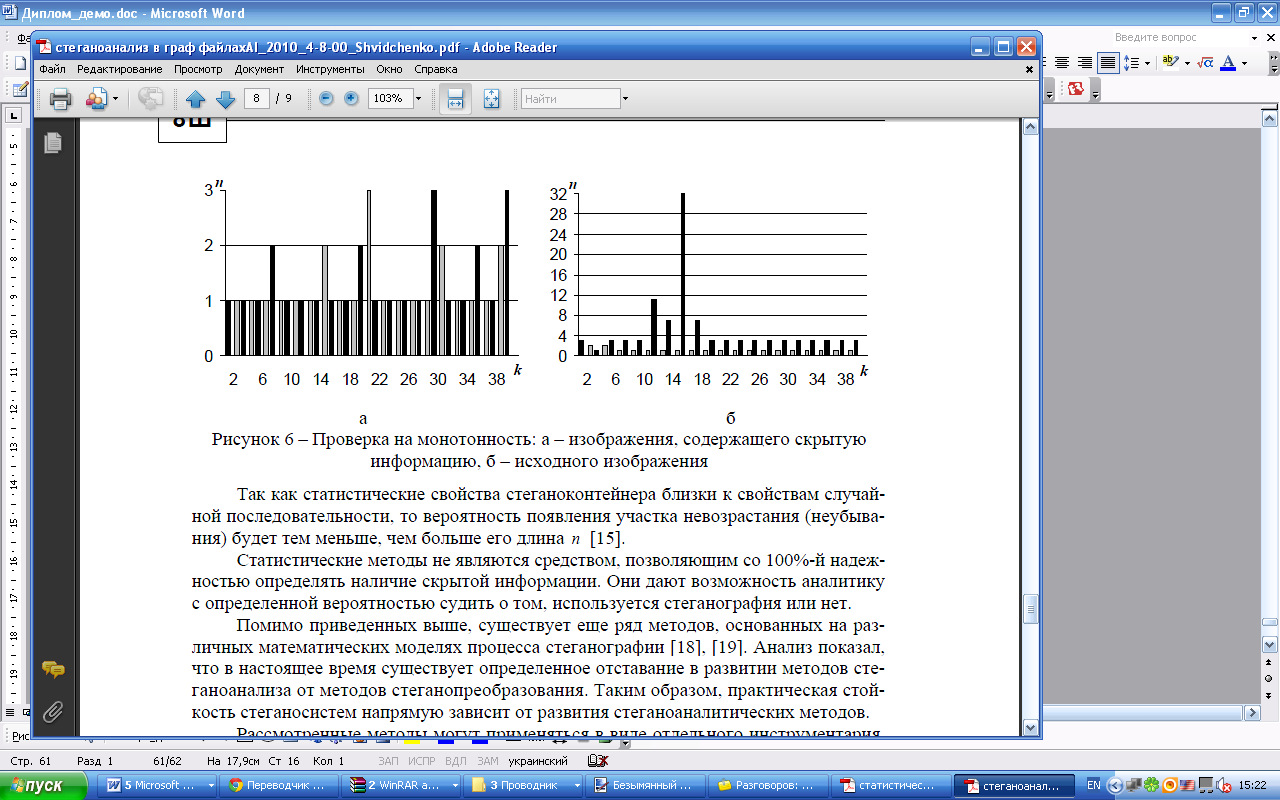


Рис.2.8. Перевірка на монотонність: а – зображення, яке містить приховану інформацію, б – початкове зображення

Так як статистичні властивості стеганоконтейнера близькі до властивостей випадкової послідовності, то ймовірність появи ділянки незростання (неспадання) буде тим менше, чим більше його довжина n.

Статистичні методи не є засобом, що дозволяє зі 100%-й надійністю визначати наявність прихованої інформації. Вони дають можливість аналітику з певною ймовірністю судити про те, використовується стеганографія чи ні. Окрім наведених вище, існує ще ряд методів, заснованих на різних математичних моделях процесу стеганографії.

Аналіз показав, що в даний час існує певне відставання у розвитку методів стеганоаналізу від методів стеганоперетворення. Таким чином, практична стійкість стеганосистем безпосередньо залежить від розвитку стеганоаналітіческіх методів.

Стеганоаналіз потенційного контейнера в умовах багаторазового використання статистичних методів за умови неспрацьовування сигнатурних і схемних методів носить умовний характер. При використанні виключно статистичних методів необхідно тривале спостереження за стеганоканалом і значні зусилля досвідченого аналітика. Крім того, необхідно знання алгоритму стеганоперетворення. Необхідною умовою для встановлення факту присутності в контейнері прихованої інформації є спрацьовування сигнатурних або схемних методів [25].

## 2.4. Оцінка якості стеганографічної системи

Створення і експлуатація надійного стеганографічного засобу передбачає наявність визначеного інструментарію для його контролю та оцінки. Кількісне оцінювання стійкості стеганографічної системи захисту до зовнішніх впливів являє собою доволі тяжку задачу, яка за звичай на практиці реалізується методами системного аналізу, математичного моделювання або експериментального дослідження.

Як правило, професійно розроблена стеганосистема забезпечує трьохрівневу модель захисту інформації, яка вирішує дві основні задачі:

* приховування самого факту наявності інформації, що захищається (перший рівень захисту);
* блокування несанкціонованого доступу до інформації, яке здійснюється шляхом вибирання відповідного методу приховування інформації (другий рівень захисту).

Також необхідно брати до уваги і ймовірність існування третього рівня – попереднього криптографічного захисту (шифрування) інформації.

На рис.2.9. представлена можлива структура процесу моделювання і оцінки стійкості стеганосистеми.

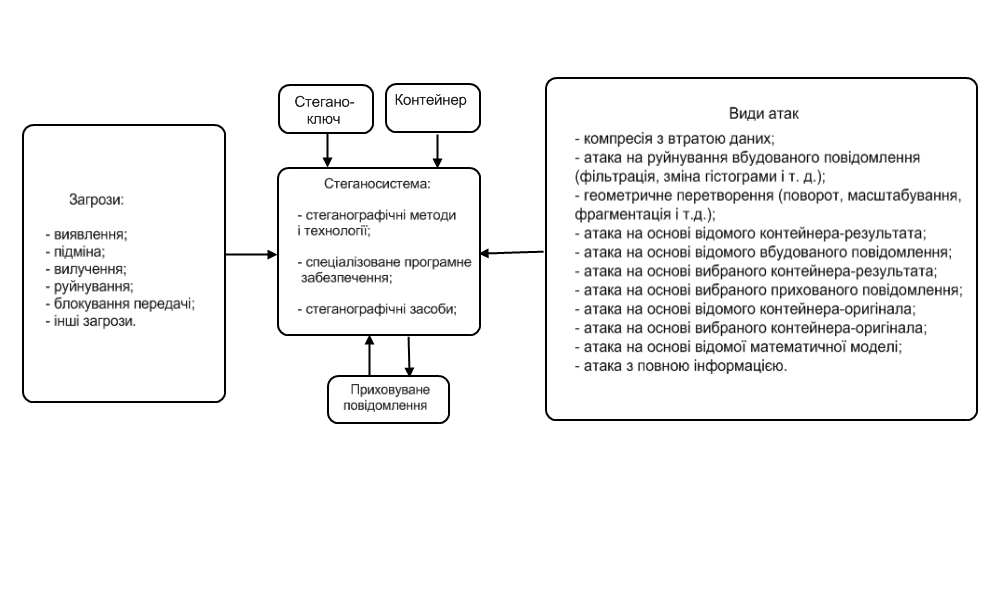


Рис.2.9. Модель аналізу загрози і оцінки стійкості стеганосистем

Як бачимо, надійність і період стійкості стеганосистеми в випадку проведення стеганоаналізу і випробувань визначаються можливостями обчислювальної системи.

Оцінка якості основної характеристики стеганосистеми – рівня приховування – забезпечується шляхом проведення аналітичних досліджень (стеганоаналізу) і натурних випробувань. Для оінки якості стеганографічного приховування часто використовують відомі методи з інших областе, в першу чергу г криптоаналізу. Оскільки абонент-отримувач може відновити приховану інформацію прийнятого повідомлення, то цілком очевидно, що існує певний механізм її вилучення.

Якщо порушник, висуваючи гіпотези про можливе стеганографічне перетворення, має деякий інструмент для їх перевірки, то він має шанс підтвердити факт існування прихованої інформації, виконати пошук механізму вилучення секретного повідомлення, а також розкрити його зміст. Тому, в першу чергу, для детектування стеганограм можна використовувати різновиди описаних вище атак на стеганосистему і значну частину методів криптоаналізу.

Достатньо ефективні в деяких випадках методи оцінки рівня приховування стеганозасобів на основі аналізу їх статистичних характеристик. Статистична теорія дає кількісні критерії ймовірності, що дозволяє створювати детектори, які будуть виявляти статистичні відмінності між послідовностями. У випадку наявності достатнього об’єму інформації для аналізу с достатньо високою ймовірністю можна робити висновки про основні характеристики послідовності, виділеної для аналізу з контейнера.

На початковому етапі аналізу рекомендується скористатися традиційним статистичними (χ2  , тести на заборонені символи, на довжину циклу і т.д.), емпіричними (перевірка частот, серій, інтервалів, перестановок; перевірка на монотонність, «покер-тестом», тестом «збирача купонів»)або спектральними тестами. Далі доцільно використовувати більш гнучкі методи, які іноді спеціально розробляються під конкретну задачу.

Для порівняльної оцінки якості стеганографічних засобів розробляють різні показники, які дають кількісні оцінки. Більше всього їх розроблено для стеганометодів, які працюють з зображеннями і відео (методів ЦВЗ). В основному такі показники оперують з зображеннями на рівні пікселів, хоча після деякої адаптації, їх можна використовувати і до інших способів опису зображень, а також до аудіо даних. Найбільш відомим показником при аналізі рівня викривлень, які вносяться в контейнер під час приховування в ньому інформації, являється взяте із радіотехніки співвідношення «сигнал/шум», яке вираховується в децибелах.

В таблиці 2.1 відображений ряд показників, які використовують під час оцінювання викривлень, які вносяться стеганоперетвореннями в зображення та основані на аналізі піксельної структури контейнера. В таблиці .



Таблиця 2.1. Найбільш поширені показники візуального спотворення

|  |  |
| --- | --- |
| Різницеві показники спотворення | |
| Максимальна різниця (Maximum Difference) | , (2.1) |
| Середня абсолютна різниця (Average Absolute Difference) | , (2.2) |
| Нормована середня абсолютна різниця (Normalized Average Absolute Difference) | , (2.3) |
| Середньоквадратична помилка (Mean Square Error) | , (2.4) |
| Нормована середньоквадратична помилка (Normalized Mean Square Error) | , (2.5) |
| Lp – норма (Lp  - norm) | , (2.6) |
| Лапласова середньоквадратична помилка (Laplacian Mean Square Error) | , (2.7) |
| Відношення «сигнал/шум» (Signal to Noise Ratio) | , (2.8) |
| Максимальне відношення «сигнал/шум» (Peak Signal to Noise Ratio) | , (2.9) |
| Якість зображення (Image Fidelity) | , (2.10) |
| Кореляційні показники спотворення | |
| Нормована взаємна кореляція (Normalized Cross-Correlation) | , (2.11) |
| Якість кореляції (Correlation Quality) | , (2.12) |

Продовження таблиці 2.1

|  |  |
| --- | --- |
| Інші показники | |
| Структурний зміст (Structural Content) | , (2.13) |
| Загальне сигма-відношення «сигнал/шум» (Global Sigma Signal to Noise Ratio) | , (2.14)  де |
| Сигма-відношення «сигнал/шум» (Sigma Signal to Noise Ratio) | , (2.15)  де |
| Нормоване відношення «сигма/помилка» (Normalized Sigma to Error Ratio) | , (2.16)  де |

Розглянуті в таблиці 2.1 показники базуються на аналізі окремих елементів сигналу (в даному випадку – пік селів зображення). Слабкі місця таких показників відомі протягом тривалого часу (наприклад, відсутність кореляції різницевих показників спотворення з зором людини). Останнім часом більшість досліджень направлено на пошуки такого показника спотворення, який був би адаптований до людської зорової та слухової системи шляхом різноманітних впливів.

В таблиці 2.1 представлені оцінки і відповідне їм зорове сприйняття внесених спотворень і якість підданих обробці зображень. Така оцінка має декілька переваг, а саме відсутність руйнування неспотворених зображень [8].

## 2.5. Висновки по розділу

В цьому розділі приділено увагу руйнівним програмним засобам, а також можливості використання стеганографії для їх впровадження. Також приведено методику оцінки якості стеганографічних систем.

Зазначено, що дії алгоритмічних і програмних закладок умовно можна розділити на три класи: зміна функціонування обчислювальної системи (мережі), несанкціоноване зчитування інформації і несанкціонована модифікація інформації, аж до її знищення. В останньому випадку під інформацією розуміються як дані, так і коди програм. Слід зазначити, що вказані класи впливів можуть перетинатися.

Розглянуто та проаналізовано сукупність методів стеганоаналізу та можливих атак на стегосистему. Увагу зупинено на використання графічних контейнерів та наведені засоби стеганоаналізу призначені для цього виду контейнерів.

Завдяки проведеній аналітичній роботі можна зробити такі практичні висновки, що стеганографія успішно може використовуватись в протиправних цілях. Тому необхідно також детально вивчати й інші сторони прихованої передачі даних, зокрема стеганоаналіз.

# РОЗДІЛ 3

## Модель РПЗ «стеганографічне перетворення»: методика реалізації та виявлення

## 3.1. Аналіз існуючих моделей РПЗ

Узагальнений опис і типізація РПЗ буде робитися відповідно до роботи ПЗ. Руйнуючим програмним засобом, в даному випадку, будемо вважати деяку програму, яка здатна виконати будь-яку не порожню підмножину перерахованих функцій:

* приховування ознак своєї присутності в програмному середовищі КС;
* реалізації самодублювання, асоціювання себе з іншими програмами та / або перенесення своїх фрагментів у інші (не займані спочатку вказаною програмою) області оперативної або зовнішньої пам'яті;
* руйнування (спотворення довільним чином) коду програм в оперативній пам'яті КС;
* переміщення (збереження) фрагментів інформації з оперативної пам'яті в деякі області оперативної або зовнішньої пам'яті прямого доступу;
* спотворення довільним чином, блокування та / або підміни ввідних в зовнішню пам'ять або в канал зв'язку масивів інформації, що утворилися в результаті роботи прикладних програм або вже знаходяться у зовнішній пам'яті, або зміни їх параметрів.

**3.1.1.Класифікація РПЗ за різними ознаками**

РПЗ, відключають захисні функції системи. У багатьох випадках РПЗ, впроваджені в захищену систему, можуть модифікувати машинний код або конфігураційні дані системи, тим самим повністю або частково відключаючи її захисні функції. У захищеної системи утворюється «чорний хід», що дозволяє зловмисникові працювати в системі, обходячи її захисні функції. Відключення програмної закладкою захисних функцій системи найчастіше використовується для зняття захисту від несанкціонованого копіювання. На рис 3.1. зображена схема класифікації сучасних РПЗ за різними ознаками.

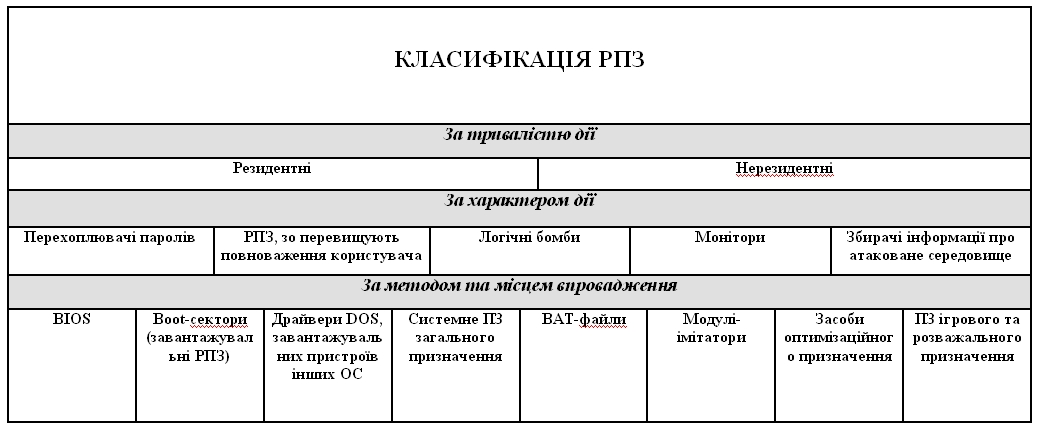


Рис. 3.1Класифікація РПЗ

*Перехоплювачі паролів*. Перехоплювачі паролів перехоплюють імена і паролі, що вводяться користувачами захищеної системи в процесі ідентифікації і аутентифікації. У найпростішому випадку перехоплені імена і паролі зберігаються в текстовому файлі, більш складні програмні закладки пересилають цю інформацію по мережі на комп'ютер зловмисника.

Існують три основні архітектури побудови перехоплювачів паролів.

1) Перехоплювачі паролів першого роду діють за наступним сценарієм. Зловмисник запускає програму, що містить програмну закладку - перехоплювач паролів. Вона імітує запрошення користувачеві для входу в систему, і чекає вводу. Коли користувач вводить ім'я і пароль, закладка зберігає їх у доступному зловмисникові місці, після чого завершує роботу і здійснює вихід із системи користувача-зловмисника. Після закінчення роботи закладки на екрані з'являється справжнє запрошення для входу користувача в систему. Користувач, що став жертвою закладки, бачить, що він не увійшов в систему і що йому знову пропонується ввести ім'я та пароль. Користувач припускає, що при введенні пароля сталася помилка, і вводить ім'я та пароль повторно. Після цього користувач входить в систему, і подальша його робота протікає нормально. Деякі закладки, що функціонують за даною схемою, перед завершенням роботи видають на екран правдоподібне повідомлення про помилку, наприклад: «Пароль введений неправильно. Спробуйте ще раз ».

2) Перехоплювачі паролів другого роду перехоплюють всі дані, що вводяться користувачем з клавіатури. Найпростіші програмні закладки даного типу просто скидають всі ці дані на жорсткий диск комп'ютера або в будь-яке інше місце, доступне зловмисникові. Більш досконалі закладки аналізують перехоплені дані і відсіюють інформацію, яка свідомо не має відношення до паролів. Ці закладки являють собою резидентні програми, що перехоплюють одне або декілька переривань, використовуваних при роботі з клавіатурою. Інформація про саму клавіші і введений символ, яка повертається цими перериваннями, використовується закладками для своїх цілей.

3) До перехоплювачів паролів третього роду відносяться програмні закладки, які повністю або частково підмінюють собою підсистему аутентифікації захищеної системи.

*Програмні закладки, що завищують повноваження користувача.* Ці закладки застосовуються для подолання тих систем захисту, в яких реалізовано розмежування доступу користувачів до об'єктів системи (в основному ці закладки застосовуються проти операційних систем).

Дані даного типу дозволяють зловмисникові здійснювати доступ до тих об'єктів, доступ до яких має бути йому заборонений відповідно до поточної стратегії захисту. У більшості систем, що підтримують розмежування доступу, існують адміністратори безпеки, які можуть здійснювати доступ до всіх або майже всіх об'єктів системи. Якщо програмна закладка наділяє користувача-зловмисника повноваженнями адміністратора і зловмисник має практично необмежений доступ до ресурсів системи, засоби і методи, використовувані такими закладками для перевищення повноважень користувача, що значною мірою визначаються архітектурою системи. Найчастіше закладки даного класу використовують помилки в програмному забезпеченні системи.

*Логічні бомби*. Це програмні закладки, які надають, як правило, руйнівного впливу на атакуючу систему і зазвичай націлені на повне виведення системи з ладу. На відміну від вірусів логічні бомби не розмножуються або розмножуються обмежено. Логічні бомби завжди призначені для атаки на конкретну комп'ютерну систему. Після того як руйнівний вплив завершено, то, як правило, логічна бомба знищується.

Іноді виділяють особливий клас логічних бомб - тимчасові бомби, для яких умовою спрацьовування є досягнення певного моменту часу. Характерною властивістю логічних бомб є те, що реалізовані ними негативні впливи на атаковану систему носять виключно руйнівний характер. Логічні бомби, як правило, не використовуються для організації НСД до ресурсів системи, їх єдиним завданням є повне або часткове руйнування системи.

*Монітори*. Це програмні закладки, що перехоплюють ті чи інші потоки даних, що протікають в атакованої системі. Зокрема, до моніторів відносяться перехоплювачі паролів другого роду. Цільове призначення моніторів може бути самим різним:

* повністю або частково зберігати перехоплену інформацію в доступному зловмисникові місці;
* спотворювати потоки даних;
* поміщати в потоки даних нав'язану інформацію;
* повністю або частково блокувати потоки даних;
* використовувати моніторинг потоків даних для збору інформації про атаковану систему.

Монітори дозволяють перехоплювати самі різні інформаційні потоки атакованої системи. Найбільш часто перехоплюються наступні потоки:

* потоки даних, пов'язані з читання, записом та іншими операціями над файлами;
* мережевий трафік;
* потоки даних, пов'язані з видаленням інформації з дисків або з оперативної пам'яті комп'ютера (так звана «прибирання сміття»).

*Збирачі інформації про атаковане середовище.* Програмні закладки цього класу призначені для пасивного спостереження за програмним середовищем, в яку впроваджена закладка. Основна мета застосування подібних закладок полягає в первинному зборі інформації про атаковану систему. Надалі ця інформація використовується при організації таких систем, які можливо застосовуватимуть програмні закладки інших класів.

Крім того, РПЗ можна класифікувати за методом і місцем їх впровадження та застосування, тобто по «способу доставки» в комп'ютерну систему (нижче наводиться приклад персонального комп'ютера):

* РПЗ, асоційовані з програмно-апаратним середовищем комп'ютерної системи (основна BIOS або розширені BIOS);
* РПЗ, асоційовані з програмами первинного завантаження (перебувають у Master Boot Record або ВООТ-секторах активних розділів), - завантажувальні РПЗ;
* РПЗ, асоційовані із завантаженням драйверів DOS, драйверів зовнішніх пристроїв інших ОС, командного інтерпретатора, мережевих драйверів, тобто із завантаженням операційного середовища;
* РПЗ, асоційовані з системним програмним забезпеченням загального призначення (вбудовані в клавіатурні та екранні драйвери, програми тестування комп'ютерів, утиліти і оболонки інтерфейсу з користувачем і т.п.);
* виконувані модулі, що містять тільки код РПЗ (як правило, впроваджувані у файли пакетної обробки типу. BAT);
* модулі-імітатори, що збігаються за зовнішнім виглядом з деякими програмами, що вимагають введення конфіденційної інформації - найбільш характерні для Unix-систем;
* РПЗ, що маскуються під програмні засоби оптимізаційного призначення (архіватори, прискорювачі обміну з диском і т.д.);
* РПЗ, що маскуються в програмні засоби ігрового і розважального призначення (як правило, використовуються для первинного впровадження закладок).

Для того щоб РПЗ змогли виконувати будь-які дії по відношенню до прикладної програми або даних, вони повинні отримати управління, тобто процесор повинен почати виконувати інструкції (команди), пов'язані з кодом РПЗ. Це можливо тільки при одночасному виконанні двох умов:

1).РПЗ повинно знаходитися в оперативній пам'яті до початку роботи РПЗ, яке є метою впливу закладки, а отже, РПЗ повинно бути додано раніше або одночасно з цією програмою;

2).РПС має активізуватися по деякою загальною як для закладання, так і для програми подією, тобто при виконанні ряду умов у програмно-апаратному середовищі управління повинно бути передано програмі-закладці.

Зазвичай виконання зазначених умов досягається шляхом аналізу й обробки закладкою загальних щодо РПЗ і прикладної програми дій (як правило, переривань) або подій (залежно від типу та архітектури операційного середовища). Причому переривання повинні супроводжувати роботу програми або роботу всього комп'ютера. Дані умови є необхідними (але недостатніми), тобто якщо вони не виконані, то активізація коду закладки не відбудеться і код не зможе надати будь-якого впливу на роботу прикладної програми.

Крім того, можливий випадок, коли при запуску програми (активізуючою подією є запуск програми) закладка руйнує деяку частину коду програми, вже завантаженої в оперативну пам'ять, і, можливо, систему контролю цілісності коду або контролю інших подій і на цьому закінчує свою роботу. Даний випадок не суперечить необхідним умовам. З урахуванням зауваження про те, що РПЗ повинна бути завантажена у ОП раніше, ніж мета його впливів, можна виділити РПЗ двох типів.

1) РПЗ резидентного типу - знаходяться в пам'яті постійно з деякого моменту часу до закінчення сеансу роботи комп'ютера (виключення живлення або перезавантаження). РПЗ може бути додано в пам'ять при початковому завантаженні комп'ютера, завантаженні операційного середовища або запуску деякої програми (яка за традицією називається вірусоносієм або просто носієм), а також запущена окремо.

2) РПС нерезидентного типу - починають роботу, як і РПС резидентного типу, але закінчують її самостійно через деякий проміжок часу або після настання деякої події, при цьому вивантажуючи себе з пам'яті повністю.

**3.1.2.Основні методи впровадження РПЗ**

1) Маскування закладки під «невинне» програмне забезпечення. Даний метод полягає в тому, що програмна закладка впроваджується в систему під виглядом нової програми, на перший погляд абсолютно нешкідливої. Програмна закладка може бути впроваджена в текстовий або графічний редактори, системну утиліту, комп'ютерну гру, зберігач екрану і т.д. Після впровадження закладки її присутність в системі не потрібно маскувати - навіть якщо адміністратор помітить факт появи в системі нової програми, він не додасть цьому значення, оскільки ця програма зовні зовсім нешкідлива.

2) Маскування закладки під «нешкідливий» модуль розширення програмного середовища. Багато програмних середовища допускають своє розширення додатковими програмними модулями. Наприклад, для операційних систем сімейства Microsoft Windows модулями розширення можуть виступати динамічно завантажувані бібліотеки (DLL) і драйвери пристроїв. У таких модулях розширення може міститися РПЗ, який може бути потенційно впроваджено в систему. Даний метод фактично є окремим випадком попереднього методу і відрізняється від нього тільки тим, що закладка представляє собою не прикладну програму, а модуль розширення програмного середовища.

3) Підміна закладкою одного або декількох програмних модулів атакованого середовища. Даний метод впровадження в систему програмної закладки полягає в тому, що в атакованому програмному середовищі вибирається один або кілька програмних модулів, підміна яких фрагментами програмної закладки дозволяє здійснювати в середовищі необхідні негативні дії. Програмна закладка повинна повністю реалізовувати всі функції підмінюваних програмних модулів.

Основна проблема, що виникає при практичній реалізації даного методу, полягає в тому, що програміст, який розробляє програмну закладку, ніколи не може бути впевнений, що створена ним закладка точно реалізує всі функції підмінюваного програмного модуля. Якщо модуль, який підмінюється, досить великий за обсягом або недостатньо детально документований, точно запрограмувати всі його функції практично неможливо. Тому описаний метод доцільно застосовувати тільки для тих програмних модулів атакованого середовища, для яких доступна повна або майже повна документація. Оптимальною є ситуація, коли є початкові коди підмінюваного модуля.

4) Пряме асоціювання. Даний метод впровадження в систему програмної закладки полягає в асоціюванні закладки з виконуваними файлами однієї або декількох легальних програм системи.

Складність завдання прямого асоціювання програмної закладки з програмою атакованого середовища істотно залежить від того, яким є атаковане середовище: однозадачним або багатозадачним, однокористувацьким або розрахованим на багато користувачів. Для однозадачних однокористувацьких систем ця задача вирішується досить просто. У той же час при впровадженні закладки в многозадачне або багатокористувацьке програмне середовище пряме асоціювання закладки з легальним програмним забезпеченням є досить нетривіальним завданням.

5) Непряме асоціювання. Непряме асоціювання закладки з програмним модулем атакованого середовища полягає в асоціюванні закладки з кодом програмного модуля, завантаженим в оперативну пам'ять. При непрямому асоціюванні виконуваний файл програмного модуля залишається незмінним, що затруднює виявлення програмної закладки.

Для того щоб непряме асоціювання стало можливим, необхідно, щоб встановлювана частина закладки вже була присутня в системі. Іншими словами, програмна закладка, впроваджувана в систему за допомогою непрямого асоціювання, повинна бути її складовою.

**3.1.3.Моделі взаємодії прикладної програми і програмної закладки**

Загальну модель РПЗ можна представити у вигляді сукупності моделей, кожна з яких відповідає описаним вище типам РПЗ і характеризує дії зловмисника, виходячи з його образу думок і можливостей.

1) Модель «перехоплення». Програмна закладка вбудовується (впроваджується) в ПЗП, ОС або прикладне програмне забезпечення і зберігає всі або вибрані фрагменти, що вводиться або виводиться у прихованій області локальної або віддаленої зовнішньої пам'яті прямого доступу. Об'єктом збереження може бути клавіатурний ввід, документи, що виводяться на принтер, або знищуються файли-документи.

Для даної моделі істотним є наявність у зовнішній пам'яті місця зберігання інформації, яке має бути організоване таким чином, щоб забезпечити її збереження протягом заданого проміжку часу і можливість подальшого знімання. Важливо також, щоб збережена інформація була яким-небудь чином замаскована від перегляду легальними користувачами.



Рис.3.2. Схема РПЗ моделі «перехоплення»

2) Модель «троянський кінь». Закладка вбудовується в постійно використовуване програмне забезпечення та по деякій активізуючій події моделює збійні ситуації на засобах зберігання інформації або в устаткуванні комп'ютера (мережі). Тим самим можуть бути досягнуті дві різні цілі: по-перше, паралізована нормальна робота комп'ютерної системи і, по-друге, зловмисник (наприклад, під виглядом обслуговування або ремонту) може ознайомитися з наявною в системі або накопиченої за допомогою використання моделі «перехоплення» інформацією. Подією, що активізує закладку, може бути певний момент часу, або сигнал з каналу модемного зв'язку (явний чи замаскований), або стан деяких лічильників (наприклад, число запусків програм).



Рис.3.3. Схема РПЗ моделі «троянський кінь»

3) Модель «спостерігач». Закладка вбудовується в мережеве або телекомунікаційне програмне забезпечення. Користуючись тим, що це ПЗ, як правило, завжди активне, програмна закладка здійснює контроль за процесами обробки інформації на даному комп'ютері, встановлення та видалення закладок, а також знімання накопиченої інформації. Закладка може ініціювати події для раніше впроваджених закладок, що діють по моделі «троянський кінь».



Рис.3.4. Схема РПЗ моделі «спостерігач»

4) Модель «компрометація». Закладка або передає задану зловмисником інформацію (наприклад, клавіатурне введення) в канал зв'язку, або зберігає її, не покладаючись на гарантовану можливість подальшого прийому або зняття. Більш екзотичний випадок - закладка ініціює постійне звернення до інформації, що приводить до зростання відношення сигнал / шум при перехопленні побічних випромінювань.



Рис.3.5. Схема РПЗ моделі «компрометація»

5) Модель «спотворення або ініціатор помилок». Програмна закладка спотворює потоки даних, що виникають при роботі прикладних програм (вихідні потоки), або спотворює вхідні потоки інформації, або ініціює (або пригнічує) виникаючі при роботі прикладних програм помилки.



Рис.3.6. Схема РПЗ моделі «спотворення або ініціатор помилок»

6) Модель «прибирання сміття». У даному випадку прямого впливу РПЗ може і не бути; вивчаються «залишки» інформації. У разі застосування програмної закладки нав'язується такий порядок роботи, щоб максимізувати кількість залишених фрагментів цінної інформації. Зловмисник одержує або дані фрагменти, використовуючи закладки моделей 2 і З, або безпосередній доступ до комп'ютера під виглядом ремонту або профілактики.



Рис.3.7. Схема РПЗ моделі «прибирання сміття»

У розглянутих різних за цілями впливу моделей закладок є важлива спільна риса - наявність операції запису, виробленої закладкою (в оперативну або зовнішню пам'ять). При відсутності даної операції ніякий негативний вплив неможливий. Цілком зрозуміло, що для спрямованого впливу закладка повинна також виконувати і операції читання. Так, наприклад, можна реалізувати функцію цілеспрямованої модифікації даних в будь-якому секторі жорсткого диска, яка можлива тільки після їх прочитання.

Таким чином, виконання коду закладки може бути супроводжено операціями несанкціонованого запису (НСЗ), наприклад, для збереження деяких фрагментів інформації, і несанкціонованого зчитування (НСЧ), яке може відбуватися окремо від операцій читання прикладної програми або спільно з ними. При цьому операції зчитування і запису можуть бути не пов'язані з отриманням інформації, наприклад зчитування параметрів пристрою або його ініціалізація - закладка може використовувати для своєї роботи і такі операції, зокрема, для ініціювання збійних ситуацій або перепризначення введення виведення.

## 3.2. Формування моделі РПЗ «стеганографічне перетворення»

Як було вказано в попередніх розділах, стеганографічні перетворення можуть використовуватись як з метою захисту інформаційних ресурсів, так і з метою реалізації зловмисних дій. Для боротьби з такого роду загрозами необхідно розуміти механізм дії таких систем. Для цього необхідно сформувати модель РПЗ «стеганографічне перетворення».

Для впровадження РПЗ даного типу буде використано стеганографічні перетворення приховування інформації. В якості контейнера - графічний файл типу \*.bmp. В якості закладки буде задіяний програмний код, який використовує механізм перехвату файлових операцій для модифікації файлів типу СОМ своїм кодом.

Робота таких РПЗ основана на тому, що програмний засіб захисту інформації (ПЗЗІ) виробляє деякі файлові операції. Для цього відкривається файл, частина його або весь файл зчитується в буфер оперативної пам'яті, обробляється і потім записується у файл з тим самим, чи новим ім'ям. Активізуючою подією в даному випадку є, як правило, відкриття файлу (int 21h, функція 3Dh), або його закриття. Таким чином, закладка породжує в системі "вхідний файл - ПЗЗІ - вихідний файл" нові зв'язки, включаючи в них свої операції і масиви даних.

Розглянемо механізм роботи закладки для DOS, яка вбудовується в ланцюжок переривання int 21h для таких функцій.

* Відкриття файлу (функція 3Dh). Закладка відфільтровує потрібні імена або дескриптор файлів.
* Читання з файлу (функція 3Fh). Закладка виконує переривання за старою адресою покажчика, потім зберігає лічений буфер у власний, зазвичай прихований файл, або виправляє в буфері деякі байти файлу, крім того можливий вплив на результати операції читання. Дані дії особливо небезпечні для програм підтвердження дійсності електронних документів (електронний підпис).
* Запис у файл (функція 40h). Закладка редагує потрібним чином буфер в оперативній пам'яті, або зберігає файл або частину його в приховану область, а потім виконує старе переривання, в результаті чого записується файл зі зміненим змістом, або якимось чином дубльований у прихованій області. Дані такого типу можуть нав'язувати істинність електронного підпису навіть тоді, коли файл було змінено.[23]

Для створення моделі стеганографічної системи буде використано відомий метод НПЗ [8]. Для його реалізації буде використано середовище MathCAD. На рис.3.9. зображена блок-схема кодера методу НЗБ.

Вибравши основні складові для створення стеганографічної системи, можна сформувати механізм роботи моделі РПЗ «стеганографічне перетворення». Основна ідея роботи даного механізму – в я кості секретного повідомлення буде використано програмний код закладки, секретне повідомлення буде впроваджено в обраний контейнер.



Рис.3.8. Схема РПЗ моделі «стеганографічне перетворення»

Для того, щоб цей механізм спрацював, необхідно використати ще одну програмну закладку моделі «спостерігач», яка ініціює подію, після виконання якої приховане повідомлення буде вилучено з контейнера, скомпільоване в виконуючий файл та запущене на виконання. На рис.3.9. показане схематичне відтворення даного механізму.



Рис.3.9. Блок-схема кодера методу НЗБ



Рис.3.10.Блок-схема декодера методу НЗБ

Принцип використання таких РПЗ дозволяє непомітно впровадити закладку будь-якого призначення. Адже об’єкт атаки отримує файл, який на перший погляд не містить шкідливої інформації, а отже не викликає підозри. Схожим принципом керувались при створенні вірусів Win95.CIH, Perrun, про які було вказано в розділі2.

## 3.3. Моделювання системи виявлення та захисту від РПЗ з використанням методів стеганоаналізу

Задача кожного захисника інформації – зменшення ризику або взагалі уникнення реалізації загроз на інформаційну систему. В рамках теми диплому буде розглянуто дещо нетрадиційний спосіб захисту. Оскільки особливу увагу приділено РПЗ та стеганографічним методам їх впровадження, тому для виявлення та запобіганню такого роду атакам буде використано методи стеганоаналізу.

Детальний опис та класифікація всіх методів стеганоаналізу представлена в третьому підрозділі другого розділу, тому основну увагу буде приділено їх практичному використанню.

Для того, щоб уникнути реалізації загрози моделі «стеганографічне перетворення» необхідно ввести додатковий рівень захисту – перевірку за допомогою методів стеганоаналізу всіх потенційно можливих для використання в стеганографічних перетвореннях контейнерів.

Для наочності використаємо метод аналізу гістограм, побудованих на частотах елементів зображення. Оскільки згідно блок-схеми для приховування повідомлення використано синій канал моделі RGB, то побудуємо гістограми частот заповненого та порожнього контейнерів для цієї складової (рис.3.11.). Побудова гістограм здійснюється за допомогою програми MathCAD.

Таку ж гістограму побудуємо для методу псевдовипадкового інтервалу, в якому інформаційні складові розміщені по всьому контейнеру, на відміну від методу НЗБ, де змінені біти розташовані по-порядку, заповнюючи контейнер з початку.



Рис.3.11. Гістограми частот: С-пустого, S-заповненого контейнерів (заповнення методом НЗБ)

Спосіб заповнення впливає на спосіб розподілення частот заповненого контейнера відповідно до порожнього.



Рис.3.12. Гістограми частот: С-пустого, S-заповненого контейнерів (заповнення методом псевдовипадкового інтервалу)

Як видно на рис.3.11 і на рис.3.12. гістограма частот заповненого контейнера швидше прямує до нуля.

Для підтвердження отриманих результатів доцільно буде вирахувати коефіцієнт кореляції між заповненим та порожнім контейнером. Для цього також використаємо програму MathCAD.

, (3.1) - зашифрований контейнер;

, (3.2) - порожній контейнер;

, (3.3) - кореляція пустого контейнера з інформаційним.

Як бачимо коефіцієнт кореляції між порожнім та заповненим контейнером прямує до одиниці.

Ще як один з прикладів використання стеганоаналізу можна продемонструвати за допомогою не спеціалізованої для такої роботи програми Adobe Photoshop CS3. За допомогою цієї програми можна зробити тест на монотонність заповненого та пустого контейнерів (рис.3.13. та рис.3.14.).

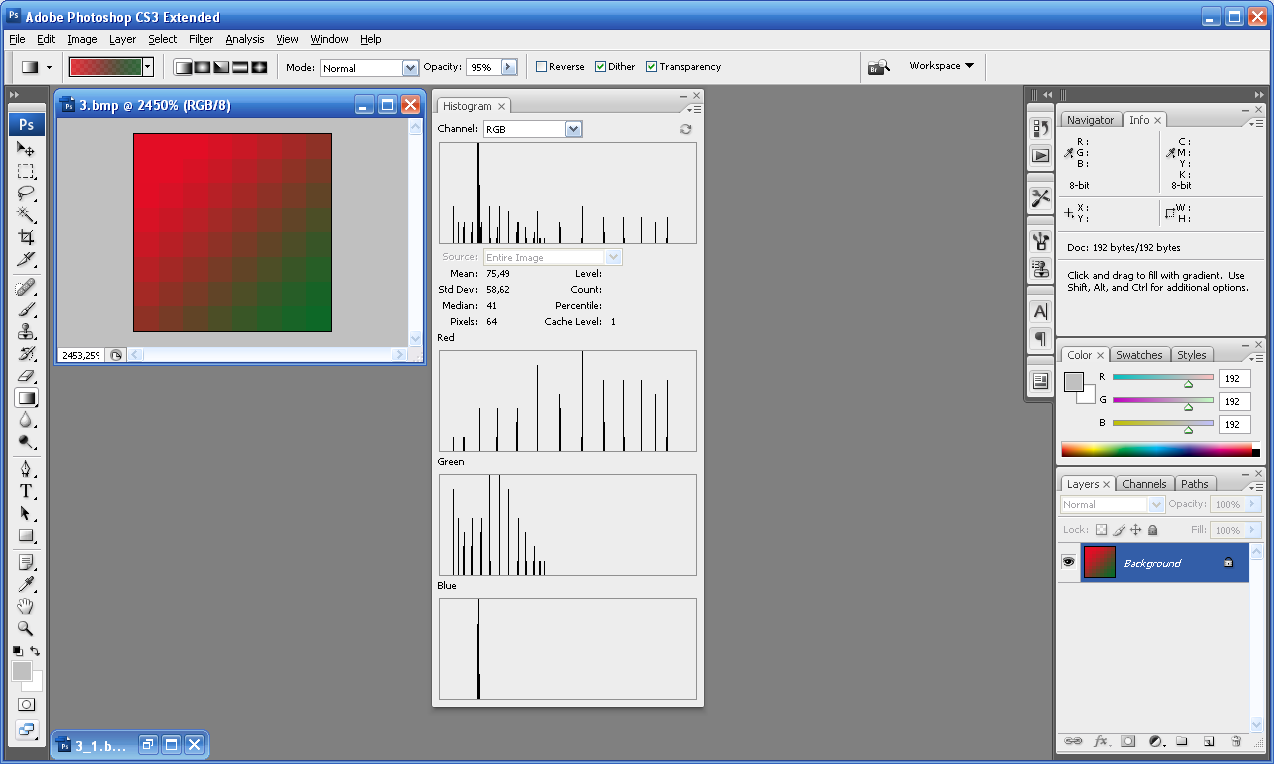


Рис.3.13.гістограма монотонності пустого контейнера

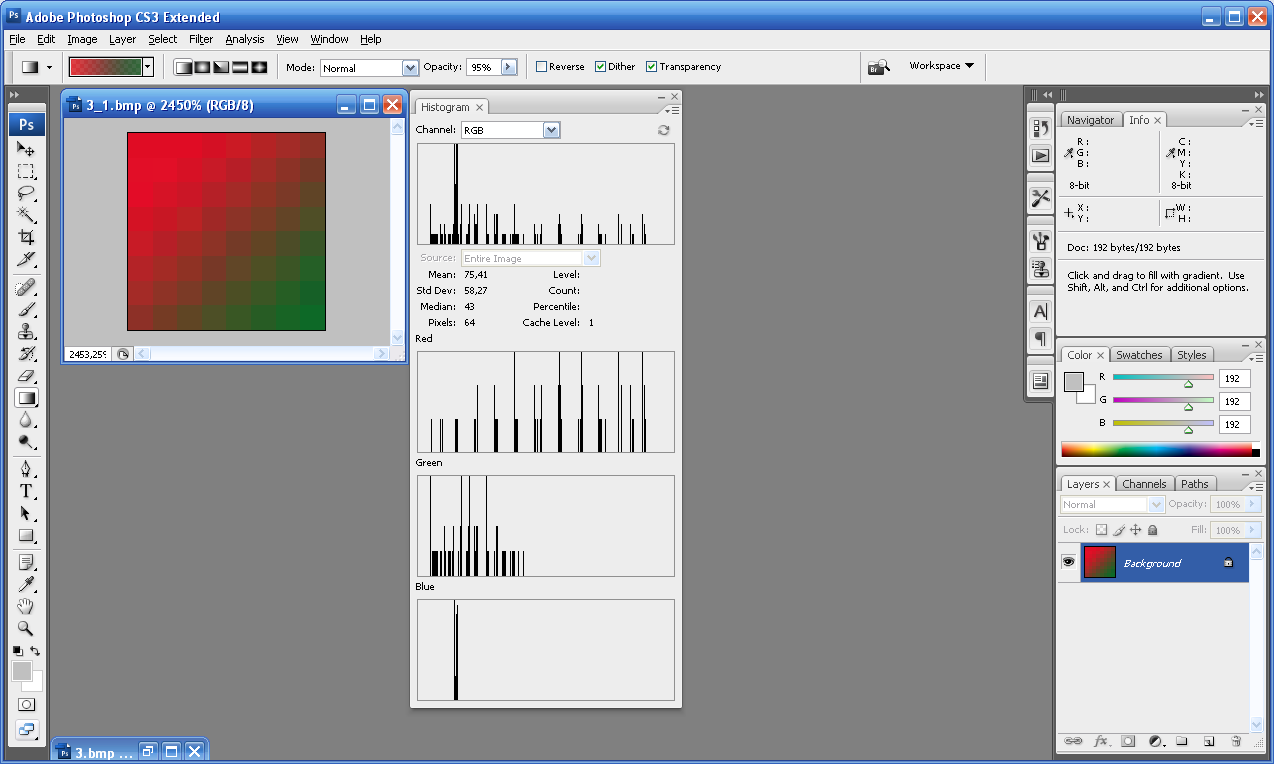


Рис.3.14.гістограма монотонності заповненого контейнера

За допомого функції побудови гістограми для кожного каналу передачі кольору видно, що в місцях заповнення контейнера повідомленням спостерігаються ділянки монотонності, які свідчать про наявність прихованого повідомлення.

Розглянуті методи можуть застосовуватися у вигляді окремого інструментарію, використовуваного стеганоаналітиком або у вигляді модулів у складі складних стеганографічних систем аналізу для забезпечення перевірки графічної інформації в автоматичному режимі. Автоматизація процесу стеганоаналізу дозволить виділяти серед безлічі результатів ті з них, які сприяють мінімізації ймовірності помилки другого роду при заданому рівні ймовірності помилки першого роду, забезпеченню наочності результатів аналізу.

Описані методи аналізу (розділ 2.3) пропонується застосовувати до потенційного контейнера послідовно. Вони представлені в порядку зменьшення ступеня довіри позитивним результатам їх застосування (прихована інформація виявлена), отриманими дослідним шляхом. При отриманні позитивної відповіді в результаті роботи чергового методу аналіз слід зупинити, а аналізований контейнер вважати носієм інформації, прихованої з використанням стеганографічних методів. Внаслідок відсутності позитивної відповіді після застосування всіх перерахованих методів аналізований контейнер слід вважати порожнім.

## 3.4. Організація системи захисту інформації

Головна проблема забезпечення захисту інформації полягає в тому, що існує безліч каналів витоку та каналів для несанкціонованого доступу, тому задача забезпечення інформаційної безпеки потребує комплексного підходу. Отже, проблема створення комплексної системи захисту інформації на об’єкті інформаційної діяльності та живучості мереж в умовах розвитку та впровадження нових інформаційних технологій є актуальною та своєчасною темою дослідження.

Основна задача системи захисту полягає у попередженні та блокуванні максимальної кількості каналів витоку, які існують для інформації, що підлягає захисту.

В рамках даної дипломної роботи буде розглянуто систему захисту інформації, яка здатна буде реагувати на стеганографічні атаки, наприклад такі, як РПЗ моделі «стеганографічне перетворення».

Як було вказано в розділі 1.3 для створення ефективної системи захисту необхідно розглядати комплексний підхід та використовувати методи захисту, які забезпечать різнобічний захист від атак та мінімізують ризик їх реалізації.

Вирізняють такі основні засоби захисту інформації: організаційні, технічні, програмні, криптографічні, стеганографічні. При чому у нашому випадку під стеганографічними засобами захисту інформації розуміються методи стеганоаналізу, які можуть мінімізувати можливість реалізації НСД шляхом використання стеганографічних закладок. Сукупність цих методів реалізує створення ефективної системи захисту інформації (рис.3.15).



Рис.3.15.Схема організації системи захисту інформаційної системи

Стеганографічна складова в сукупності методів захисту інформації відіграє все важливішу роль у зв’язку з постійним розвитком інформаційних технологій. Легковажне ставлення до стеганографії як засобу захисту так і засобу реалізації атак на стеганографічну систему може призвести до негативних наслідків та значних збитків. Адже відсутність повноцінного правового забезпечення провокує використання даних методів в неправомірних цілях (рис.3.16.). Двобічне використання методів стеганографії та стеганоаналізу потребує детального вивчення та затвердження відповідними нормативними актами. Щоб це давало змогу реально усвідомити рівень відповідальності при вчиненні злочинів таким чином та документально підтверджувати такі методи захисту, як, наприклад, використання ЦВЗ, адже це хороше вирішення проблеми захисту авторських прав та гідне бути визнаним на рівні цифрового підпису.

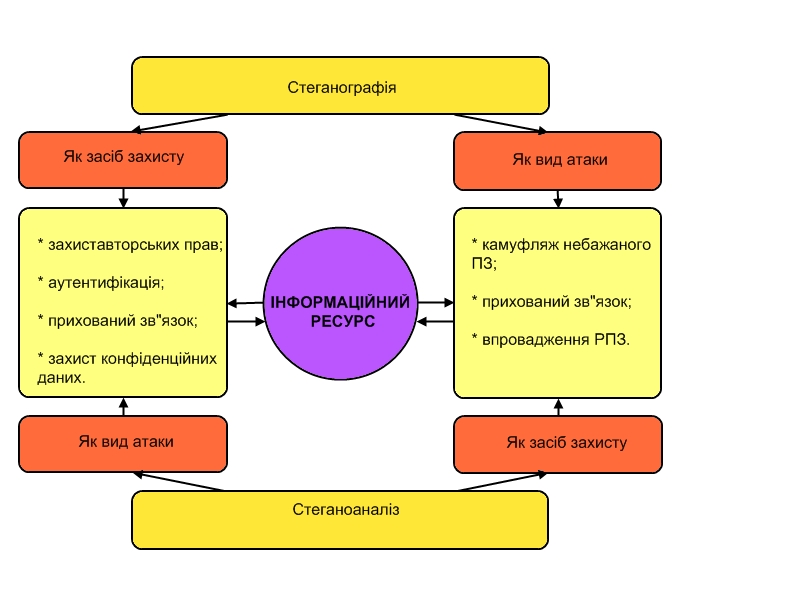


Рис.3.16. Використання стеганографії та стеганоаналізу

Тому задача захисту інформації повинна включати в себе розгляд та детальне вивчення стеганографічних методів та методів стеганоаналізу, бо їх використання дозволяє створювати додатковий рівень захисту. Також це дозволить бути готовими до таких атак як стегозакладки, камуфляж небажаного ПЗ та створювати надійні стеганографічні системи для використання у тих випадках, коли прихований зв’язок є оптимальним.

## 3.5. Висновки по розділу

В розділі проаналізовані та проілюстровані існуючі моделі РПЗ. Також сформована ще одна модель РПЗ, яка використовує такий спосіб впровадження як стеганографічне перетворення.

Створена модель узагальнює можливі способи використання стеганографії в протиправних цілях, основуючись на попередньому досвіді створення таких руйнівних програмних засобів як Win95CIH та W32/Perrun, що в свій час завдали збитків цифровому світу.

В цьому розділі дипломної роботи також змодельована можлива система виявлення та захисту від стеганографічних закладок за допомогою використання стеганоаналізу. Організовано систему захисту інформації, яка включає в себе додатковий рівень – стеганографічний, використання якого дозволить ефективніше забезпечувати інформаційну безпеку.

# ВИСНОВКИ

В дипломній роботі основну увагу приділено стеганографічним перетворенням та методам стеганоаналізу та можливості їх використання для вирішення проблеми захисту інформації в комп’ютерних системах.

Всебічний розгляд стеганографічних перетворень на основі графічних контейнерів дозволяє сформувати загальне уявлення про можливу небезпеку стеганографічнісних закладок, адже з розвитком інформаційних технологій їх реалізація стає дедалі реальнішою. Перші спроби використання таких руйнівних програмних кодів були зафіксовані ще у 1998 при написанні відомого вірусу під кодовою назвою Win95.CIH та у 2002 році при написанні вірусу W32/Perrun.

В дипломній роботі розроблена схема реалізації РПЗ моделі «стеганографічне перетворення» та створена модель використання методів стеганоаналізу для її виявлення. В роботі було визначено основні етапи процедури впровадження стеганографічних закладок в інформаційну систему та було сформовано модель системи захисту інформації для боротьби з РПЗ з використанням стегоаналітичних засобів. В цій системі як окремий і самостійний рівень захисту виокремлено стеганографію, яка охоплює сукупність засобів для реалізації прихованої передачі інформації та методів виявлення таких модифікацій.

Хоча в роботі всі ці методи розглянуті лише на базі графічного контейнеру, що не дозволяє охопити повноту та різноманітність існуючих в наш час методів стеганографії, проте це не впливає значною мірою на висвітлення основної мети та завдань поставлених при написанні цієї дипломної роботи. Також це дає можливість подальшого розвитку та дослідження даної теми. Адже з лавиноподібним розвитком інформаційних технологій інтерес до методів прихованої передачі інформації та її виявлення постійно зростає. Це змушує бути на сторожі під час організації надійної системи захисту.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Virus.Win32.Perrun.a // електронний ресурс [http://www.securelist.com/ru/ descriptions/old20931](http://www.securelist.com/ru/%20descriptions/old20931).
2. ГОСТ 34.003-90 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения".
3. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография – Солон-Пресс, 2009, - 264 с.
4. Дрюченко М.А. Алгоритмы выявления стеганографического скрытия информации в jpeg-файлах //Вест. Воронеж. гос. ун. Системный анализ и информационные технологии. – 2007. - №1. – с.21-30.
5. Закон України “Про основні засади забезпечення кібербезпеки України”.//Відомості Верховної Ради (ВВР), 2017, № 45, ст.403
6. Закон України “Про захист інформації в автоматизованих системах”.// Відомості Верховної Ради (ВВР), 1994, N 31, ст.286.
7. Закон України “Про інформацію”.// Відомості Верховної Ради (ВВР), 1992, N 48, ст.650. Із змінами, внесеними згідно із Законом N 1642-III від 06.04.2000, ВВР, 2000, N 27, ст.213.
8. Казарин О.В. Теория и практика защиты программ. // электронный ресурс - <http://vtabakerke.ru/K/Kazarin/glava1_8.html>.
9. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика – К.: «МК-Пресс», 2006. – 288 с.
10. Криптографічні методи захисту // електронний ресурс [www.bestreferat.ru](http://www.bestreferat.ru/) /referat-194986.html
11. Ліпкан В.А. Національна безпека України: – Навчальний посібник. – К.: Кондор, 2008 – 552с.
12. Мельников В. Защита информации в компьютерных системах // Электронинформ – Финансы и статистика, М: -2004, - 419 с..
13. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності // Журнал Верховної Ради України «Віче»
14. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
15. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.
16. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.
17. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.
18. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.
19. Овсянников В. Скрытая утечка информации // электронный ресурс – 2010, - <http://old.cio-world.ru/it-expert/541220/>.
20. Организационная защита информации //електронний ресурс - <http://itsecblog.ru/organizacionnaya-zashhita/>
21. Современные методы защиты информации. //электронный ресурс - <http://works.tarefer.ru/69/100026/index.html>.
22. Тарасов Д.О., Мельник А.С., Головобородько М.М. Класифікація та аналіз безкоштовних програмних засобів стеганографії., - 2010.
23. Титоренко Г.А. Информационные технологи управления //Учебное пособие для вузов -2-е изд.,доп. – Юнити-Дана, М: - 2003, - 439 с.
24. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. // Сборка лекций.
25. Шангіна Л.В. Національна безпека і оборона. //Журнал українського центру економічних і політичних досліджень імені О.Разумкова – УЦПД: 2001 - №1(13) – с.17,29.
26. Швидченко И.В. Методы стеганоанализа для графических файлов // «Штучний інтелект», Институт кибернетики имени В.М. Глушкова НАН Украины: - К.:2010 - №4.