18. Сидельников В.М., Шестаков С.О. О системе шифрования, построенной на основе обобщенных кодов Рида-Соломона.//Дискретная математика.-1992.-Т.4.№3.-С.57-63.

19. Кузнецов А.А., Евсеев С.П. Разработка теоретико-кодовых схем с использованием эллиптических кодов. // Системи обробки інформації. – Харків: ХВУ. –2004 – Вип. 5. – С. 127-132.

УДК 004.681.3

Гулак Г.М.
Державний університет
інформаційно-комунікаційних технологій

ХАРАКТЕРИСТИКА НЕБЕЗПЕЧНИХ ВІДМОВ ЗАСОБІВ, ЩО РЕАЛІЗУЮТЬ СТЕГАНОГРАФІЧНІ МЕТОДИ ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

Ретельно обґрунтовані та досліджені методи перетворення інформації в стеганографічних системах (далі – стегосистемах) можуть не досягати поставленої мети, якщо апаратно-програмні засоби, які їх реалізують не відповідають певному рівню функціональної безпеки [1]. Це означає, що конструктивні, алгоритмічні и схемно-технічні рішення, обрані під час проектування цих засобів, не адекватні можливим збоям технічних та програмних компонент, не здатні знизити до нуля ймовірність проведення ефективної атаки на стегосистему у випадку ситуації з відмовою [2].

Оцінювання рівня безпеки та надійності засобів, що реалізують стеганографічні перетворення (ЗРСП), здійснюється шляхом проведення їх інженерного аналізу, у рамках якого виконуються реєстрація, вимірювання, впорядкування, узагальнення реальних характеристик ситуацій з відмовами та визначення їх наслідків для безпеки інформації. У підсумку проведення інженерного аналізу мають бути зроблені висновки щодо достатності обраних рішень, а також, за необхідності, сформовані пропозиції щодо вдосконалення функціональної безпеки ЗРСП.

При цьому функціональну безпеку ЗРСП на відміну від [1] будемо розуміти не в сенсі катастрофічності наслідків відмови взагалі, а лише у вузькому змісті інформаційної безпеки. Аналогічно визначенням стандартів [3] під функціональною безпекою ЗРСП будемо розуміти їх здатність тривало правильно виконувати завдання за призначенням, не утворюючі, у разі виходу з ладу їх компонентів, передумов для витоку інформації з обмеженим доступом, іншої критичної інформації. Таким чином можливо сформулювати у якості головного завдання інженерного аналізу ЗРСП визначення складових функціональної безпеки, рівня захищеності від виходу з ладу компонентів та ступеню впливу ймовірних відмов на стеганографічні якості цих засобів.

Як і у випадку інженерних досліджень надійності будь-якої складної системи [4,5], звичайно, інженерний аналіз ЗРСП повинен передбачати виявлення та оцінку загроз безпеці інформації з боку апаратних компонент, програмного забезпечення (ПЗ) та людського фактору.

Звернемо увагу, що введене поняття функціональної (інформаційної) безпеки стегосистеми та характеристики її рівня перекликаються з показниками надійності звичайної технічної системи. Суттєва різниця полягає у тому, що показники надійності враховують будь яки відмови та збої системи, а характеристики інформаційної безпеки ЗРСП повинні виходити тільки з тих відмов, наслідком яких може бути суттєве погіршення стеганографічних властивостей цих засобів.

Слід зазначити, що у наукових публікаціях [6,7,8] приділяється недостатня увага інженерно-технічним аспектам створення апаратно-програмних ЗРСП, с точки зору забезпечення надійності їхнього функціонування та безпеки інформації в умовах виникнення апаратних та

програмних збоїв та відмов. Водночас, потреби практики нагально потребують розробки та наукового обґрунтування методів та принципів побудови надійних ЗРСП.

Викладене обумовлює актуальність проведення досліджень у галузі інженерного аналізу відповідних ЗРСП.

Безпеку стегосистеми будемо визначати по відношенню до ймовірних загроз та можливих їх реалізацій, тобто конкретних атак на систему. При цьому, в випадку відмов ймовірні загрози безпеці стегосистеми характеризують можливі наслідки для її стійкості, а також загальні можливості потенційного зловмисника щодо порушення конфіденційності, цілісності (імітозахищеності, достовірності) інформації, а не конкретні методи (алгоритми) їх здійснення.

Вочевидь, вихідні дані для проектування відповідних засобів серед інших вимог повинні включати формальний опис порушника системи безпеки, що атакує стегосистему (інакше – зловмисника). Під зловмисником будемо розуміти особу, яка оснащена технічними та програмними засобами та володіє певним обсягом спеціальних знань. Метою його діяльності є пошук слабких місць стегосистеми для:

- виявлення факту та умов застосування стегосистеми у процесі утворення прихованого каналу передачі інформаційних повідомлень;
- проведення пасивних атак на стегосистему для ознайомлення зі змістом конфіденційної інформації;
- здійснення маніпуляцій з даними, порушення їх цілісності задля вчинення підлогу, передачі викривлених повідомлень (активні атаки);
- замаскованого блокування каналу передачі даних, що утворюється за допомогою стегосистеми, шляхом створення та пересилання фальшивих повідомлень (стеганограм - «фантомів»), яки за зовнішніми ознаками та змістом майже не відрізняються від істинних (активні атаки).

За силою атаки, перша є найслабкішою, оскільки практично не потребує розкриття особливостей побудови стегосистеми, остання – найсильніша тому, що для її проведення необхідно достеменно знати усі аспекти побудови та функціонування стегосистеми.

Оскільки для стегосистем діючими нормативними документами моделі порушників не визначені, уявляється доцільним скористатися відомими моделями для криптосистем, як такими, що практично адекватно відповідають умовам та цілям застосування стегосистем. А саме, будемо відрізняти чотири типи порушників залежно від його можливостей атакувати стегосистеми:

I. Випадковий порушник системи безпеки, що володіє звичайною обчислювальною технікою, комунікаційним обладнанням, програмним забезпеченням та «озброєний» загальними відомостями з питань захисту інформації та безпеки телекомунікацій. Будемо вважати, що його обчислювальні можливості характеризуються функцією, що залежить від часу, а саме - $W_I(t)$;

II. Порушник – хакер, який добре знає особливості побудови та функціонування комплексів захисту інформації, а також методи подолання захисних механізмів, працює з обмеженими матеріальними, фінансовими та часовими ресурсами, використовуючи для проведення атак найбільш потужну загальнодоступну обчислювальну техніку та спеціальні програмні засоби (у т.ч., створені власноруч). Нехай $W_{II}(t)$ – характеристика його обчислювальних можливостей;

III. Порушник корпоративного типу здійснює пошук вразливості на професійному рівні, додатково до можливостей попереднього рівня має матеріальну та фінансову підтримку потужної бізнес – структури. Його обчислювальні можливості визначаються функцією часу $W_{III}(t)$;

IV. Порушник користується науковим, технічним та фінансовим потенціалом спеціальної служби розвиненої країни світу. $W_{IV}(t)$ – характеристика його обчислювальних можливостей.

Вочевидь, що функції $W_I(t), W_{II}(t), W_{III}(t), W_{IV}(t)$ зростаючі, при цьому для $\forall t>0$ має місце нерівність:

$$W_I(t)<W_{II}(t)<W_{III}(t)<W_{IV}(t)$$

Можливо відмітити, що зростання вимог до кожного наступного рівня у наведеній класифікації суттєво скорочує коло реально можливих порушників.

Також зауважимо, що відмови ЗРСТ, внаслідок яких підвищується імовірність реалізації ризику проведення ефективних атак, наприклад, тільки з боку порушників типу IV, можуть мати менш фатальні наслідки для суб'єктів господарювання, які користуються стегосистемою, ніж у випадку, коли відмови ЗРСТ створюють передумови для проведення атак порушником типу I. Але у той же час для користувача ЗРСП на державному рівні відмова засобу, внаслідок якої стегосистема може стати об'єктом атаки навіть порушника типу III є взагалі неприйнятною.

Цей приклад свідчить про залежність наслідків відмови від типу користувача системи, що також відрізняє поняття інформаційної безпеки засобу від поняття надійності.

З метою впорядкування наслідків відмов систем залежно від ступеню їх впливу на якість функціонування програм або даних об'єкта управління розглядається [1] п'ять категорії ситуацій з відмовами. При цьому рівень якості ПЗ, необхідний для їх безпечного функціонування, визначається виходячи з небезпеки відмов та можливих наслідків для програм, системи та користувачів.

Якість функціонування систем та ПЗ в цих умовах, збитки або певні втрати від відмов характеризують категорії *A* (катастрофічна), *B* (небезпечна), *C* (суттєва) и частково *D* (несуттєва). Категорія *E* - невпливова ситуація з відмовою, внаслідок якої практично не змінюються функціональні та експлуатаційні характеристики, суттєво не зростає робоче навантаження на персонал.

У випадку ЗРСП зазначені категорії ситуацій з відмовами доцільно інтерпретувати як різні ступені втрат внаслідок впливу відмови на інформаційну безпеку відповідного засобу (утворення умов для реалізації ризику успішної атаки на стегосистему).

Позначимо через $W_I(T), W_{II}(T), W_{III}(T), W_{IV}(T)$ обчислювальні потужності кожного з потенційних порушників за деякий час *T*.

Будемо вважати, інформація, що підлягає захисту за допомогою ЗРСП, безпека якого підлягає оцінці, має деякий середній рівень вартості [9]. Це припущення з одного боку робить її привабливою для усіх категорій порушників, з іншого – встановлює обмеження на витрати, пов'язані з побудовою захисних механізмів [6].

Початкову складність (до виникнення будь якої відмови) проведення найбільш ефективної стегоаналітичної атаки з метою встановлення факту застосування стегосистеми для утворення прихованого каналу передачі інформаційних повідомлень позначимо через $V>W_{IV}(T)$, після відмови цю величину будемо позначати як V_F: $V_F. \le V$

Тоді до множини *E* віднесемо усі подій з відмовами, що не впливають на рівень безпеки ЗРСП, що підлягає оцінці. До множин *D,C,B* та *A* віднесемо ті події з відмовами, внаслідок початкова складність проведення найбільш ефективної атаки з метою встановлення факту застосування стегосистеми для утворення прихованого каналу передачі інформаційних повідомлень може бути знижена до рівнів V'_F, V''_F, V'''_F, V''''_F відповідно:

$$\begin{aligned} A&=\{a_F: V''''_F \le W_I(T)\} \\ B&=\{b_F: W_I(T)<V'''_F \le W_{II}(T)\} \\ C&=\{c_F: W_{II}(T)<V''_F \le W_{III}(T)\} \\ D&=\{d_F: W_{III}(T)<V'_F \le W_{IV}(T)\} \\ E&=\{e_F: V_F=V\} \end{aligned} \qquad (1)$$

При цьому логічно вважати, що найгіршим, або інакше – катастрофічним випадком є відмова, внаслідок якої атака на стегосистему може бути проведена випадковим порушником.

Вочевидь з (1) слідує, що множини E,D,C,B та A не перетинаються, тому для ймовірності $p_{від}$ виникнення в ЗРСП відмови маємо: $p_{від}=p_e+p_d+p_c+p_b+p_a$, де складові правої частини рівняння є ймовірностями належності відмови до однієї з п'яти визначених множин.

У визначених умовах у разі $n \cdot p_{від} \to \lambda_{від}=\lambda_e+\lambda_d+\lambda_c+\lambda_b+\lambda_a$ при $n \to \infty$ для оцінки розподілу відмов, що мають наслідком погіршення стеганографічних властивостей, можливо скористатися апроксимацією у вигляді розподілу Пуассона:

$$e^{-(\lambda_d+\lambda_c+\lambda_b+\lambda_a)} \cdot \frac{\lambda_d^j \cdot \lambda_c^k \cdot \lambda_b^l \cdot \lambda_a^m}{j!\cdot k!\cdot l!\cdot m!}$$

Зокрема, для ймовірності надійної роботи з точки зору інформаційної безпеки $p_{ніб}$ маємо:

$$p_{ніб} = e^{-(\lambda_d+\lambda_c+\lambda_b+\lambda_a)}$$

З урахуванням викладеного, у підсумку проведення інженерного аналізу ЗРСП мають бути оцінені відповідні параметри та розрахована ймовірність небезпечних ситуацій у випадку виникнення відмов.

Список літератури.

1. *Липаев В.В.,* Технологические процессы и стандарты обеспечения функциональной безопасности в жизненном цикле программных средств, Информационный бюллетень "Jet Info 08(135)/2004", www.jetinfo.ru

2. *Гулак Г.М.* Оцінка ризиків у ході проведення інженерного аналізу безпеки стеганографічних систем/ Защита информации: сборник научных трудов.– Киев, НАУ, 2008. С.259-264

3. *ГОСТ 27.002-89.* Надежность в технике. Основные понятия. Термины и определения. - М.: Издательство стандартов, 1989. –37с.

4. *ДСТУ 3524-97 (ГОСТ 27.205-97).* Надійність техніки. Проектна оцінка надійності систем з урахуванням технічного і програмного забезпечення та оперативного персоналу. Основні положення. - К.: Держстандарт України, 1999. –21с.

5. *Иванов М.А.* Криптографические методы защиты информации в системах и сетях. - М.: КУДИЦ-ОБРАЗ, 2001. -368с.

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

7. Основы компьютерной стеганографии: Учеб. Пособие для вузов/ Аграновский А.В., Девянин П.Н., Хади Р.А., Черемушкин А.В. – М.: Радио и связь, 2003. – 152с.: ил.

8. *Методы и средства защиты информации,* В 2-х томах/ Ленков С.В., Перегудов Д.А., Хорошко В.А., Под ред. В.А. Хорошко. – К.: Арий, 2008. – Том II. Информационная безопасность. –344с., ил.

УДК 681.3.06

Терейковський І.А.
Державний університет
інформаційно-комунікаційних технологій

МЕТОДИ КОННЕКТЕВІЗМУ ТА ЗАХИСТ В НИХ

Сучасний стан розвитку комп'ютерних систем і мереж характеризується підвищенням вимог до рівня захисту інформації, який вже практично не можливо забезпечити за допомогою комплексних систем захисту інформації, контури контролю та управління яких використ-