УДК 004.056

Дрєєв О.М., Дрєєва Г.М.
Кіровоградський національний технічний університет

Визначення оптимальної кратності резервування інформації в однорангових мережах з ненадійними вузлами

Вступ. Розглянуто однорангову мережу для розподіленого захищеного збереження файлів. Визначається оптимальна фрагментація файлів та дублювання інформації в умовах нестаціонарності зв'язку окремих хостів.

Прийнято схему за якою файли в мережі зберігаються розподілено частинами, при цьому прийнято заходи що до неможливості розшифрування окремого фрагменту файлу. Для отримання розшифрованої інформації потрібно мати повний набір шифрованих фрагментів файлу. Ненадійність вузлу мережі є ймовірність того, що хост з комплексу можливих причин може стати недоступним — p. Приймемо, що файл мережі може бути скомпрометовано, якщо на окремому вузлі зберігається одночасно всі фрагменти цього файлу. Ймовірність такої події позначено як q, величина є розрахованою при умові випадкового розподілення фрагментів файлу. Також потрібно врахувати ймовірність події, коли відсутній доступ до повного набору фрагментів файлу або файл було скомпроментовано — μ.

Більшість з вказаних величин є властивостями конкретної мережі, або є результатом розрахунків. Тому, як засоби керування надійністю мережі є значення K — кількість фрагментів, на які поділяється кожен файл; D — коефіцієнт дублювання інформації, використовується для забезпечення цілісності інформації в разі втрати зв'язку з окремим хостом мережі; n — кількість активних хостів однорангової мережі.

Мета: визначити значення параметрів K, D при яких мінімізується ймовірність порушення інформаційної цілісності μ.

У випадках використання однорангових нестаціонарних мереж, коли кожен хост може перервати зв'язок або змінити своє фізичне або адресне положення, використання адресації фрагментів за допомогою хешування є недоцільним. В цьому випадку є застосовним випадкове розташування фрагментів із широкомовними запитами для їх збирання до єдиного файлу. Завдяки цьому, при аналізі розташування фрагментів, можна використовувати математичний апарат теорії ймовірності.

Ймовірність компрометації файлу q. В разі розбиття файлу K фрагментів, ймовірність того, що фрагмент міститься на певному хості складає D/n. Тоді ймовірність присутності повного набору K фрагментів на одному вузлі є $q=(D/n)^K$. В такому випадку, зловмисник матиме можливість організації атак на дешифрування цілісного файлу.

Ймовірність компрометації або втрати файлу μ. Дана величина є сукупністю можливих подій, коли наступає компрометація або втрата файлу. За правилами дій з ймовірностями, можна використати протилежну подію, як добуток ймовірності, що файл не буде скомпрометовано та ймовірності того, що файл не буде втрачено. Для факту втрати одного з

файлів, достатньо щоб “одночасно” було втрачено зв’язок з більше ніж D хостів. Ймовірність такої події складає:

$$P = \sum_{m=D}^{n} C_n^m p^m (1-p)^{(n-m)}.$$

Тепер з ймовірностей P та q, можна виразити ймовірність порушення роботи системи:

$$\mu = 1-(1-P)(1-q),$$

або

$$\mu(n,K,D) = 1-\left(1-\sum_{m=D}^{n} C_n^m p^m (1-p)^{(n-m)}\right)\left(1-(D/n)^K\right).$$

Приклад: маємо мережу з n=20 комп’ютерів для яких ймовірність вийти з мережі складає p=0,08. Тоді ймовірність роботи системи без відмов залежить від D та K. Цю залежність показано на рисунку 1.

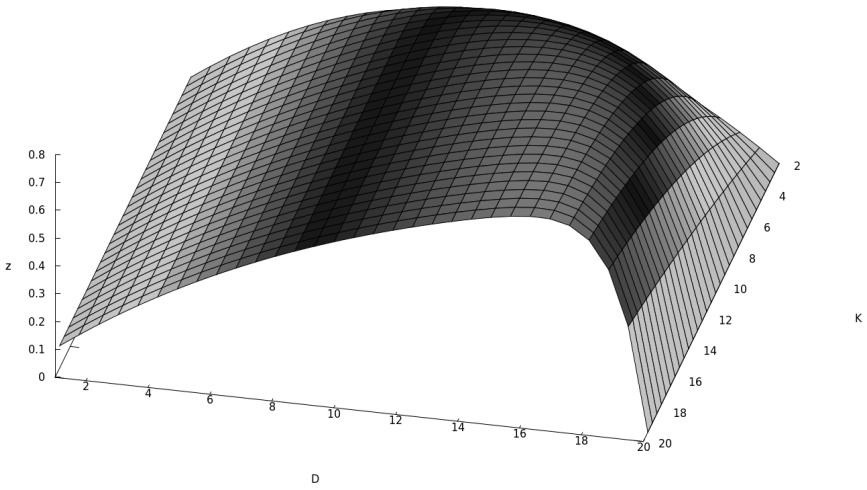

Рисунок 1 – Залежність ймовірності безвідмовного доступу до файлів від резервування та фрагментації файлів в розподіленій системі збереження

Висновки. У випадках ненадійності хостів, використання дублювання та фрагментації файлів дозволяє визначити параметри оптимального функціонування за надійністю доступу та захисту даних.

Список використаних джерел

1. *Дрєєв О.М. Методи підвищення якості обслуговування у телекомунікаційних системах та мережах / О.М. Дрєєв, Г.М Дрєєва, О.А. Смірнов // Зб. тез доп. Акад. внутрішніх військ МВС України «Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку» 20-21 березня 2013р. — Х. : АВВ. — 2013. — С. 18-19.*
2. *Смирнов А.А. Проблемы анализа и оценки рисков информационной деятельности/ А.А. Смирнов, А.В. Коваленко, Н.Н. Якименко, А.П. Доренский// Системи обробки інформації : зб. наук. праць. — 2016. — № 3. — С. 40-42.*