Формування множини параметрів для класифікації службової інформації

Conference Paper · September 2024

CITATIONS
0

READS
2

1 author:

Yurii Dreis
Mariupol State University
92 PUBLICATIONS **40** CITATIONS

SEE PROFILE

Дрейс Юрій
кандидат технічних наук, доцент,
доцент кафедри системного аналізу та інформаційних технологій,
Маріупольський державний університет
ORCID: 0000-0003-2699-1597

ФОРМУВАННЯ МНОЖИНИ ПАРАМЕТРІВ ДЛЯ КЛАСИФІКАЦІЇ СЛУЖБОВОЇ ІНФОРМАЦІЇ

За останні роки стрімко зростають обсяги службової інформації (СІ), що накопичуються, зберігаються та використовуються у професійній діяльності. При цьому надмірна концентрація СІ спеціального призначення та приналежності, а також різке розширення кола користувачів, що мають безпосередній доступ до цієї інформації, породжує проблему забезпечення її захисту від можливої втрати чи розголошення. Підвищення рівня складності методів і засобів добування СІ, а також існуючі способи використання інформаційних технологій призводять до появи реальних та потенційних загроз в інформаційній сфері. Реалізація цих загроз може призвести до витоку СІ та нанесення можливої шкоди державі. Величина такої шкоди зазвичай важко формалізована, нечітко визначена і, при необхідності визначення її у процедурі віднесення відомостей до СІ, має містити набір базових ідентифікуючих та оціночних параметрів. Одним із підходів до вирішення такого завдання є використання відповідних моделей, методів та систем, які основі на використання нечітких множин, орієнтованих на обробку слабо структурованих даних з метою встановлення фактів нанесення шкоди, наприклад, від витоку ДТ [1-3], персональних даних [2-5] або СІ [5-6]. Виходячи з цього, розробка моделей, які дозволяють формалізувати процес класифікації СІ за набором базових параметрів представлення можливої шкоди державі (установі, відомству) у разі її витоку є актуальним науково-практичним завданням.

Для вирішення поставленого завдання пропонується математична модель формування величин (як базова кортежних модель), основу якої становить кортеж, що складається з ідентифікатора (ІД) виду СІ як інформації з обмеженим доступом (ІзОД), а також інші компоненти, як підмножини [1-6]: нечітких (лінгвістичних) еталонів [1-3]; поточних значень нечітких параметрів [2-4]; базових детекційних правил [3-5]; можливих ідентифікаційних та оціночних параметрів [4-6];

Так відповідно до законодавства інформація («*information*» І) за порядком доступу поділяється на відкриту («*public information*») РІ та ІзОД («*classified information*») СІ. Для формалізації процесу формування вказаних компонент введемо множину можливих видів СІ, виток (втрата чи розголошення) якої може нанести шкоду національній безпеці у визначеному часовому проміжку τ_f (f – номер часового проміжку, $f = \overline{1,max_\tau}$), тобто [1-3]:

$$CI^{\tau_f} = \{\bigcup_{i=1}^{n} CI_i^{\tau_f}\} = \{CI_1^{\tau_f}, CI_2^{\tau_f}, ..., CI_n^{\tau_f}\},\ (i = \overline{1,n}), \quad (1)$$

де n – кількість можливих видів ІзОД, кожен з яких відображається узагальненим кортежем:

$$CI_i^{\tau_f} = \left\langle CI_i, P_i, T_i^e, P_i^{\tau_f}, DR_i \right\rangle, \quad (2)$$

в якому [1]: CI_i – ІД i-го виду ІзОД; P_i – підмножина можливих параметрів, що використовуються для визначення i-го виду ІзОД; T_i^e – підмножина можливих нечітких (лінгвістичних) еталонів, що відображають судження експерта відносно наявності базових параметрів можливої шкоди (по типу процедури віднесення відомостей до ІзОД) із підмножини P_i для обмеження доступу; $P_i^{\tau_f}$ – підмножина поточних значень нечітких параметрів, сформованих на основі T_i^e у момент часу τ_f ($f = \overline{1,max_\tau}$) за часовий проміжок $\tau_h = \tau_f - \tau_{f-1}$; DR_i – підмножина базових детекційних правил (причинно-наслідкових і просторово-часових характеристик та ознак І), що стали основною для побудови узагальненої схеми класифікації інформації за визначеним порядком та ступенем обмеження доступу до видів ІзОД [4-6]: за порядком доступу; за правовим режимом; за правом доступу; за наявним переліком або зводом відомостей; за грифом обмеження доступу матеріального носія інформації; за вимогами обмеження доступу (трискладовий тест); за видом діяльності та інші.

Таким чином, запропонована базова кортежних модель формування набору базових компонент, яка за рахунок формалізації процедури обмеження доступу до інформації, дозволяє сформувати набір приватних кортежів, що відображають процеси класифікації ІзОД, наприклад службової інформації, для становлення базових параметрів представлення шкоди національній безпеці України від її витоку у заданому часовому проміжку.

Список використаної літератури:

1. Yu. Dreis, et al., Model to Formation Data Base of Internal Parameters for Assessing the Status of the State Secret Protection. *Cybersecurity Providing in Information and Telecommunication Systems.* Vol. 3654. 2024. 277-289.

2. O. Korchenko, Yu. Dreis, et al., Method of Fuzzy Classification of Information with Limited Access. *2nd International Conference on Advanced Trends in Information Theory*. 2020. 255–259. doi: 10.1109/ATIT50783.2020.9349358

3. Yu. Dreis, et al., Restricted Information Identification Model. *Cybersecurity Providing in Information and Telecommunication Systems*. Vol. 3288. 2022. 89–95.

4. О. Корченко, Ю. Дрейс, І. Лозова, Модель та метод оцінки ризиків захисту персональних даних під час їх обробки в автоматизованих системах. *Захист інформації*. 2016. Т.18 (1). С.39-47. doi: 10.18372/2410-7840.18.10111

5. Корченко О. Г, Дрейс Ю. О. Охорона конфіденційної інформації підприємства: навч. посіб. Житомир: ЖВІ НАУ, 2011. 172 с.

6. Дрейс Ю. О. Службова інформація: розмір істотної шкоди у разі розголошення. *ITSec*: XI міжнар. наук.-техн. конф. Київ, 2021. С.7-8.