УДК 004.771

МОДЕЛЬ КОРИСТУВАЧА ЗАХИЩЕНОЇ МЕРЕЖІ НА ОСНОВІ КЛАСТЕРНОГО АНАЛІЗУ

Д.В. Кусков[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут»*

Анотація

В роботі побудовано модель користувача системи контролю доступу до мережі за допомогою кластерного аналізу.

Ключові слова: захист мережі, модель користувача, кластерний аналіз, інформаційна безпека.

Вступ

При дослідженні комплексної системи контролю доступу на основі підходу NAC було виявлено, що рішення щодо надання користувачу доступу здійснюється на основі політики, заданої в мережі. Користувач проходить перевірку на задоволення встановленій політиці та після цього здійснює процес автентифікації і отримує доступ до мережі або до серверів відновлення. Тому метою даної роботи є розробка моделі користувача на основі його дій в мережі для визначення його звичної поведінки та подальшого виявлення аномальних дій даного користувача у мережі.

1. Методика досліджень

При побудові моделі було проаналізовано найважливіші параметри роботи користувача в мережі та вибрані ті з них, які найкраще будуть описувати його дії та виявляти аномалії:

- ID користувача;
- Тип операційної системи;
- Тип програмного забезпечення;
- Номер мережевого порту;
- Тривалість сеансу;
- Об'єм трафіку.

Для кожного із 4 користувачів були отримані дані декількох десятків сеансів та занесені у таблиці для кожного користувача окремо. Параметри, такі як, тип ОС, тип ПЗ та номер порту, значення яких описуються словами чи мають невпорядковані значення, були проіндексовані для подальшої зручності у проведенні кластерного аналізу.

Далі було проведено процедуру ієрархічного кластерного аналізу за допомогою пакету IBM SPSS. Так як вихідні змінні мають різну природу, перед цим потрібно стандартизувати вихідні дані. Для аналізу було вибрано метод найближчого сусіда, у якому відстань між двома кластерами визначається відстанню між двома найбільш близькими об'єктами (найближчими сусідами) в різних кластерах. У якості метрики використовуємо Евклідову метрику.

[a] d.kusaff@gmail.com

Суть процедури кластерного аналізу полягає в тому, що постійні та схожі дії користувача будуть об'єднані у кластер, що дозволить побудувати профіль його нормальних дій, а усе що буде входити у кластер на дуже пізніх етапах кластеризації, буде вважатися як аномальна дія, непритаманна даному користувачу.

2. Результати досліджень

При впровадженні даної моделі, продемонстровано процедуру поетапного об'єднання сеансів кожного користувача у кластери, що дозволяє визначити індивідуальні профілі поведінки користувачів у мережі на основі заданих параметрів. Результати показують, що при виникненні одиночної події, яка не схожа на інші притаманні даному користувачу, ця подія увійде у кластер на останньому етапі кластеризації.

Висновки

Було розроблено модель користувача на основі його дій в мережі для визначення його звичної поведінки, яка може бути використана у сучасних системах контролю доступу користувачів до корпоративної мережі.

Перелік використаних джерел

1. Мандель И. Д. Кластерный анализ. – М.: Финансы и статистика, 1988. – 176 с.
2. Наследов А. SPSS 19. Профессиональный статистический анализ данных. – Спб.: Питер. – 2011 – 400 с.