Секция «Вычислительная математика и кибернетика»

Разработка подсистемы обнаружения внутренних утечек корпоративной информации с использованием подхода иммунных сетей

Тихомиров Александр Владимирович
Аспирант
Национальный исследовательский ядерный университет «МИФИ», Факультет кибернетики, Москва, Россия
E-mail: Al.V.Tikhomirov@gmail.com

Проблемы, связанные с защитой внутренней корпоративной информации от ее утечки наружу, достаточно актуальны на сегодняшний момент в связи с высоким ростом ценности корпоративной информации для конкурентов.

В данном исследовании обсуждаются внутренне утечки информации - утечки через собственных сотрудников (инсайдеров), связанные с ненадлежащим использованием доступной им по должностным обязанностям информации. На текущий момент в области обеспечения безопасности информации имеется достаточное количество средств, позволяющих свести к минимуму вероятность утечки при внешней атаке. Однако существующие системы малоэффективны в решении задач выявления утечек в результате действий инсайдеров.

При построении систем, направленных на защиту от утечек информации, систем обнаружения вторжений, а также антивирусных систем в основном используются два метода анализа:

- сигнатурный анализ;
- динамический анализ.

В данном исследовании был использован одним из возможных способов решения рассматриваемой задачи - применение динамического подхода, основанного на поведенческом анализе операций сотрудников при работе с информационной системой, с использованием методов иммунных сетей – высокопараллельных структур для обработки данных, в которых реализованы механизмы обучения, памяти и ассоциативного поиска для решения задач распознавания и классификации[2]. Для построения профилей поведения пользователей системы предлагается анализировать действия, выполняемые сотрудниками при работе с системой. Для этого предлагается использовать модификацию метода секвенционного анализа Apiori, адаптированную для работы на потоке данных. На этом этапе выполняется:

- кодирование входного потока (на основе бинарного алфавита);
- асинхронное сжатие потока с задержка.

После получения для каждого пользователя набора профилей, характеризующих его нормальное поведение (в котором отсутствуют действия, направленные на кражу информации), необходимо проверить его дальнейшие действия на отсутствие соответствий с выработанной моделью.

Для проверки применимости разработанной методики был создан прототип подсистемы обнаружения внутренних утечек информации. По результатам апробации разработанного прототипа с использованием выборочного набора данных можно выделить следующие характеристики предлагаемой методики:

- самоадаптируемость под изменяющееся нормальное поведение сотрудника (например, связанное с изменяющимися должностными обязанностями);
- пассивный режим противодействия утечкам;
- возможность обработки асинхронного потока от нескольких источников.

Т.о., можно сделать вывод о применимости подхода на основе поведенческого анализа с применением методов иммунных сетей для решения задачи обнаружения внутренних утечек корпоративной информации.

Литература

1. Дасгупта Д. Искусственные иммунные системы и их применение./ Пер. с англ. Под ред А.А.Романюхи. – М.: ФИЗМАТЛИТ, 2006. – 344 с.
2. Leandro N. De Castro, Fernando J. Von Zuben Immune and Neural Network Models: Theoretical and Empirical Comparisons, International Journal of Computational Intelligence and Applications (IJCIA), 1(3), p. 239-257, 2001.
3. Машечкин И.В. и др. Мониторинг и анализ поведения пользователей компьютерных систем. – МГУ им. Ломоносова, 2008.