Ю. А. Горбунов, **И. А. Жуйков**, **Е. Л. Кротова** (Пермь, ПГТУ)**. Выявление злоумышленника статистическими методами в компьютерных системах.**

Задача аутентификации — подтверждения подлинности идентификатора объекта — последние 5 лет является одной из самых обсуждаемых практически на всех конференциях по информационной безопасности международного и национального уровня [1]. Предложенный в работе способ заключается в построении модели поведения злоумышленника в системе с помощью существующих статистических методов.

Построение адекватной модели злоумышленника сведено к моделированию двумерного случайного вектора, компоненты которого независимы и принадлежат классу строго устойчивых распределений. Для определения параметров случайного вектора используем подход, предложенный в [2]. Моделируем необходимое число стандартных нормальных величин на основе псевдослучайных последовательностей, переходим к инвариантам распределения, исключая мешающий масштабный параметр, который будет оценен с помощью метода квантилей. Выделяем из наблюдений строго устойчивую компоненту, исключая нормальную составляющую смеси распределений, и проверяем простую гипотезу о параметре устойчивости с помощью метода Колмогорова–Смирнова. Вычисляя значения локального наклона по Бахадуру, проверяем, достаточен ли объем обучающей выборки. Проведенная процедура позволяет построить профиль легального пользователя. При нарушении критического числа эвристических правил проверяем гипотезу о принадлежности текущего профиля пользователя построенной статистической модели легального пользователя. Если мы отвергаем проверяемую гипотезу, то формируем соответствующую запись в журнале, выдаем сообщение об ошибке и высылаем отчет о нарушителе на станцию администратора.

СПИСОК ЛИТЕРАТУРЫ

1. *Сабанов А. Г.* Актуальные задачи аутентификации, 2009. http://www.razvedka.ru/catalog/582/607/11034.htm.
2. *Бородулина Е. Л.*, *Кротова Е. Л.* Метод расщепления строго устойчивых смесей нормального закона для случая показателя устойчивости $\alpha = 1$ и $\alpha = 2$. Математическое моделирование. М.: Институт математического моделирования РАН, 2008, т. 20, № 7, с. 3–12.
3. *Столингс В.* Основы защиты сетей. Приложения и стандарты. М.: Издательский дом «Вильямс», 2002.