Ю.А.Горбунов, **И.А.Жуйков**, **Е.Л.Кротова** (Пермь, ПГТУ). **Использование вероятностного подхода для различения профиля легального пользователя от злоумышленника.**

В современных компьютерных системах актуальной является задача различения нарушителя от авторизированного пользователя автоматизированного рабочего места (АРМ). На сегодняшний момент для решения этой задачи широкое распространение получили эвристические системы, проверяющие соблюдение некоторых, обговоренных заранее, правил поведения легального пользователя АРМ. К таким правилам может относиться объем внешнего и внутреннего трафика, порядок и специфика использования пакетов прикладного программного обеспечения, особенности работы с данными баз данных (только чтение, только запись и др.). Этот подход имеет несколько минусов: во-первых, жесткие границы, различающие нарушителя от законного пользователя; во-вторых, в данном подходе существует необходимость хранить эти эвристические правила на том же компьютере, на котором совершается обработка секретной информации, что дает возможность злоумышленнику изменить границы заданных критериев различения.

Предлагаемый в работе вероятностный подход для построения критерия различения нарушителя от легального пользователя позволяет избежать указанных отрицательных моментов системы безопасности. Построения критерия различения на основе методов проверки простой статистической гипотезы различения двух распределений, где альтернативой является функция распределения вероятностей, соответствующая профилю нарушителя. Несомненным плюсом этого подхода является возможность построения обучаемого решающего правила. Кроме того, при различных уровнях секретности информации можно изменять значение уровня значимости, что позволит расширить границы, соответствующие поведению легального пользователя.

СПИСОК ЛИТЕРАТУРЫ

1. *Столингс В.* Основы защиты сетей. Приложения и стандарты. М.: Издательский дом «Вильямс», 2002, 432 с.
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, № 07, с. 3–12.