И. А. Жуйков, **Ю. А. Горбунов**, **Е. Л. Кротова** (Пермь, ПГТУ)**. Определение параметров математической модели профиля пользователя АРМ.**

На современном этапе для решения задачи обнаружения вторжений в работу компьютеризированной системы все чаще стали применятся вероятностные модели и методы, широкое распространение получило использование модели Маркова и фильтра Блума для проверки надежности словаря паролей системы [1]. Если вторжение в систему состоялось, то необходимо как можно раньше его выявить, это позволит идентифицировать нарушителя и лишить его доступа к системе прежде, чем он успеет нарушить целостность данных, хранящихся в системе. В нашем исследовании продолжена работа по различению легального пользователя от нарушителя по наблюдениям за поведением пользователя АРМ с помощью построения критерия различения двух вероятностных семейств. Предполагается, что поведение легальных пользователей отличается от поведения нарушителей и соответствующие различия можно представить в количественном отношении. На основе данных, характеризующих поведение легальных пользователей за определенный промежуток времени строятся профили легальных пользователей [2]. Для оценивания параметров этих вероятностных моделей предлагается использовать семейство строго устойчивых распределений, подходящих для аналитической модели исходных данных. Ранее для подобных моделей использовали нормальные законы распределения. Оценивание параметров построенной модели предлагается осуществлять согласно методике предложенной П. Н. Сапожниковым [3]. Проводиться сравнительный анализ предложенного решающего правили и обнаружения нарушителя по набору эвристических правил. С помощью вычисления значения локального наклона по Никитину [4] оценивается необходимый объем выборки для построения адекватной модели легального пользователя АРМ.

СПИСОК ЛИТЕРАТУРЫ

1. *Столингс В.* Основы защиты сетей. Приложения и стандарты. М.: Издательский дом «Вильямс», 2002.
2. *Горбунов Ю. А.*, *Жуйков И. А.*, *Кротова Е. Л.* Использование вероятностного подхода для различения профиля легального пользователя от злоумышленника. — Обозрение прикл. и промышл. матем., 2009, т. 16, в. 3, с. 460–461.
3. *Sapozhnikov P. N.* Pseudomixers for strong stable mixers of standard normal law. — XXIII International Seminar on Stability Problems for Stochastic Models. Pamplona (Spain), 2003, p. 49.
4. *Никитин Я. Ю.* Асимптотическая эффективность непараметрических критериев. М: Физматлит, 1995.