А. В. Аграновский, **К. Ю. Гуфан** (Ростов-на-Дону, ФГНУ НИИ «Спецвузавтоматика»). **Методы выявления аномалий в поведении пользователей электронных платежных систем с целью обнаружения мошеннических атак.**

Службы электронной коммерции, в том числе и электронные платежные системы (ЭПС) являются одним из быстроразвивающихся сегментов Интернет. Такие тенденции привлекают в ЭПС большое количество мошенников и лиц, использующих виртуальные транзакции для незаконных операций. По этой причине, проблема обнаружения и предупреждения мошеннических атак являются актуальной.

Нами была разработана система, позволяющая по информации о транзакциях и состояниях счетов ЭПС обнаруживать мошеннические операции как в процессе атаки (постоянный мониторинг работы ЭПС), так и после ее осуществления.

Была разработана модель взаимодействия пользователей ЭПС в рамках работы служб электронной коммерции. Проведен анализ основных угроз мошенничества, а так же классических схем мошеннических атак на ЭПС. В разработанной системе учитывается возможность использования мошенниками промежуточных ЭПС, информация о транзакциях внутри которых не известна, для осуществления незаконных операций.

На основе проведенного анализа были выработаны схемы обнаружения различных видов мошенничества с использование классического и специализированного математического инструментария [1].

Система обнаружения мошеннических атак включает в себя следующие элементы.

1. Предобработка данных (кодирование, нормировка, сжатие).

2. Построение групп пользователей и транзакций по различным критериям с использованием скрытых марковских моделей [2].

3. Анализ графов транзакций. Построение портрета типичного поведения пользователя (группы пользователей) ЭПС.

4. Статистический анализ динамики транзакций и работы электронных счетов, обнаружение подозрительных на мошенничество аномалий.

5. Сравнение поведений пользователей (групп пользователей) с шаблонами известных и типичных для ЭПС мошеннических атак.

Для реализации описанных элементов были применены различные методы и алгоритмы, позволяющие с достаточной степенью достоверность обнаруживать мошеннические атаки, при минимизации трудоемкости (временной и ресурсной) работы системы, а так же уменьшения числа ложных срабатываний.

СПИСОК ЛИТЕРАТУРЫ

1. *Wu V.*, *Kumar V.*, *Ross Quinlan J. et al.* Top 10 algorithms in data mining. — Knowledge and Information Systems, 2008, v. 14, i. 1, p. 1–37.
2. *Baumes J.*, *Goldberg M.*, *Magdon-Ismail M.*, *Wallace W.* On hidden groups in communication networks. Technical report TR 05-15, CS Dept., RPI 2005, p. 1–25.