МЕТОДИКА ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК НА БАЗЕ СИГНАТУРНЫХ И СТАТИЧЕСКИХ МЕТОДОВ

Чипига А.Ф., Пелешенко В.С., Лазарев Н.В.

Северо-Кавказский государственный технический университет,

zik@ncgtu.ru,

Ставрополь

При обнаружении сетевых атак, одновременно используя сигнатурные и статистические методы, предложена методика, включающая в себя следующие этапы:

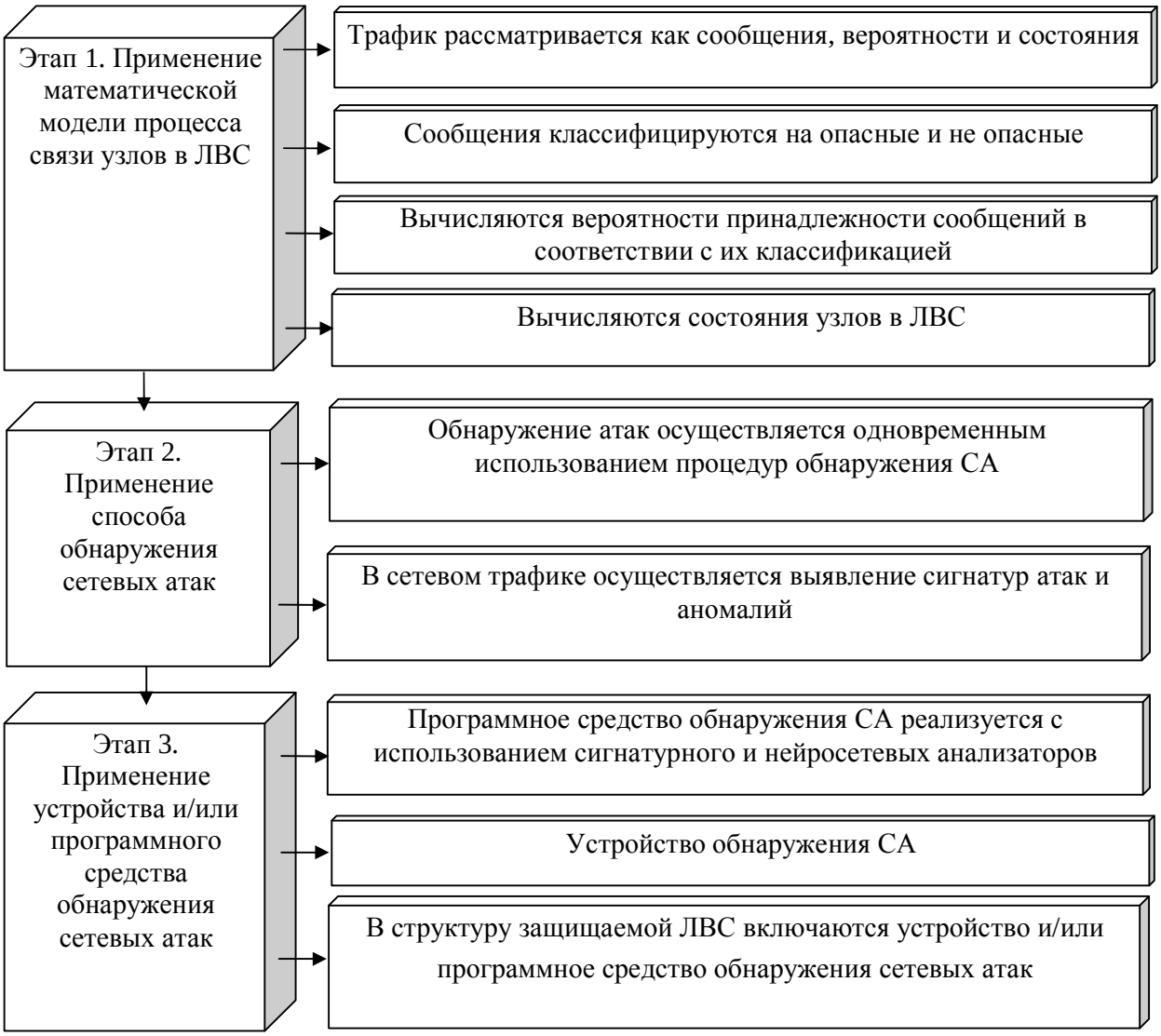

Рисунок 1 – Этапы реализации методики обнаружения СА

Формализованная методика обнаружения и предотвращения сетевых атак сводится к математическому отображению множества процедур как

предотвращения, так и обнаружения сетевых атак и их осуществления. Такие процедуры представляются в виде следующего множества:

$$G = \{g_1, g_2, ..., g_8\}, \quad (1)$$

где $g1$ – обнаружение СА в реальном режиме времени, $g2$ – обнаружение СА в регламентированном режиме времени, $g3$ – хостовый сбор данных для анализа, $g4$ – сетевой сбор данных для анализа, $g5$ – применение сигнатурных методов, $g6$ – применение статистических методов, $g7$ – сбор информации для обработки из хранилищ данных, $g8$ – сбор информации для обработки непосредственно из ЛВС.

Пара $g_1 \cup g_2$ показывает одновременное обнаружение СА в реальном и регламентируемом режимах времени и обозначается, как $g_{1,2}$, пара $g_3 \cup g_4$ показывает одновременное хостовое и сетевое обнаружение СА и обозначается, как $g_{3,4}$, пара $g_5 \cup g_6$ показывает одновременное применение сигнатурных и статистических методов и обозначается, как $g_{5,6}$, пара $g_7 \cup g_8$ показывает одновременный сбор информации из хранилищ данных и непосредственно из ЛВС и обозначается как $g_{7,8}$. Объединение вида $g_{1,2} \cup g_{3,4} \cup g_{5,6} \cup g_{7,8}$ обозначается как G' и означает обнаружение и предотвращение сетевых атак.

СПИСОК ЛИТЕРАТУРЫ

1. А.Ф. Чипига, В.С. Пелешенко. Построение нейросистем выявления и предотвращения атак // Материалы V региональной научно-практической конференции «Совершенствование методов управления социально-экономическими процессами и их правовое регулирование». Ставрополь, 2005.

2. А.Ф. Чипига, В.С. Пелешенко. «Формализация процедур обнаружения и предотвращения сетевых атак» // журнал «Известия ТРТУ». Таганрог: Изд-во ТРТУ, 2006.