МЕТОДИКА ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК НА БАЗЕ СИГНАТУРНЫХ И СТАТИЧЕСКИХ МЕТОДОВ

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

Северо-Кавказский государственный технический университет,

Ставрополь, Россия

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

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:

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

где g_1 – обнаружение СА в реальном режиме времени, g2 – обнаружение СА в регламентированном режиме времени, g_3 – хостовый сбор данных для анализа, g_4 – сетевой сбор данных для анализа, g_5 – применение сигнатурных методов, g_6 – применение статистических методов, g_7 – сбор информации для обработки из хранилищ данных, g_8 – сбор информации для обработки непосредственно из ЛВС.

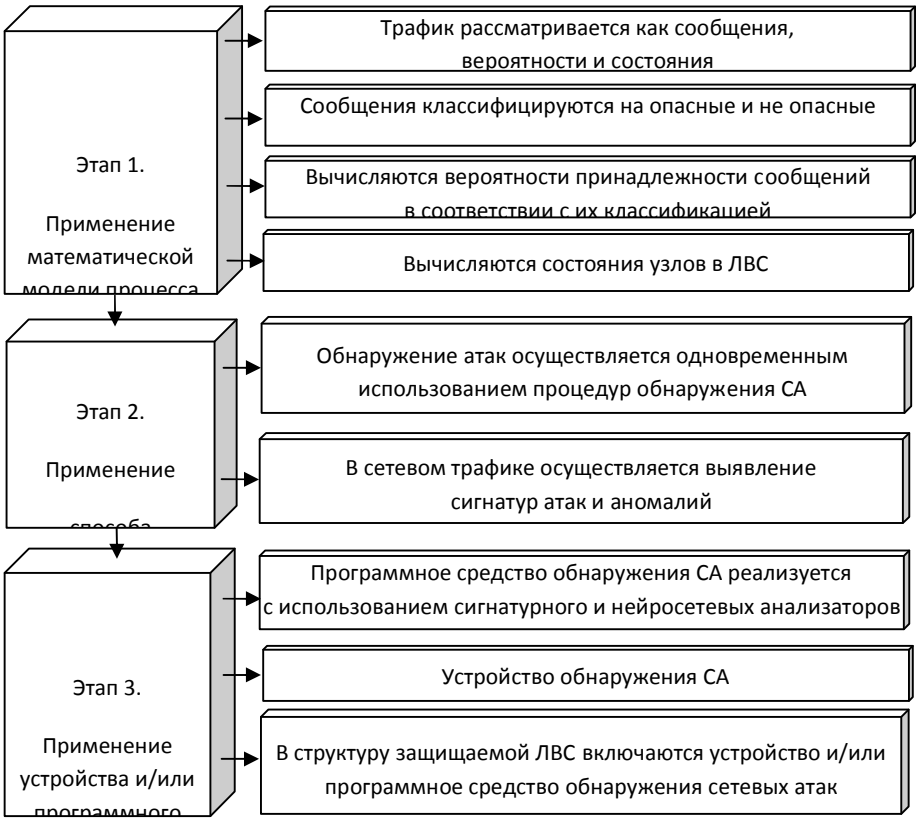

Рисунок 1. Этапы реализации методики обнаружения СА

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