УДК 681.3

ВЫБОР ИНФОРМАТИВНЫХ ПАРАМЕТРОВ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ДЛЯ РЕШЕНИЯ ЗАДАЧ ОБЕСПЕЧЕНИЯ ЕЕ ЗАЩИТЫ

Бакиров Т.К.
Научный руководитель – Валеев С.С.
Уфимский государственный авиационный технический университет

На сегодняшний день существует две разновидности систем контроля и диагностики состояния защиты вычислительной сети (ВС): системы анализа защищенности (САЗ) и системы обнаружения атак (СОА). При этом САЗ осуществляют анализ состояния ВС или ее элемента с точки зрения наличия в ней уязвимостей и угроз, СОА – непрерывный контроль этого состояния и его отклонений, свидетельствующих об атаке. Задачу САЗ можно рассматривать как проблему поиска текущего состояния в общем информационном пространстве ее состояний

$$\mathbf{S}=\{S_0, S_1, S_2, \ldots, S_n\}.$$

Задачу СОА можно сформулировать как проблему контроля переходов рассматриваемого объекта из одного состояния в другое в рассматриваемом пространстве состояний **S**:

$$\mathbf{T}=\{T_i \mid \forall i : T_i=(S_j, S_k),\ 0\le j\le n,\ 0\le k\le n\}.$$

Анализ текущего состояния объекта и его переходов возможен на основе множества входных и выходных его параметров $\mathbf{C}_0=\mathbf{C}_{IN}\cup\mathbf{C}_{OUT}$, например, входящего и исходящего трафика ВС. Количество возможных параметров объекта является бесконечным, поэтому актуальной является задача выбора параметров, наиболее значимых или информативных для анализа состояния объекта, которое является неопределенным в каждый момент. Эту задачу можно сформулировать как выбор из множества $\mathbf{C}_0$ такого подмножества **C**, которое будет достаточным для контроля состояния системы из множества состояний **S** в любой момент. Достаточным называется такое подмножество параметров, которое обеспечивает возможность контроля состояния системы с затратами $E=E(\mathbf{C})$, не превышающими некоторый заданный порог E_0. При этом затраты E можно выразить следующим образом:

$$E=E_m+E_w,$$

где E_m – стоимость измерения параметров;

E_w – стоимость потерь, вызываемых ошибками контроля.

Вычисление потерь от ошибок контроля состояния системы зачастую связано с большими вычислительными затратами. Поэтому часто используются другие критерии информативности признаков, менее требовательные к вычислениям и, вместе с тем, жестко связанные с оценкой потерь.

Одним из распространенных критериев информативности является оценка на основе энтропии – меры неопределенности случайной величины. Однако использование энтропии требует вычисления и использования вероятностей и их законов распределения для рассматриваемых случайных величин. Существуют критерии информативности, основанные на анализе других характеристик некоторой выборки состояний системы $\mathbf{S}_0\subseteq\mathbf{S}$. Решение указанной задачи при этом заключается в оптимизации требуемого набора параметров путем их ранжирования по используемому критерию информативности.

В настоящий момент рассматривается возможность моделирования процесса решения задачи выбора информативных параметров ВС с использованием перечисленных подходов.