С. А. Чурилов (Ростов-на-Дону, ФГНУ НИИ «Спецвузавтоматика»).
Методика оценки реальной защищенности информации в информационно-вычислительной сети.

В настоящее время необходимо производить оценку защищенности информации в рамках информационно-вычислительной сети (ИВС), по результатам которой формируется перечень актуальных угроз и разрабатывается комплекс мер по их нейтрализации. В работе, представленной данным докладом, представлена методика формирования оценки защищенности информации в ИВС, которая основывается на комбинировании экспертных оценок и показателей, полученных в ходе сканирования сети с помощью программных сканеров. В качестве показателя защищенности информации в ИВС принимается двухкомпонентный вектор, первой компонентой которого является уровень уязвимости сетевого ресурса ИВС, а второй компонентой — его уровень критичности в рамках исследуемой сети. Под уровнем критичности сетевого ресурса ИВС понимается показатель того, насколько сильно отразится на работоспособности всей ИВС и отдельных ее частей нарушение процесса выполнения функциональных обязанностей, возложенных на данный ресурс в рамках всей ИВС. Под уровнем уязвимости сетевого ресурса ИВС понимается показатель того, насколько опасными являются уязвимости, которые были обнаружены на нем. На основании заданных значений уровня уязвимости сетевого ресурса, а также его уровня критичности формируется оценка защищенности информации следующим образом. Пусть $Vuln\_Level$ — уровень уязвимости сетевого ресурса, $Critical\_Level$ — уровень критичности сетевого ресурса, Max_Vuln_Level — максимально возможное значение уровня уязвимости сетевого ресурса, $Max\_Critical\_Level$ — максимально возможное значение уровня критичности сетевого ресурса. Тогда значение показателя защищенности информации вычисляется по следующей формуле:

$$\frac{Vuln\_Level}{Max\_Vuln\_Level} \times \frac{Critical\_Level}{Max\_Critical\_Level}.$$

Для значений уровня защищенности сетевого ресурса определяется вербальная интерпретация данного показателя.

Представленная методика может быть использована для проведения мероприятий по оценке реальной защищенности информации в информационно-вычислительной сети от воздействий со стороны злоумышленника.

СПИСОК ЛИТЕРАТУРЫ

1. *Лепихин В. Б.* Сравнительный анализ сканеров безопасности. Ч. 1. Тест на проникновение. Учебный центр «Информзащита», 2008.