А. П. Р о с е н к о (Ставрополь, СГУ)**. О критерии нормирования уровня безопасности конфиденциальной информации.**

Актуальность проблемы заключается в необходимости разработки возможных подходов к нормированию уровня безопасности конфиденциальной информации (КИ) [1, 2]. В связи с этим нормирование уровня безопасности КИ в случае воздействия на автоматизированную информационную систему (АИС) внутренних и внешних угроз можно представить следующим образом [2].

Пусть $P_{\text{угр}_i}$ — вероятность реализации i-й угрозы, а ΔW_iЦ величина ущерба, нанесенного собственнику КИ в результате реализации злоумышленником i-й угрозы. Можно показать, что

$$Q_{\text{оп}_i} = P_{\text{угр}_i} \Delta W_i, \tag{1}$$

где $Q_{\text{оп}_i}$ — критерий, характеризующий степень опасности последствий от реализации злоумышленником i-й угрозы.

В [2] показано, что критерий вида (1) применяется в качестве критерия нормирования уровня безопасности конфиденциальной информации. Это связано с тем, что все воздействующие на АИС внутренние угрозы имеют различную степень опасности — $Q_{\text{оп}}$. Чем более ценная информация, циркулирует в компьютерной системе, тем более надежные методы и средства выбирает собственник КИ для ее защиты (через параметр ΔW_i). Как правило, это достигается принятой и реализованной политикой безопасности. С другой стороны, злоумышленник применяет методы и средства несанкционированного доступа к КИ в зависимости от ее ценности (через параметр $P_{\text{угр}_i}$).

В [2] показан возможный вариант установления градаций параметров $P_{\text{угр}_i}$ и ΔW_i. При этом градация вероятности реализации угроз может быть различной — от невероятной, что соответствует $P_{\text{угр}} \approx 0$, до практически достоверной, что соответствует $P_{\text{угр}} > 0,5$.

В свою очередь градация значения ущерба ΔW, в результате реализации злоумышленником внутренней или внешней угрозы, может принимать значения от незначительного ущерба собственнику КИ, соответствующего значению величины ущерба $\Delta W \approx 0\%$, до катастрофического ущерба, когда величина ущерба достигает значения $\Delta W > 50\%$.

Рассмотренный подход показывает, что при наличии априорных исходных данных можно уже в настоящее время осуществлять процедуру нормирования уровня безопасности КИ в зависимости от воздействия на АИС различных по природе возникновения внутренних и внешних угроз. Ранжируя степень опасности угроз по возрастанию (убыванию) значения $Q_{\text{оп}}$ представляется возможным определить наиболее опасные угрозы и разработать мероприятия по их парированию.

СПИСОК ЛИТЕРАТУРЫ

1. *Новиков В. А.* О проблемах нормативного обеспечения в области защиты информации. — Первый региональный научно-практический семинар «Информационная безопасность» — Юг России. Таганрог: Изд-во ТРТУ, 1999, с. 67–68.
2. *Росенко А. П.* Теоретические основы анализа и оценки влияния внутренних угроз на безопасность конфиденциальной информации. — Монография. М.: Гелиос АРВ, 2008, 154 с.