МЕТОДЫ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

К.В. Чопик, В.М. Алефиренко

На сегодняшний день информация представляет огромную ценность, и поэтому сам факт получения информации злоумышленником приносит ему определенный доход, тем самым причиняя ущерб организации, чья информационная система (ИС) была скомпрометирована. В связи с этим, вопрос оценки защищенности всей ИС в целом является самым главным. Проведя такую оценку, можно выбрать наиболее эффективную систему защиты для каждого частного случая построения ИС. К основным методам, позволяющим оценить защищенность ИС как на этапе проектирования, так и на этапе эксплуатации, относятся: метод оценки на основе графов защищенности и метод оценки на основе нечеткой логики.

Метод оценки на основе графов защищенности обеспечивает повышение эффективности управления защитой информации в ИС за счет комплексного показателя защищенности и применения графа защищенности, который учитывает действительную структуру ИС [1]. Преимуществом данного метода является то, что с его помощью можно получить количественные оценки уровня защищенности ИС для различных типов угроз. Недостатком метода является то, что для его реализации необходима высокая квалификации персонала и относительно большие временные затраты для оценки уровня защищенности в больших информационных системах.

Метод оценки защищенности при помощи нечеткой логики основан на использовании формализованных качественных понятиях [2]. Однако, при этом остается проблема предварительного определения и выбора следующих параметров: выбор представления лингвистических переменных, определение граничных значений выходных данных, выбор метода дефаззификации. Решение данной задачи требует достаточно высокой квалификации персонала. Вся остальная обработка входных данных проводится системой в виде «черного ящика», то есть на вход системы с нечеткой логикой подаются параметры, выбранные для оценивания, а на выходе формируется определенное управляющее воздействие. Применение данного метода позволяет уйти от субъективности персонала за счет автоматизированной обработки статистики по исследуемым инцидентам.

Таким образом, сочетание рассмотренных методов для оценки защищенности информационных систем позволяет учитывать всевозможные прецеденты информационной безопасности, что в свою очередь позволит с большей эффективностью оценивать их защищенность и более динамично управлять конкретной информационной системой.

Литература

1. Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности / А.В. Козленко [и др.] // Труды СПИИРАН. – 2012. – № 2 (21). – С. 41–55.

2. Жукова М.Н., Коромыслов Н.А. Модель оценки защищенности автоматизированной системы с применением аппарата нечеткой логики // Известия ЮФУ. Технические науки. – 2013. – № 12 (149). – С. 63–69.