МЕТОД НЕЧЕТКИХ МНОЖЕСТВ КАК СПОСОБ ЗАЩИТЫ ИНФОРМАЦИИ

К.Ю. Гиро, В.А. Федоренко

Сегодня одним из наиболее перспективных направлений научных исследований в области анализа, моделирования и прогнозирования слабо структурированных процессов и явлений являются нечеткая логика и математический аппарат теории нечетких множеств. Механизм нечеткого логического вывода, позволяет объективно отражать причинно-следственные связи между слабо структурированными и/или вовсе неструктурированными характеристиками, более адекватен процессу выявления информационных угроз на самой ранней стадии, «пластично» учитывает особенности потенциальных атак.

Теория нечетких множеств хорошо согласуется с условиями моделирования систем защиты, так как многие исходные данные моделирования (например, характеристики угроз и отдельных механизмов защиты) не являются строго определенными. Одним из главных преимуществ нечеткого моделирования является его способность к быстрой адаптации на предмет решения новых классов информационных угроз. На основе базовых лингвистических правил создается так называемая «грубая» нечеткая модель, которая в условиях эксплуатации системы информационной защиты и программной симуляции может быть скорректирована и представлена второй моделью. Далее, в процессе эксплуатации пользователь этой модели может обнаружить новые закономерности и взаимосвязи и, тем самым, трансформировать ее в более адекватную причинно-следственную связь. Процесс адаптации нечеткой модели является итерационным и длится ровно столько, сколько необходимо шагов для идентификации новых параметров, обеспечивавших адекватное сходство с реальными векторами признаков информационных угроз.

Выделяют 3 этапа формирования нечетких множеств угрозы информационной безопасности.

Этап 1. Формирование модели угроз, определение взаимосвязи между угрозами и рисками информационной безопасности.

Этап 2. Построение функций принадлежности начальных нечетких множеств уровня ущерба информационной системе.

Этап 3. Построение обобщенного нечеткого множества уровня воздействия класса угроз на информационную систему.

Достоинства метода:

- не использует аппарат теории вероятностей в силу отсутствия реальной статистики воздействия угроз;
- не применяет процедуру оценки степени соответствия информационной системы определенному набору требований по обеспечению информационной безопасности, что может быть весьма дорогой процедурой для предприятия.

Таким образом, учитывая все достоинства и особенности метода, математический аппарат нечеткой логики является адекватным инструментом для решения задач информационной безопасности [1, 2].

Литература

1. Асланов К.Дж. Построение интеллектуальных интегрированных систем информационной безопасности в открытых корпоративных сетях: диссертация / Азербайджанский государственный университет экономики. Баку, 2018. 92 с.

2. Дубинин Е.А. Методика получения нечеткого множества уровня воздействия класса угроз на информационную систему // Информационно-управляющие системы. 2006. № 5. С. 76–80.