О ПРОБЛЕМАХ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Милько Дмитрий Сергеевич, Аспирант ИРГУПС

Оценка угроз безопасности информации необходима для разработки соответствующей модели угроз. Результаты оценки угроз применяются для выбора и обоснования требуемых мер при построении систем защиты информации. В феврале 2021 г. вступил в силу новый методический документ Федеральной службы по техническому и экспортному контролю Российской Федерации (ФСТЭК России), обязательный к исполнению всеми организациями, которые проводят оценку угроз безопасности информации. Описан подход к автоматизации исключения неактуальных угроз безопасности информации путем разработки экспертной системы. Сформирована база знаний экспертной системы, описан подход к формированию базы знаний. Сформулированы ключевые понятия для экспертной системы оценки угроз, такие как область знаний, эксперт, пользователь. Приведена схема работы экспертной системы оценки угроз безопасности информации. Приведены практические результаты, полученные от внедрения разработанной базы знаний экспертной системы, на предприятии, занимающемся технической защитой конфиденциальной информации. Приведено обоснование выбора экспертной системы в качестве метода автоматизации процедуры оценки угроз безопасности информации. Проведено сравнение экспертных систем с более современными технологиями автоматизации (искусственные нейронные сети). Сделаны выводы об эффективности разработанной базы знаний, а также о необходимости разработки более удобного интерфейса и машины логического вывода.