УДК 004.891:[621.396+004.056]

ПРОДУКЦИОННАЯ ЭКСПЕРТНАЯ СИСТЕМА ОЦЕНКИ ЗАЩИЩЁННОСТИ ТЕРМИНАЛОВ ОТОБРАЖЕНИЯ ИНФОРМАЦИИ В СОСТАВЕ РАДИОТЕХНИЧЕСКИХ КОМПЛЕКСОВ

О.О. НАУМОВ[1], А.С. МАМАЕВ[2]

[1]*«Технологический университет имени дважды Героя Советского Союза, летчика-космонавта А.А. Леонова» - филиал федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет геодезии и картографии» (г. Королев, Российская Федерация)*
[2]*Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА - Российский технологический университет» (г. Москва, Российская Федерация)*

E-mail: mamaev@mirea.ru

Аннотация. Рассматривается задача формализованной оценки уровня защищённости терминалов индивидуальных средств отображения специальной информации (ТИСОСИ) в радиотехнических комплексах. Предложена архитектура экспертной системы на основе продукционной модели представления знаний. Обоснован выбор продукционного подхода. Разработаны структура базы знаний, лингвистические шкалы и примеры правил логического вывода. Приведены ожидаемые результаты практической реализации.
Abstract. The paper considers the problem of formalized security assessment of terminals for individual display of special information (TISOSI) in radio engineering complexes. An architecture of an expert system based on a production knowledge representation model is proposed. The choice of the production approach is justified. The structure of the knowledge base, linguistic scales and examples of inference rules are developed. The expected results of practical implementation are given.

Введение

Недостаточная защищённость терминальных программ от анализа, как отмечают Маркин и Макеев [1], способна привести к серьёзным негативным последствиям. В радиотехнических комплексах терминалы индивидуальных средств отображения специальной информации (ТИСОСИ) являются конечными точками доступа к обрабатываемым данным. Их защищённость определяется множеством трудно формализуемых факторов: корректность настройки мандатного доступа, квалификация пользователя, соблюдение регламентов аудита. Большинство этих факторов имеет качественную природу, что затрудняет применение детерминированных или вероятностных методов оценки. Цель работы — разработать архитектуру продукционной экспертной системы для формализованной оценки уровня защищённости терминалов ТИСОСИ. Для этого необходимо обосновать выбор модели представления знаний, определить шкалы оценок и сформировать правила логического вывода.

Основная часть

Терминал ТИСОСИ — это автоматизированное рабочее место для отображения телеметрии, баллистических расчётов и команд управления [1]. Защищённость терминала определяется техническими, человеческими и организационными факторами.

Для слабоструктурированных задач информационной безопасности наиболее адекватна продукционная модель [2]. Продукционная модель, в отличие от нейро-нечётких [3], обеспечивает прозрачность вывода. Специалист может проследить сработавшее правило [4], что важно для отчётности и расследований.

Предлагаемая система включает базу знаний, механизм прямого вывода и подсистему объяснения. Лингвистические переменные вводятся с терм-множеством «низкий — средний — высокий» [2, 5]. На рис. 1 представлена архитектура экспертной системы.

Типовое взвешенное правило имеет вид: ЕСЛИ (ОС сертифицирована, вес 0,3) И (мандатный контроль включён, 0,4) И (аудит активирован, 0,2) И (пользователь обучен, 0,1) ТО уровень технической защищённости — ВЫСОКИЙ при сумме весов $\geq 0{,}7$.

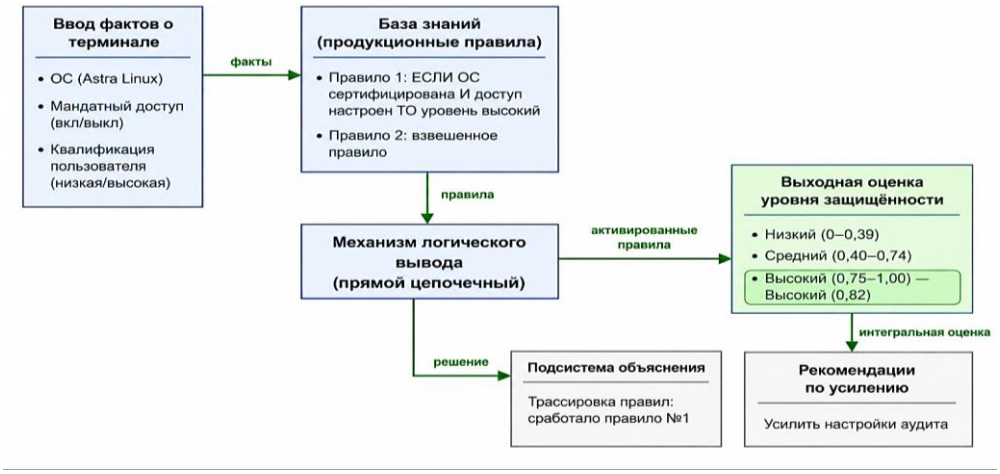

Рис. 1. Архитектура продукционной экспертной системы

Формально степень активации правила можно представить как:

$$\mu_R = \frac{\sum_{i=1}^{n} w_i \cdot \mu_i}{\sum_{i=1}^{n} w_i}, \qquad (1)$$

где w_i – весовой коэффициент i-го условия, μ_i – степень его истинности (0 или 1 для бинарных фактов, либо значение функции принадлежности для нечётких переменных). Решение о классе защищённости принимается по максимальному значению активации среди правил, ведущих к разным заключениям.

База знаний формируется на основе экспертного опроса с вычислением индивидуальных коэффициентов значимости экспертов (стаж, сертификаты, опыт аттестации) [4]. Итоговая оценка уровня защищённости по трёхуровневой шкале («низкий» — 0–0,39; «средний» — 0,40–0,74; «высокий» — 0,75–1,00) выдаётся лицу, принимающему решение, вместе с трассировкой сработавших правил.

Экспертная система позволит сотрудникам служб ИБ за 10–15 минут получать формализованное заключение о защищённости терминала с указанием конкретных недостатков. Как показано в работах по управлению информационной безопасностью [5], регулярный мониторинг и количественная оценка уровня защищённости являются необходимыми условиями устойчивого функционирования системы защиты. Предварительные расчёты показывают, что применение предложенной системы снижает трудоёмкость оценки в 3–4 раза по сравнению с неформализованным экспертным анализом.

Заключение

Разработана архитектура продукционной экспертной системы для оценки защищённости терминалов ТИСОСИ. Основные результаты: обоснован выбор продукционной модели представления знаний; определена трёхуровневая шкала итоговых оценок; сформирован пример взвешенного правила логического вывода. Цель работы достигнута. Предложенное решение отличается «прозрачностью» решений, что критически важно для практического использования в радиотехнических комплексах. Перспективным направлением дальнейших исследований является автоматическое формирование рекомендаций по устранению выявленных недостатков.

Список использованных источников

1. Маркин Д.О., Макеев С.М. Система защиты терминальных программ от анализа на основе виртуализации исполняемого кода // Вопросы кибербезопасности. 2020. № 1(35). С. 29–41. DOI: 10.21681/2311-3456-2020-01-29-41.

2. Ажмухамедов И.М., Князева О.М. Унификация подходов к управлению уровнем информационной безопасности в организациях различного профиля // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2015. № 1. С. 66–77.

3. Glushenko S.A. An adaptive neuro-fuzzy inference system for assessment of risks to an organization’s information security // Business Informatics. 2017. No. 1(11). P. 68–77. DOI: 10.17323/1998-0663.2017.1.68.77.

4. Милько Д.С., Данеев А.В., Горбылев А.Л. База знаний экспертной системы оценки угроз безопасности информации // Доклады ТУСУР. 2022. Т. 25. № 1. С. 61–69. DOI: 10.21293/1818-0442-2021-25-1-61-69.

5. Салютина Т.Ю., Корчака В.С. Исследование методических аспектов оценки эффективности системы информационной безопасности бизнеса и разработка проекта внедрения DLP-системы на предприятии в условиях цифровизации // Экономика и бизнес: теория и практика. 2025. № 3(121). С. 291–295. DOI: 10.24412/2411-0450-2025-3-291-295.