П. Н. Лось

ИСПОЛЬЗОВАНИЕ ЭКСПЕРТНЫХ СИСТЕМ ДЛЯ АНАЛИЗА И ОЦЕНКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В этом документе рассматриваются вопросы использования экспертной системы(ЭС) для предметной области компьютерной безопасности.

Введение

Аудит компьютерной безопасности является важной частью системы безопасности любой организации. Успех обеспечения ИБ — заключается в комплексном подходе. При этом все средства, методы и мероприятия, используемые для защиты информации, объединяются в единый целостный механизм — систему защиты. От части решение задач обеспечения информационной безопасности организации может быть получено на базе использования экспертных систем, как части системы защиты информации.

I. Использование ЭС для аудита безопасности

Рассмотрим подробнее что же такое «Анализ системы защиты информации» и для чего он применяется. Одно из его определений [1] — это комплексное изучение фактов, событий, процессов, явлений, связанных с проблемами защиты информации, в том числе данных о состоянии работы по выявлению возможных каналов утечки информации, о причинах и обстоятельствах, способствующих утечке и нарушениям режима секретности (конфиденциальности) в ходе повседневной деятельности предприятия.

Аудит безопасности часто используется для обнаружения аномальных событий, которые выходят за рамки мер безопасности в реальном времени. Методы искусственного интеллекта (в частности, методы экспертных систем) могут многое предложить специалистам по компьютерной безопасности. Экспертные система предназначена для автоматизации процедур аудита безопасности и снижения нагрузки на аудиторов. Экспертная система должна уметь взять на себя те функции, которые выполняет специалист-эксперт или выполнить роль ассистента для лица, принимающего решения. Использование экспертных систем позволит управляющей информационной системе получать решение непосредственно от программы и полностью исключить необходимость использования человека в управляющей системе. С другой стороны, экспертная система может повысить эффективность работы человека, предлагая наиболее верное решение поставленной задачи.

II. Построение ЭС для аудита безопасности

При проектировании экспертной системы выполняются следующие шаги.

1. Определяются основные угрозы информационной безопасности и производится их классификация.

2. Для каждой угрозы информационной безопасности определяется список уязвимостей, через которые эта угроза может быть реализована.

3. С помощью информационной безопасности для каждой уязвимости определяется список требований, которые должны быть выполнены, чтобы избежать осуществления угрозы.

4. Каждому запросу присваивается вес, выражающий степень важности требований.

Таким образом, экспертная система состоит из модулей, которые включают в себя требования безопасности, предъявляемые к каждой уязвимости..

III. Выводы

Для повышения качества аудита безопасности целесообразно применять экспертные системы. Применение ЭС для обеспечения информационной безопасности на предприятии позволяет существенно повысить уровень информационной безопасности, несколько упростить процесс обнаружения и анализа проблем информационной защиты, а так же использовать опыт экспертов в области информационной безопасности.

1. Курило А.П., Зефиров С.Л., Голованов В.Б. Аудит информационной безопасности.– М.: Издательская группа «БДЦ-пресс», 2006 г.

Лось Павел Николаевич, магистрант кафедры интеллектуальных информационных технологий БГУИР pasha-los96@yandex.ru.

Научный руководитель: Захаров Владимир Владимирович, доцент кафедры интеллектуальных информационных технологий БГУИР, кандидат технических наук, доцент, zvv@open.by.