ОБЗОР И АНАЛИЗ ИНТЕЛЛЕКТУАЛЬНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

В.А. ВИШНЯКОВ

В докладе представлены результаты анализа применения интеллектуальных средств защиты информации (ИСЗИ). Выделены следующие направления: экспертные системы, нейронные сети, интеллектуальные агенты.

Схемы обнаружения атак включают: определение вторжения и выявление аномалий. К первым относятся атаки, использующие известные уязвимости информационной системы (ИС). Ко вторым — неизвестную деятельность. Обнаружение аномалий происходит с использованием базы знаний (БЗ) и логического вывода. БЗ содержит описание известных действий хакеров Обнаружение вторжения происходит, если действия пользователя не совпадают с установленными правилами.

В ИСЗИ экспертные системы в БЗ содержат описание классификационных правил, соответствующим профилям легальных пользователей и сценариям атак на ИС. Обсуждаются недостатки ЭС в защите информации.

Нейронные сети, часто использующие для решения задач классификации и кластеризации, к которым можно отнести выявление вторжения в ИС. Возможность обучения — важное качество нейросетевых СЗИ, которое позволяет адаптироваться к изменению входной информации и поведения хакеров.

Новым направлением в ИСЗИ является использование интеллектуальных агентов, использующих технологии Semantic Web, работающих в распределенной ИС и запрограммированных на поиск, как вторжения, так и аномалий.

ИССЛЕДОВАНИЕ «РЕСПУБЛИКА БЕЛАРУСЬ И МИРОВАЯ ПРАКТИКА: КРАТКИЙ ОБЗОР, ОСНОВНЫЕ ТЕНДЕНЦИИ В СЕГМЕНТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

В.В. МАЛИКОВ, И.В. БЕНЕДИКТОВИЧ, С.А. ЧУРЮКАНОВ

Проведен анализ статистических данных исследования в области информационной безопасности (ИБ) за 2012 г., проведенного компанией Ernst & Young и подготовлен аналитический обзор «Сравнительный обзор подходов к обеспечению информационной безопасности (Республика Беларусь и мировая практика)».

Основные результаты проведенной экспертной оценки:

1. В Беларуси C-level (уровень правления и высшего руководства) направления безопасности представлен, как правило, CSO (Chief Security Officer). CISO себя называют руководители подразделений ИБ, которые, как правило, занимаются только безопасностью ИТ-систем, а не общей информационной безопасностью организации.

2. Следует отметить, что в Беларуси более $1 млн компании на ИБ не тратят. Экономика определяет сущность доходов/расходов. При этом если взять затраты на ИБ менее $0,1 млн. у 56% респондентов, то среднемесячные затраты ориентировочно составят — $8,33 тыс.

3. Численная оценка проведения аудитов только собственными силами составляет минимум 14%.

4. Признание увеличения уровня угроз и уменьшения инцидентов (при минимальных затратах на ИБ), показывает, что около 33–38% организаций из числа «затраты на ИБ менее $0,1 млн» находятся в группе высокого риска осуществления инцидентов ИБ со стороны злоумышленников.

Таким образом, дальнейшее проведение указанного выше исследования, позволит получить новые научно-обоснованные результаты, которые повысят эффективность внедрения и использования средств и систем защиты информации, а также обеспечат гарантированную защиту объектов различных категорий.