Необходимость формализации требований к методам и способам оценки защищенности вычислительных систем и ресурсов

Актуальность

- Эффективность реализации большинства бизнес- и производственных процессов связана с обеспечением информационной безопасности
- Поддержание необходимого и достаточного уровня защищенности вычислительных систем и ресурсов к воздействию компьютерных атак
- Непрерывное развитие и совершенствование законодательства в области технической и криптографической защиты информации

Поиск ответов

- Допустима ли обработка информации, распространение и (или) предоставление которой ограничено, в той или иной информационной системе?
- Насколько и как долго реализованные механизмы безопасности смогут противостоять выявленным угрозам информационной безопасности?
- Содержит ли используемое программное обеспечение уязвимости, которые могут быть использованы для получения несанкционированного доступа к активам?
- Как оценить уровень защищенности и как определить является ли он достаточным в данной среде функционирования информационной системы?

Методы, способы и инструменты

Методы (метод «белого ящика», метод «черного ящика»).

Способы (только сканирование на наличие уязвимостей; сканирование с имитацией атак и имитацией действий злоумышленника; имитацией физического проникновения; с попыткой заражения активов вредоносным программным обеспечением).

Средства анализа защищенности (сетевые сканеры уязвимостей; сканеры уязвимостей построенные на базе агентов; свободно распространяемые инструменты и инструменты, разработанные самостоятельно; полноценные экспертные системы).

Квалификация и опыт

Знание типовых угроз и уязвимостей, критериев и подходов к анализу защищенности, владение методами анализа и специализированным инструментарием, профессиональное знание различных программно-аппаратных платформ, используемых в современных компьютерных сетях, умение оценивать и управлять рисками, –далеко не полный перечень профессиональных качеств, которыми должны обладать технические специалисты, проводящие работы по анализу защищенности информационных систем.

Экономический фактор

Разнообразие, непрерывное развитие и сложность сферы информационных технологий и информационной безопасности приводят к тому, что специалистам необходимы годы на обучение, совершенствование практик и поддержание необходимого уровня знаний чтобы стать экспертом в области оценки защищенности вычислительных систем и ресурсов информационных систем.

Стоимость услуг сторонних экспертов в области информационной безопасности в целом и в области оценки защищенности вычислительных систем и ресурсов в частности может составлять значительную часть бюджета, выделяемого на обеспечение непрерывного функционирования информационной системы и ее системы защиты информации.

Заключение

Разработка и внедрение методик с формализованными требованиями к методам и способам оценки защищенности вычислительных систем и ресурсов и обоснованными метриками для получения количественных оценок показателей защищенности являются актуальными задачам.

Методики должны оперировать понятиями, поддающимися математической формализации и состоящими из простых элементов, допускающих количественные оценки или имеющих качественные характеристики, представленные конечными списками возможных состояний. Итоговые оценки должны присваиваться путем математических расчетов по представленным формулам и на основе конкретно определенных исходных данных. Количество исходных параметров, основанных на экспертных оценках, должно быть сведено к минимуму.

Спасибо за внимание