CRAMM

написано Александр Астахов | 11 июня, 2023

Не менее основательный подход используется и в широко известном методе оценки рисков *CRAMM*, разработанном Службой безопасности Великобритании (UK Security Service) по заказу британского правительства. В методе CRAMM основной способ оценки рисков – это тщательно спланированные интервью, в которых используются подробные опросные листы, примеры которых приведены в Приложениях №№ 4, 7 и 8.

Метод CRAMM используется в сотнях организаций по всему миру, благодаря, кроме всего прочего, и наличию весьма развитого программного инструментария, разрабатываемого британской компанией Insight Consulting, приобретенной в начале 2000-х годов концерном SIEMENS. Инструментарий CRAMM содержит базу знаний по рискам и механизмам их минимизации, средства сбора информации, формирования отчетов, а также реализует алгоритмы для вычисления величины рисков.

CRAMM (UK Government Risk Analysis and Management Method):

- *Разработан Службой Безопасности Великобритании (UK Security Service) по заданию Британского правительства и взят на вооружение в качестве государственного стандарта.*
- *Используется начиная с 1985 г. правительственными и коммерческими организациями Великобритании. За это время приобрел популярность во всем мире.*
- *Фирма Insight Consulting Limited занимается разработкой и сопровождением одноименного программного продукта.*

В отличие от метода OCTAVE, в CRAMM используется несколько

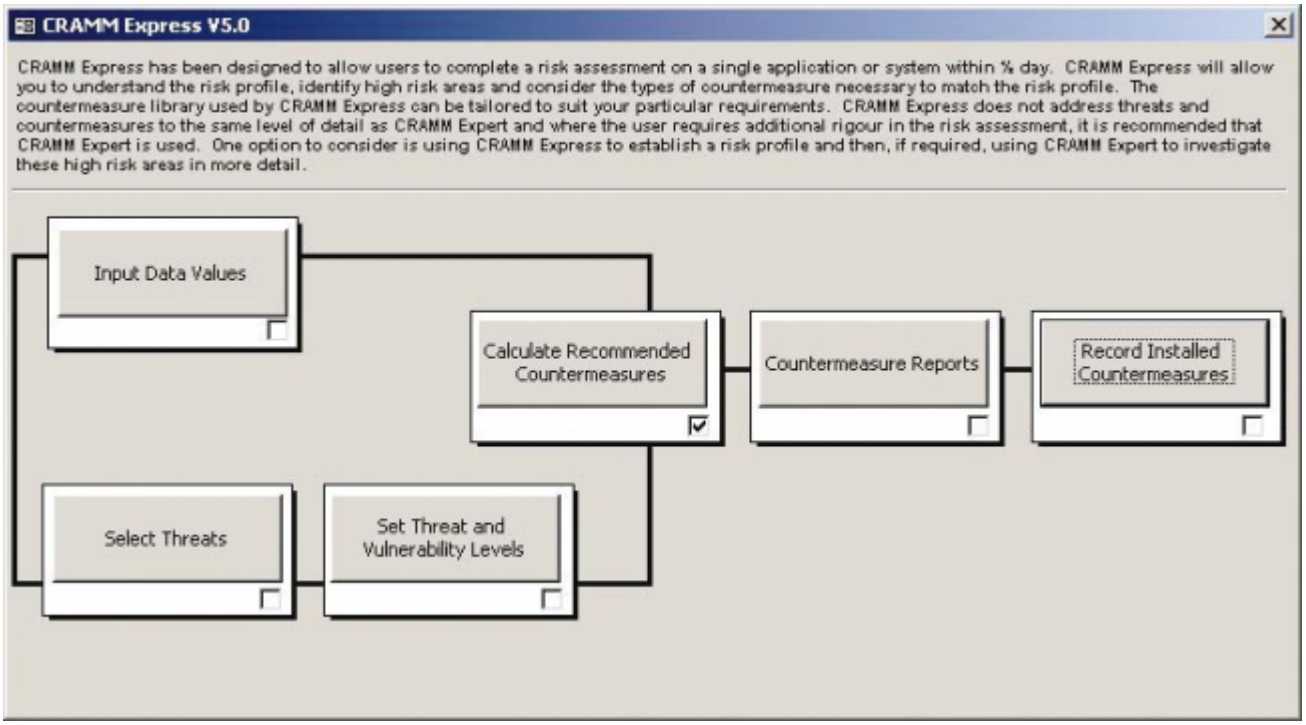
иная последовательность действий и методы определения величины рисков. Сначала выявляется сама целесообразность детальной оценки рисков. Если информационная система организации недостаточно критична, то к ней применятся стандартный набор механизмов контроля, описанный в международных стандартах и содержащихся в базе знаний CRAMM, которая в основном базируется на британском стандарте BS 7799.

*На первом этапе*в методе CRAMM строится модель активов информационной системы, описывающая взаимосвязи между информационными, программными и техническими активами, а также оценивается ценность активов исходя из возможного ущерба, который организация может понести в результате их компрометации.

*На втором этапе*производится оценка рисков, включающая в себя идентификацию и оценку вероятности угроз, оценку величины уязвимостей и вычисление рисков для каждой тройки: актив – угроза – уязвимость. В CRAMM оцениваются так называемые «чистые» риски, безотносительно к реализованным в системе механизмам контроля. На этапе оценки рисков предполагается, что контрмеры вообще не применяются.

*На заключительном этапе*определяется набор контрмер по минимизации идентифицированных рисков и производится сравнение рекомендуемых и существующих контрмер, после чего формируется план обработки рисков.

CRAMM Express. Этапы оценки и обработки рисков



Этапы управления рисками по методу CRAMM:

1. *Подготовка, выбор подхода (базовый уровень или детальная оценка рисков).*
2. *Оценка критичности активов. Модель активов, ущерб, ценность активов.*
3. *Оценка рисков. Угрозы, уязвимости, величина рисков*
4. *Выбор контрмер. Сравнение рекомендуемых и существующих контрмер, план обработки рисков.*

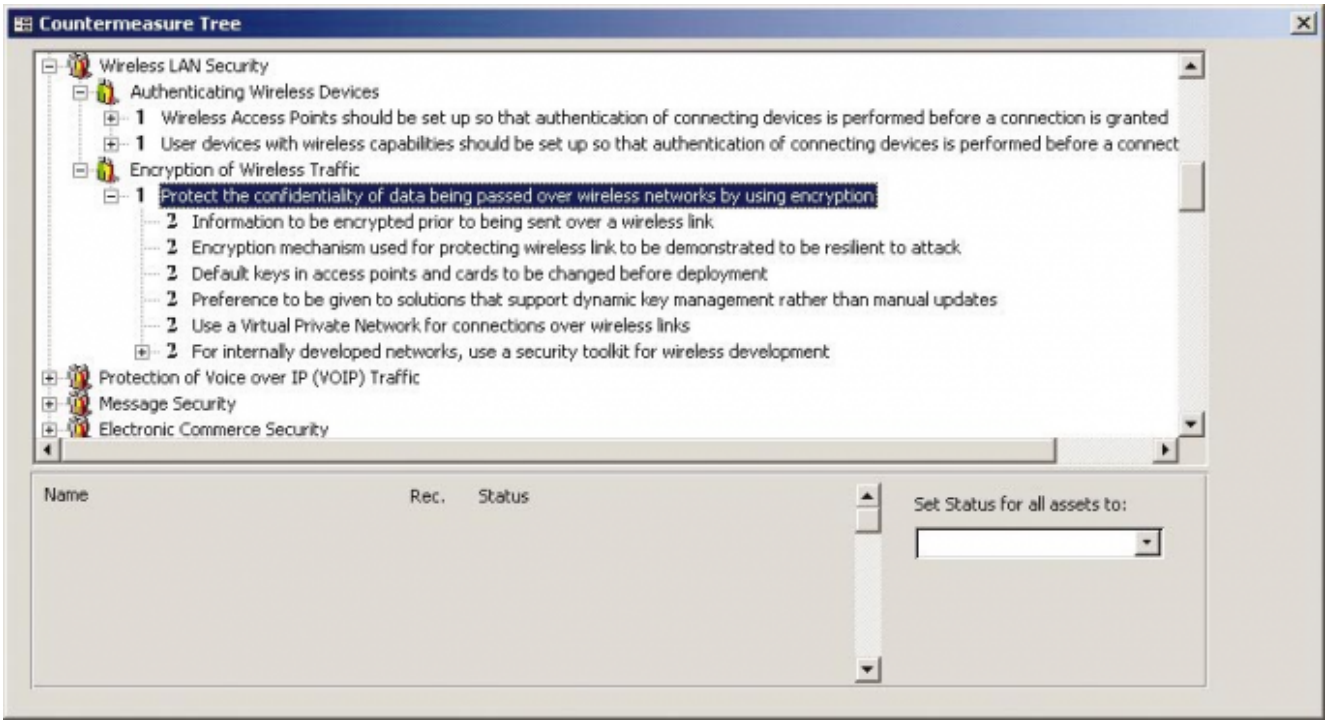
Возможности программного инструментария CRAMM значительно превышают возможности, необходимые лишь для оценки рисков и включают в себя следующее:

- база данных, содержащая 3000 контрмер, охватывающих все аспекты информационной безопасности, совместимая с BS 7799, ISO 15408 и другими стандартами;
- 400 типов ресурсов ИС, более 25 различных видов ущерба, более 10 способов оценки ущерба, 38 типов угроз, более

150 возможных комбинаций ущерба, угрозы и уязвимости, 7 уровней риска;

- набор инструментальных средств для прохождения процедуры аудита и сертификации на соответствие BS 7799;
- набор типовых политик безопасности и других документов, настраиваемых для каждой организации;
- средства планирования непрерывности бизнеса;
- средства проведения высокоуровневого анализа рисков (всего за 2 часа) при помощи CRAMM v.5 Express;
- средства документирования механизмов безопасности и результатов аудита.

CRAMM. База контрмер



Хорошо структурированный и широко опробованный метод CRAMMобладает необходимой гибкостью и универсальностью, что позволяет использовать его в проектах любого уровня сложности. В тоже время CRAMM не лишен и определенных недостатков, в числе которых можно отметить следующее:

- требует специальной подготовки и высокой квалификации;
- в гораздо большей степени подходит для аудита уже существующих, нежели для разрабатываемых систем;

- аудит по методу CRAMM – процесс трудоемкий и может потребовать месяцев непрерывной работы;
- генерирует большое количество бумажной документации, которая не всегда полезна на практике;
- как и у многих других импортных продуктов, в CRAMM существуют проблемы с отображением кириллицы.

Особенно огорчает российских пользователей системы CRAMM тот факт, что возможность внесения дополнений в базу знаний фактически не доступна пользователям, что вызывает значительные трудности при адаптации этого метода к потребностям организации. Кроме того, CRAMM не позволяет создавать собственные шаблоны отчетов или модифицировать имеющиеся.

CRAMM. Контроль статуса механизмов безопасности