УПРАВЛЕНИЕ РИСКАМИ. МЕТОД CRAMM

Антон Алексеев,
тренер-консультант
IT Expert

Управление рисками – деятельность, направленная на принятия и выполнения управленческих решений, с целью снижения вероятности возникновения неблагоприятного результата и минимизации возможных потерь, вызванных его реализацией. Очень полезно, когда эта деятельность реализована в виде полноценного циклического управляемого и измеряемого процесса.
Управлять рисками требуется на разных стадиях жизненного цикла сервиса. Существует ряд методом способствующих оптимизации прилагаемых к этому усилий. Здесь мы рассмотрим один из них – метод CRAMM, вышедший в свет примерно в тоже время, что и первая версия библиотеки ITIL.

История создания метода
В 1985 году Центральное агентство по компьютерам и телекоммуникациям (CCTA - Central Computer and Telecommunications Agency) Великобритании начало исследования существующих методов анализа ИБ, чтобы рекомендовать методы, пригодные для использования в правительственных учреждениях, занятых обработкой несекретной, но критичной информации. Ни один из рассмотренных методов не подошел. Поэтому был разработан новый метод, соответствующий требованиям CCTA Он получил название CRAMM- CCTA Risk Analysis & Management Method - метод CCTA анализа и контроля рисков. Затем появилось несколько версий метода, ориентированных на требования

Министерства обороны, гражданских государственных учреждений, финансовых структур, частных организаций.
Метод Реализован в специализированном программном обеспечении, настраиваемом под различные сферы деятельности при помощи «профилей» (коммерческий, гражданское государственное учреждение, финансовый сектор и проч.).

Текущая версия CRAMM 5 , соответствует стандарту BS 7799 (ISO 17799).

Целью разработки метода являлось создание формализованной процедуры, позволяющей:

- убедиться, что требования, связанные с безопасностью, полностью проанализированы и документированы;
- избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков;
- оказывать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем:
- обеспечить проведение работ в сжатые сроки;
- автоматизировать процесс анализа требований безопасности;
- представить обоснование для мер противодействия;
- оценивать эффективность контрмер, сравнивать различные их варианты;
- генерировать отчеты.

Концепция, положенная в основу метода
Анализ рисков включает идентификацию и вычисление уровней (мер) рисков на основе оценок, присвоенных ресурсам, угрозам и уязвимостям ресурсов.
Контроль рисков состоит в идентификации и выборе контрмер, благодаря которым удается снизить риски до приемлемого уровня.
Формальный метод, основанный на этой концепции, позволяет убедиться, что защита охватывает всю систему и существует уверенность в том, что:

- все возможные риски идентифицированы;
- уязвимости ресурсов идентифицированы и их уровни оценены;
- угрозы идентифицированы и их уровни оценены;
- контрмеры эффективны;
- расходы, связанные с ИБ, оправданы.

Исследование ИБ системы с помощью CRAMM проводится в несколько этапов.

На первой стадии, **Initiation**, производится формализованное описание границ информационной системы, ее основных функций, категорий пользователей, а также персонала, принимающего участие в обследовании.

Риск определяется как – возможность потерь в результате какого-либо действия или события, способного нанести ущерб.

На стадии идентификации и оценки ресурсов, **Identification and Valuation of Assets**, описывается и анализируется все, что касается идентификации и определения ценности ресурсов системы. В конце этой стадии заказчик исследования будет знать, удовлетворит

ли его существующая традиционная практика или он нуждается в проведении полного анализа рисков. В последнем случае будет построена модель информационной системы с позиции информационной безопасности.

Критерии оценки ценности ресурсов:

- Ущерб для репутации организации
- Безопасность персонала
- Разглашение персональных сведений
- Разглашение коммерческих сведений
- Неприятности со стороны правоохранительных органов
- Финансовые потери
- Невозможность нормальной работы организации

Стадия оценивания угроз и уязвимостей, **Threat and Vulnerability Assessment**, не является обязательной, если заказчика удовлетворит базовый уровень информационной безопасности. Эта стадия выполняется при проведении полного анализа рисков. Принимается во внимание все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. В конце стадии заказчик получает идентифицированные и оцененные уровни угроз и уязвимостей для своей системы.

Основные шаги:

- Идентификация угроз ресурсов и возможных уязвимостей.
- Группировка по угрозам или воздействиям с целью минимизации объема работы по анализу рисков.
- Измерение рисков.
- Получение отчета и обсуждение результатов с заказчиками.
- Коррекция по результатам обсуждения.

Оценка риска выполняется по двум факторам: вероятность реализации и размер ущерба.

$$Риск = P_{реализации} \cdot Ущерб$$

Дальнейшая детализация вероятности реализации

$$P_{реализации} = P_{угрозы} \cdot P_{уязвимости}$$

Угроза – действие или событие, способное нанести ущерб безопасности.

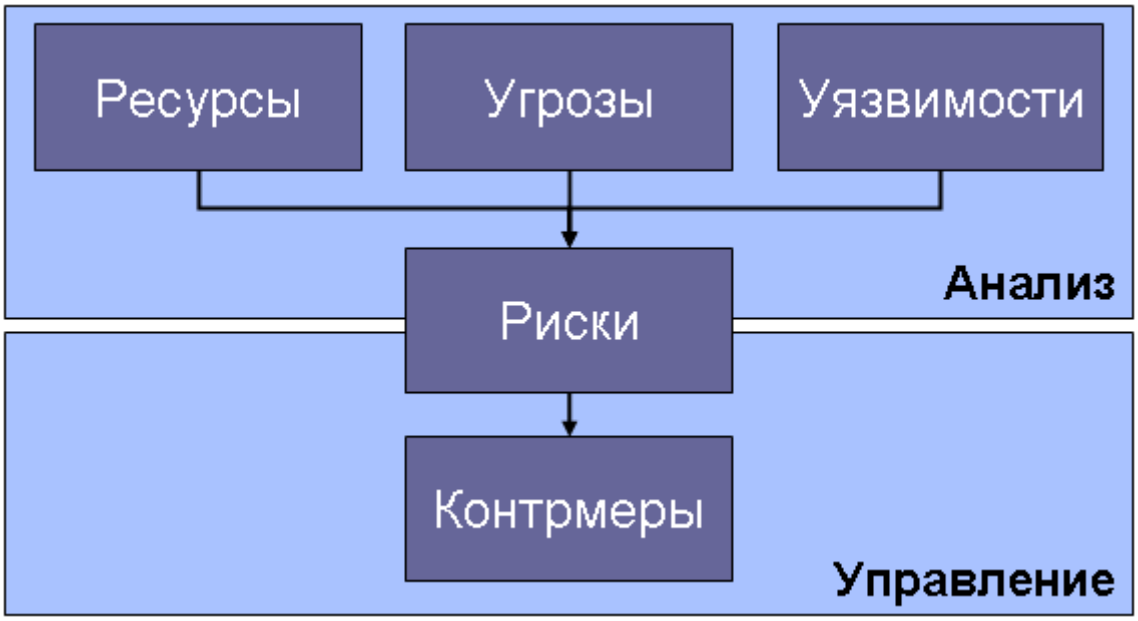
Уязвимость – слабость в защите ресурса или группы ресурсов, допускающая возможность реализации угрозы.

Стадия анализа рисков, **Risk Analysis**, позволяет оценить риски либо на основе сделанных оценок угроз и уязвимостей при проведении полного анализа рисков, либо путем использования упрощенных методик для базового уровня безопасности.

На стадии управления рисками, **Risk Management**, производится поиск адекватных контрмер. По существу речь идет о нахождении варианта системы безопасности, наилучшим образом удовлетворяющей требованиям заказчика. В конце стадии он будет знать, как модифицировать систему в терминах мер уклонения от риска, а также путем выбора специальных мер противодействия, ведущих к снижению или минимизации оставшихся рисков.
Выбор контрмер. Основные шаги:

- Генерация вариантов контрмер.
- Выбор подходящих вариантов и анализ их эффективности.
- Сравнительный анализ различных вариантов (What if)
- Получение отчета и обсуждение результатов с заказчиками.
- Коррекция по результатам обсуждения.

Каждая стадия объявляется законченной после детального обсуждения и согласования результатов с заказчиком.



Достоинства и недостатки метода CRAMM

Достоинства:

- хорошо апробированный метод
- удачная система моделирования ИТ
- обширная БД для оценки рисков и выбора контрмер
- возможность использования как средства аудита

Недостатки:

- большой объем отчетов
- сравнительно высокая трудоемкость

Таким образом, рассмотренная методика анализа и управления рисками полностью применима и в российских условиях. ПО анализа рисков существенно снижает трудоемкость выполнения всех этапов анализа рисков. Применение ПО целесообразно при проведении внешнего и внутреннего аудита информационной безопасности. При этом использование ПО требует высокой квалификации аналитика, достаточно длительного периода обучения и опыта применения.
Метод может быть использован как деятельность в любом процессе требующем оценки рисков и выбора контрмер например: управление инцидентами, проблемами (особенно в части проактива), изменениями, непрерывностью, безопасностью, и др.

Имея в арсенале вашей процессной модели процесс управления рисками можно значительно повысить эффективность и рациональность остальных процессов, а например, такие как, управление безопасностью и непрерывностью в принципе не мыслимы без зрелого управления рисками.

Каким образом управление рисками связано с другими процессами управления ИТ сервисами, и какие еще существуют методы оценки рисков, мы рассмотрим в следующих наших заметках.

Дополнительная информация по методу CRAMM:
http://www.cramm.com/downloads/datasheets.htm