IRADD

«BCM-Analyser». Математические принципы и методы

В отличие от аналогов, «BCM-Analyser» характеризуется следующими возможностями:

- обеспечивает автоматический поиск наиболее оптимального решения минимизирующего риск. Для определения оптимального решения пользователю теперь не нужно решать практически не решаемую задачу, так как поиск оптимального решения произведет программный комплекс;
- позволяет значительно повысить точность вычисления возможных рисков и оптимальных способов воздействия на них, за счет более полного учета реальных характеристик контрмер – стоимости внедрения и эксплуатации, эффективности конкретных функций, зависимостей с другими контрмерами и т.п.;
- позволяет использовать данное средство не только для расчета рисков информационной безопасности, но и в любых других областях, в которых требуется принятие решения среди множества альтернатив. Например, выбор способов охраны территорий и помещений, грузов и ценностей, способов обнаружения и тушения пожаров, есть задачи неразрывно связанные с задачами, решаемыми в области информационной безопасности, что требует единого подхода к анализу и обработке рисков;
- унифицирует используемые способы минимизации рисков и зависимости между ними, позволяет задавать контрмеры, реализующие любую из возможных стратегий воздействия на риск (принятие, уменьшение, перенос или избежание риска).

Для реализации данных возможностей в «BCM-Analyser» заложены основные математические принципы и методы представленные ниже.

Этапы работы с «BCM-Analyser» включают следующую последовательность действий:

1. Выявление сущностей (помещений, машины, оборудования, вычислительной техники, информации, людей и других активов, которые могут использоваться для осуществления какой-либо деятельности).
2. Определение свойств сущностей. Свойства сущностей – характеристики сущностей, от состояния которых зависит возможность эффективного использования сущности для осуществления рассматриваемого вида деятельности. Пример свойств – целостность сущности, доступность (наличие в нужном месте в нужное время), конфиденциальность сущности-информации
3. Определение потенциального ущерба, который будет нанесен бизнесу при нарушении каждого из выявленных свойств.
4. Определение угроз, которые влияют на данные свойства.
5. Определение показателей угроз.
6. Определение возможных контрмер.
7. Определение показателей контрмер.
8. Определение показателей системы защиты.
9. Выбор оптимального варианта системы защиты от рисков.

Этап 1. На этапе выявления сущностей производится определение максимально возможного состава сущностей, от которых зависит эффективность функционирование рассматриваемого вида деятельности.

Этап 2. На этапе определения свойств сущностей, для каждой сущности определяются все возможные свойства, нарушение которых потенциально может нанести ущерб эффективности функционирования рассматриваемого вида деятельности

Этап 3. На этапе определения потенциального ущерба, по каждому свойству каждой сущности определяется ожидаемый размер ущерба, который будет нанесен деятельности при нарушении каждого из этих свойств. Ущерб, в общем случае, есть функция времени. Ущерб определяется в единицах (денежных, либо условных). При определении ущерба не учитывается возможность использования каких-либо контрмер. Определение ущерба может производиться любым путем, который дает приемлемый для целей оптимизации результат (аналитическим, статистическим и т.п.). Ущерб S_{los} по каждому свойству каждой сущности может быть представлен в виде функции 1.

$$S_{los} = S_u^o(t), \qquad (1)$$

где o - сущность, $o \in O$,

u - свойство данной сущности, $u \in U$,

t - время от реализации угрозы.

Этап 4. На этапе определения угроз, которые могут воздействовать на сущности, выявляются все возможные угрозы, которые могут нарушить свойства сущностей и, соответственно, нанести ущерб эффективности функционирования рассматриваемого вида деятельности.

Этап 5. На этапе определения показателей угроз определяется:

- вероятность реализации каждой из угроз (V_y);
- ожидаемое время действия угроз, при условии отсутствия контрмер, на свойство u данной сущности o за промежуток времени T - (t_k^u).

Вероятность реализации угроз, время может определяться любым доступным способом, в том числе, могут использоваться следующие методы:

- аналитический, посредством расчета значений;
- статистический, посредством применения статистики возникновения угроз в аналогичных видах деятельности;
- экспертный, посредством сбора и обработки мнений экспертов в предметной области.

Этап 6. На этапе определения возможных контрмер выявляется максимально возможное количество контрмер (правовых, финансовых, страховых, организационных, технических, организационно-технических и других мер и средств), которые могут позволить реализовать хотя бы одну из стратегий управления рисками в отношении выявленных на этапе 4 угроз и применимых в отношении выявленных на этапе 1 сущностей.

Этап 7. Этап определения показателей контрмер заключается в задании для каждой контрмеры следующих показателей:

- показателя стоимости контрмеры;
- функций, которые реализует контрмера для снижения ущерба от угроз;
- показателей, характеризующих эффективность контрмеры;
- зависимостей между функциями контрмеры и функциями других контрмер.

При задании показателя стоимости контрмеры S_k^T определяются величины следующих затрат:

- постоянных затрат на эксплуатацию контрмеры;
- разовых затрат, например, на внедрение, применение, установку, закупку и т.п. контрмеры;
- затрат на контрмеру, появляющихся в случае использования этих контрмер для нейтрализации угроз (к таким затратам относится, например, стоимость вызова ремонтной организации);
- других возможных видов затрат связанных с использованием контрмеры.

Исходя из заданных затрат, показатель стоимости контрмеры рассчитывается по следующей формуле:

$$S_k^T = \sum_{i=1}^{n} S_i^T \ , \qquad (2)$$

где k - номер контрмеры,

n - общее количество возможных видов затрат,

S_i^T - затраты вида i, которые могут быть понесены за период времени T.

При задании показателей, характеризующих эффективность контрмеры, по каждой контрмере определяются:

- по каждой функции f контрмеры, по каждой угрозе к снижению ущерба от которой она приводит, вероятность того, что контрмера не сможет успешно выполнить данную функцию - V_f^y;
- время, необходимое на реализацию каждой из функций t_f во время которого угроза наносит ущерб деятельности.

Вероятности могут определяться любым доступным способом, в том числе, могут использоваться следующие методы:

- аналитический, посредством расчета значений вероятности;
- статистический, посредством применения статистики предотвращения угроз;

- практический, посредством проведения испытаний эффективности конкретных контрмер;
- экспертный, посредством сбора и обработки мнений экспертов в предметной области относительно величины вероятностей угроз.

Функции, которые реализуют контрмеры, и зависимости между ними могут быть представлены в виде ориентированного графа, в котором дуги есть функции, узлы результат выполнения типовых функций. Пример такого графа представлен на рисунке 1.

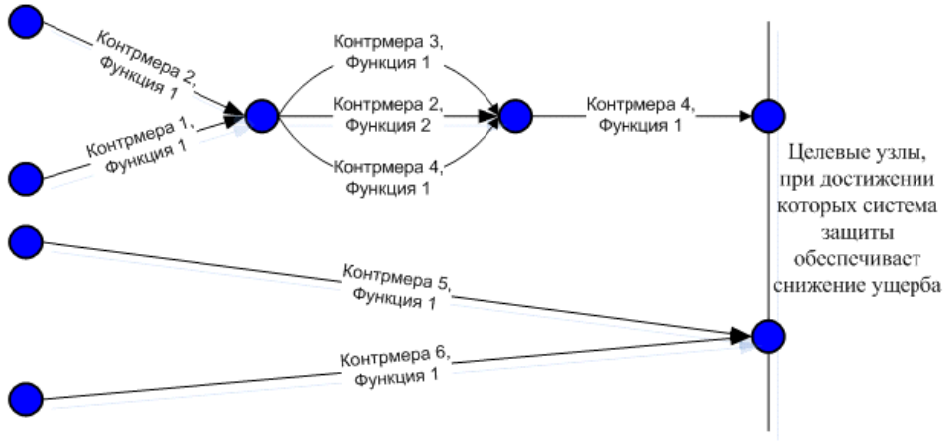

Рисунок 1 – Пример графа функций

Для нейтрализации угрозы, система защиты должна выполнить все функции соответствующие данной угрозе, т.е. пройти от начальных узлов (узлов, в которые не входит ни одна дуга) до целевых узлов.

Этап 8. Этап определения показателей системы защиты выполняется в целом для варианта системы защиты от рисков. Каждый вариант системы защиты от рисков может включать произвольное количество контрмер (определенных на этапе 6) или не включать их совсем. Каждый вариант системы защиты, в общем случае, характеризуется совокупностью следующих показателей:

- Стоимостным показателем.
- Показателем, характеризующим остаточный риск.
- Показателем, характеризующим остаточный ущерб.

Этап 8 выполняется автоматически.

Стоимостной показатель

Стоимостной показатель определяет совокупную стоимость владения вариантом системы защиты от рисков S_{tco}^{T} за заданный промежуток времени T (на основе данных определенных на этапе 7). Расчет стоимостного показателя производится по следующей формуле:

$$S_{tco}^{T} = \sum_{k=1}^{K} S_{k}^{T} \ , \qquad (3)$$

где K - общее количество контрмер.

Показатель, характеризующий остаточный риск

Показатель, характеризующий остаточный риск S_{or}^{T}, при условии использования данного варианта системы защиты от рисков, в данный промежуток времени T, рассчитывается (на основе данных определенных на предыдущих этапах) по следующей формуле.

$$S_{or}^{T} = \sum_{o=1}^{n} \sum_{u=1}^{x} (S_{o}^{u}(t_k) \times \sum_{y=1}^{m} (V_y \times V_s)) \, , \qquad (4)$$

где

o - номер сущности из сущностей определенных на этапе 1,

n - общее количество сущностей определенных на этапе 1,

u - номер свойства данной сущности o;

x - общее количество свойств, у данной сущности o, определенное на этапе 2,

y - номер угрозы влияющей на данное свойство u данной сущности o;

m - общее количество угроз влияющих на данное свойство u данной сущности o;

$S_{u}^{o}(t_k^u)$ - значение функции ущерба (определенной на этапе 3) по данному свойству u данной сущности o в значение времени t_k^u;

V_s - вероятность того, что вариант системы защиты не сможет снизить ущерб от угрозы y в случае ее проявления, рассчитываемая по следующему алгоритму.

1. Для каждого узла графа функций системы защиты, последовательно, начиная с определенных узлов, находится вероятность не достижения данного узла j по формуле (5). Итоговый результат этапа – нахождение вероятности не достижения каждого из целевых узлов системы защиты $V_{j,p}$.

$$V_j = \prod^{\forall i} (V_i + \prod^{\forall f_{i,j}} V_{f_{i,j}}^{y} - V_i \times \prod^{\forall f_{i,j}} V_{f_{i,j}}^{y}) \, , \qquad (5)$$

где

i - номер смежного узла, из которого входит дуга в данный узел j;

$f_{i,j}$ - функция контрмеры, направленная из узла i в узел j, в общем случае более чем одна;

V_i - вероятность неблагоприятного результата выполнения типовых функций входящих в узел i, для узлов, в которые не входит ни одна дуга, равна 0. Узлы, в которые не входит ни одна дуга далее называются «начальными узлами»;

$V_{f_{i,j}}^{y}$ - вероятность, не выполнения данной функции $f_{i,j}$ системы.

2. Нахождение вероятности того, что вариант системы защиты не сможет снизить ущерб от угрозы y в случае ее проявления V_s, по формуле 6.

$$V_s = \prod^{\forall(j,p)} V_{j,p}, \qquad (6)$$

где (j,p) - целевой узел.

Показатель, характеризующий остаточный ущерб

Показатель, характеризующий остаточный ущерб S_{oy}^{T}, при условии использования данного варианта системы защиты от рисков, в данный промежуток времени T рассчитывается (на основе данных определенных на этапе 7) по формуле (7).

$$S_{oy}^{T} = \sum_{o=1}^{n}\sum_{u=1}^{x}\sum_{y=1}^{m}\left(\frac{\sum_{k=1}^{K}\left(\left(S_o^u\left(\sum^{\forall t_f \in K_c} t_f\right) + \sum^{\forall k \in K_c} S_{f,k}\right) \times V_c\right)}{N} \times V_y\right) \qquad (7)$$

где

$S_{f,k}$ - стоимость реализации данной функции контрмеры, в случае ее использования для воздействия на угрозу;

K_c - маршрут от начального узла до целевого, при реализации которого обеспечивается нейтрализация данной угрозы y;

$\forall t_f \in K_c$ - выражение, описывающее все значения t_f функций в данном маршруте K_c;

K - общее множество вариантов маршрутов, при реализации любого из которых обеспечивается нейтрализация данной угрозы y в данном варианте построения системы защиты;

k - номер маршрута из множества K ;

N - количество маршрутов в множестве K ;

V_c - вероятность того, что для нейтрализации ущерба от угрозы сработает данный маршрут K_c, рассчитываемая по формуле (8).

$$V_c = 1 - \sum^{\forall f_{i,j} \in K_c} V_{f_{i,j}} \qquad (8)$$

Этап 9. На этапе выбора оптимального варианта системы защиты от рисков, для различных вариантов организации системы защиты от рисков, производится расчет величины S_z по формуле (9), на основе формул определенных на этапе 8.

$$S_z = S_{tco}^T + S_{or}^T + S_{oy}^T, \qquad (9)$$

где z - номер варианта организации системы защиты от рисков.

Генерация вариантов организации системы защиты от рисков может производиться произвольным способом, например:

- путем полного перебора всех возможных вариантов. Данный способ дает возможность поиска наиболее оптимального варианта системы защиты от рисков, однако, при большом количестве контрмер, требует значительного машинного времени;
- путем использования любого возможного метода оптимизации перебора. Данный способ также дает возможность поиска наиболее оптимального варианта системы защиты от рисков, но, возможно, с некоторой погрешностью;
- путем произвольного задания вариантов, что дает возможность проверки эффективности конкретных вариантов организации системы защиты от рисков.

Поиск оптимального варианта организации системы защиты от рисков заключается в нахождении такого варианта z, при котором значение S_z минимально.