

ОПТИМИЗАЦИЯ РАСПРЕДЕЛЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТЕ¹

Вопросам проектирования систем защиты информации (СЗИ) посвящено достаточно много различных работ. В частности, методология проектирования СЗИ четко сформулирована в монографии В. А. Герасименко [1] и в дальнейшем развита в учебнике [2].

Не вдаваясь в подробное описание методов проектирования, которое читатель может изучить самостоятельно, прочитав, например, соответствующую главу учебника [2], мы сосредоточим здесь внимание на принципиальных вопросах оценки эффективности процессов защиты, реализуемых создаваемой СЗИ.

На основе изложенного в [3] энтропийного подхода может быть построена модель решения данной задачи, сходная по своей постановке с моделью анализа гравитационного взаимодействия системы материальных точек.

Пусть T_{lr} — количественная оценка эффективности средств защиты, находящихся в l -й зоне защищаемого объекта и используемых в СЗИ для противодействия r -й потенциальной угрозе; Q_l — полная эффективность всех средств защиты, находящихся в l -й зоне объекта; D_r — необходимая эффективность защиты для гарантированного противодействия r -й угрозе (фактически это количественная оценка угрозы). В качестве ресурсной переменной рассматриваемой системы можно задать C_{lr} — усредненные затраты на реализацию средств защиты, находящихся в l -й зоне объекта и нацеленных на противодействие r -й угрозе, плюс затраты на ликвидацию последствий в случае реализации угрозы.

Естественно, что количественные оценки всех введенных нами переменных могут быть получены исключительно с использованием тех или иных методов экспертных оценок. Более того, используемые нами в дальнейших выкладках методы, основанные на энтропийном подходе, требуют, чтобы величины T_{lr} , Q_l и D_r были выражены целыми натуральными числами. Этого легко добиться, присвоив их значениям определенный ранг, который будет характеризовать эффективность определенным количеством условных единиц.

По аналогии с гравитационной моделью Ньютона интересующая нас модель оценки эффективности защиты может быть представлена в виде

$$T_{lr} = k \frac{Q_l D_r}{C_{lr}^2}, \quad (1)$$

где k — некоторая константа, а затраты на реализацию выступают в качестве «расстояния».

Однако у этого уравнения имеется очевидный недостаток: если удвоить заданные значения Q_l и D_r , то эффективность противодействия угрозам учетверится, а естественно ожидать, что она лишь удвоится. Чтобы избежать этого недостатка, величины T_{lr} всегда должны удовлетворять следующим ограничениям:

$$\begin{aligned} \sum_r T_{lr} &= Q_l, \\ \sum_l T_{lr} &= D_r. \end{aligned} \quad (2)$$

Этим ограничениям можно удовлетворить, если ввести наборы констант A_l и B_r , связанные соответственно со средствами защиты l -й зоны объекта и r -й угрозой. Назовем их балансирующими

¹ Данная работа выполнена в НИЯУ МИФИ при финансовой поддержке Министерства образования и науки Российской Федерации в рамках проекта «Создание инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных средств защиты информации на базе перспективных высокоскоростных интерфейсов информационного взаимодействия», выполняемого совместно с ООО «ОКБ САПР».



множителями. Кроме того, нет оснований считать, что «расстояние» играет в уравнении (1) такую же роль, как и в ньютоновской физике, поэтому введем более общую функцию «расстояния» в виде некоторой «ресурсной» функции $f(C_{lr})$. Модифицированная гравитационная модель примет, таким образом, следующий вид:

$$T_{lr} = A_l B_r Q_l D_r f(C_{lr}), \quad (4)$$

$$\text{где } A_l = \left[\sum_r B_r D_r f(C_{lr}) \right]^{-1};$$

$$B_r = \left[\sum_l A_l Q_l f(C_{lr}) \right]^{-1}.$$

Уравнения для A_l и B_r решаются традиционными методами, и можно легко проверить, что они гарантируют удовлетворение ограничениям (2) и (3). Величины C_{lr} в этой модели могут служить общей мерой сопротивления реализации r -й угрозы в l -й зоне объекта. Поскольку оценка этой меры производится экспертами с учетом не только стоимости защиты, но и таких параметров, как вероятность проявления угрозы, время ее реализации и др., то назовем C_{lr} «обобщенными затратами».

Введем также дополнительное к (2) и (3) ограничение на T_{lr} , имеющее вид:

$$\sum_l \sum_r T_{lr} C_{lr} = U, \quad (5)$$

где U — полный ресурс системы.

Перейдем теперь к основной цели нашего исследования и определим необходимое распределение T_{lr} , максимизируя энтропию системы, выраженную в виде [4]:

$$\ln W(\{T_{lr}\}) = \ln T! - \sum_l \sum_r \ln T_{lr}!, \quad (6)$$

где $W(\{T_{lr}\})$ — полное число состояний системы, соответствующее распределению $\{T_{lr}\}$; T — полная эффективность всех средств защиты объекта, выраженная, как это было принято нами выше, в условных единицах и представляющая сумму рангов эффективности указанных средств.

Для получения набора T_{lr} , максимизирующего $\ln(\{T_{lr}\})$ из уравнения (6) при ограничениях (2), (3) и (5), следует максимизировать лагранжиан, равный

$$L = \ln W + \sum_l \lambda_l (Q_l - \sum_r T_{lr}) + \sum_r \lambda_r (D_r - \sum_l T_{lr}) + \mu (U - \sum_l \sum_r T_{lr} C_{lr}), \quad (7)$$

где λ_l , λ_r и μ — множители Лагранжа.

Поскольку предполагается, что T_{lr} достаточно велики, можно воспользоваться формулой Стирлинга, согласно которой

$$\ln T_{lr} = T_{lr} \ln T_{lr} - T_{lr}. \quad (8)$$

Тогда из (6) получим

$$\ln W = - \sum_l \sum_r T_{lr} \ln T_{lr}. \quad (9)$$

Значения T_{lr} , которые доставляют максимум L и, следовательно, являются искомым распределением средств защиты по зонам объекта и потенциальным угрозам, представляют собой решение системы уравнений

$$\frac{\delta L}{\delta T_{lr}} = 0 \quad (10)$$

совместно с ограничениями (2), (3) и (5).

Дифференцируя (7), будем иметь

$$\frac{\delta L}{\delta T_{lr}} = - \ln T_{lr} - \lambda_l - \lambda_r - \mu C_{lr}. \quad (11)$$



Это выражение равно нулю, когда

$$T_{lr} = \exp(-\lambda_l - \lambda_r - \mu C_{lr}). \quad (12)$$

Подставляя (12) в (2) и (3), получим

$$\exp(-\lambda_l) = Q_l \left[\sum_r \exp(-\lambda_r) - \mu C_{lr} \right]^{-1}, \quad (13)$$

$$\exp(-\lambda_r) = D_r \left[\sum_l \exp(-\lambda_l) - \mu C_{lr} \right]^{-1}. \quad (14)$$

Чтобы представить окончательный результат в более привычном виде, запишем

$$A_l = \frac{1}{Q_l} \exp(-\lambda_l), \quad (15)$$

$$B_r = \frac{1}{D_r} \exp(-\lambda_r). \quad (16)$$

Отсюда

$$T_{lr} = A_l B_r Q_l D_r \exp(-\mu C_{lr}), \quad (17)$$

где в соответствии с уравнениями (13)–(16) имеем

$$A_l = \left[\sum_r B_r D_r \exp(-\mu C_{lr}) \right]^{-1}, \quad (18)$$

$$B_r = \left[\sum_l A_l Q_l \exp(-\mu C_{lr}) \right]^{-1}. \quad (19)$$

Таким образом, искомое распределение описывается модифицированной гравитационной моделью с наперед заданной функцией f . Величина μ , характеризующая среднее значение затрат на одну условную единицу эффективности средств защиты, определяется из системы ограничений задачи. В случае одинаковой эффективности применяемых средств защиты величина μ будет характеризовать среднюю эффективность их применения против конкретных угроз. В итоге нами получен показатель эффективности средств защиты, который учитывает не только суммарную эффективность применяемых средств защиты, но и их оптимальное распределение по зонам защищаемого объекта или системы исходя из наиболее эффективного противодействия потенциальным угрозам безопасности информации.

СПИСОК ЛИТЕРАТУРЫ:

1. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. Кн. 1 и 2. М.: Энергоатомиздат, 1994.
2. Герасименко В. А., Малюк А. А. Основы защиты информации: учебник. М.: МИФИ, 1997.
3. Малюк А. А. Энтропийный подход к моделированию систем и процессов защиты информации // Безопасность информационных технологий. 2011. № 4. С. 15–19.
4. Вильсон А. Энтропийные методы моделирования сложных систем / Пер. с англ. М.: Наука, 1978.

