А. А. Малюк

К ВОПРОСУ О ФОРМИРОВАНИИ ОПТИМАЛЬНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Целью данной статьи является анализ возможных подходов к оптимизации системы защиты информации (СЗИ). Не вдаваясь в исследование методов проектирования СЗИ, сведения о которых читатель может почерпнуть, например, в работе [1], мы сосредоточим здесь внимание на принципиальных вопросах оценки эффективности процессов защиты, реализуемых создаваемой системой.

На основе изложенного в [2] энтропийного подхода может быть построена модель решения данной задачи, сходная по своей постановке с задачей анализа гравитационного взаимодействия системы материальных точек.

Представим защищаемый объект или систему в виде n-рубежной модели защиты. Пусть при этом 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.

Количественные оценки всех введенных нами переменных могут быть получены с использованием тех или иных методов экспертных оценок. При этом 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 некоторым количеством условных единиц.

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

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

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:

$$\sum_r T_{lr} = Q_l, \qquad (2)$$

$$\sum_l T_{lr} = D_r. \qquad (3)$$

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 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 будет иметь, таким образом, следующий вид:

$$T_lr = A_l B_r Q_r D_r f(C_{lr}), \tag{4}$$

где $$A_l = \left[\sum_r B_r D_r f(C_{lr}) \right]^{-1}, \tag{5}$$

$$B_r = \left[\sum_l A_l Q_l f(C_{lr}) \right]^{-1}. \tag{6}$$

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:

$$\sum_l \sum_r T_{lr} C_{lr} = U, \tag{7}$$

где U — полный ресурс системы.

Перейдем теперь к основной цели нашего исследования и определим необходимое распределение T_{lr}, максимизируя энтропию системы, выраженную в виде [3]:

$$ln\, W(\{T_{lr}\}) = ln\, T! - \sum_l \sum_r ln\, T_{lr}!, \tag{8}$$

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 (8) при ограничениях (2), (3) и (7), следует максимизировать лагранжиан, равный

$$L = ln\, W + \sum_l \lambda_l (Q_l - \sum_r T_{lr}) + \sum_r \lambda_r (D_r - \sum_l T_{lr}) + \mu (U - \sum_l \sum_r T_{lr} C_{lr}), \tag{9}$$

где λ_l, λ_r и μ — множители Лагранжа.

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

$$ln\ T_{lr} = T_{lr} ln\ T_{lr} - T_{lr}. \tag{10}$$

Тогда из (8) получим

$$\ln W = -\sum_l \sum_r T_{lr} \ln T_{lr}\ . \tag{11}$$

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

$$\frac{\delta L}{\delta T_{lr}} = 0. \tag{12}$$

совместно с ограничениями (2), (3) и (7).

Дифференцируя (9), будем иметь

$$\frac{\delta L}{\delta_{lr}} = -\ln\ -\lambda_\lambda - \lambda_r - \mu C_{lr`}. \tag{13}$$

Это выражение равно нулю, когда

$$T_{lr} = exp(-\lambda_\lambda - \lambda_r - \mu C_{lr`}). \tag{14}$$

Подставляя (14) в (2) и (3), получим

$$exp(-\lambda_l) = Q_l\left[\sum_r exp(-\lambda_r) - \mu C_{lr`}\right]^{-1}, \quad (15)$$

$$exp(-\lambda_r) = D_r\left[\sum_l exp(-\lambda_l) - \mu C_{lr`}\right]^{-1}. \quad (16)$$

Чтобы представить окончательный результат в более привычном виде, запишем

$$A_l = \frac{1}{Q_l} exp(-\lambda_l), \quad (17)$$

$$B_r = \frac{1}{D_r} exp(-\lambda_r). \quad (18)$$

Отсюда

$$T_{lr} = A_l B_r Q_l D_r \, exp(-\mu C_{lr}), \quad (19)$$

где в соответствии с уравнениями (15)—(18) имеем

$$A_l = \left[\sum_r B_r D_r \, exp(-\mu C_{lr})\right]^{-1}, \quad (20)$$

$$B_r = \left[\sum_l A_l Q_l \, exp(-\mu C_{lr})\right]^{-1}. \quad (21)$$

Таким образом, искомое распределение описывается модифицированной гравитационной моделью с заранее 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., Малюк А. А.* Основы защиты информации. М.: МИФИ, 1997.
2. *Малюк А. А.* Энтропийный подход к моделированию систем и процессов защиты информации // Безопасность информационных технологий. 2011. № 4. С. 15–19.
3. *Вильсон А.* Энтропийные методы моделирования сложных систем / Пер. с англ. М.: Наука, 1978.