2 Забезпечення комп'ютерної безпеки в державних, банківських та інших інформаційних системах

УДК 004.056.5

КОЛИЧЕСТВЕННЫЕ ОЦЕНКИ КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Денис Кудин, Владислав Корольков*
Центр информационной безопасности,
** Запорожский национальный технический университет*

Аннотация: **Рассмотрена постановка формальной задачи синтеза оптимальной системы защиты информации и дано обоснование показателей качества ее функционирования.**
Summary: **This paper examines the formal task to synthesize an optimal information security system and substantiates the quality coefficients of this system's performance.**
Ключевые слова: **Информационная система, защита информации, угроза, модель, ущерб, вероятность.**

I Введение

Оценки параметров системы защиты информации (СЗИ) в условиях высокой степени неопределенности условий ее функционирования должны вычисляться с использованием не одной математической модели, а согласованного семейства моделей, адаптивно конструирующихся одна из другой и, таким образом, непрерывно совершенствующихся на основе оптимального выбора исходных данных.

Согласно [1], при синтезе систем защиты исходными должны являться следующие положения:

- выбор математически продуктивного критерия оптимальности в соответствии с архитектурой системы защиты и технологией обработки информации в информационной системе (ИС);
- четкая математическая формулировка задачи, учитывающая все априорные сведения и позволяющая решить ее в соответствии с принятым критерием.

Итогом решения задачи синтеза оптимальной системы защиты и его конечной целью должны быть следующие результаты:

- архитектура системы защиты;
- количественная оценка качества ее функционирования;
- оценка практической чувствительности разработанных моделей к отклонениям от априорных данных;
- физическая реализуемость синтезируемых систем защиты в современных системах обмена данными (соответствие технологии обработки информации уровню ее защиты).

Целью данной статьи является рассмотрение формальной задачи синтеза СЗИ и показателей качества функционирования СЗИ, таких как вероятность появления угроз, вероятность устранения угроз, предотвращенный ущерб за счет ликвидации угроз.

II Обоснование показателя качества СЗИ

Злоумышленник с помощью некоторого источника угроз (ИУ) генерирует совокупность угроз ИС (пусть она будет конечной и счетной, $i = \overline{1,n}$). Каждая *i*-я угроза характеризуется вероятностью появления $2^{L_H/2}$ и ущербом $g^1 g^1 = g^{(k+1)\max(2^k-1)}$, приносимым информационной системе [1–3].

Система защиты информации выполняет функцию полной или частичной компенсации угроз для ИС. Основной характеристикой СЗИ является вероятность устранения каждой *i*-й угрозы $d^{n-1} \equiv 1 (\mathrm{mod}\, n)$.

За счет функционирования СЗИ обеспечивается уменьшение ущерба W, наносимого ИС воздействием угроз. Обозначим общий предотвращенный ущерб ИС через W, а предотвращенный ущерб за счет ликвидации *i*-й угрозы через $\overline{\omega}_i$.

После введенных обозначений можно сформулировать в общем виде задачу синтеза системы защиты информации в ИС. Необходимо выбрать вариант реализации СЗИ, обеспечивающий максимум предотвращенного ущерба от воздействия угроз при допустимых затратах на СЗИ.

Формальная постановка задачи имеет вид: найти

$$T^0 = \operatorname{argmax}\overline{W}(T)$$
$$T^0 \in T^+ \tag{1}$$

при ограничении

$$C(T^0) \le C_{доп}. \tag{2}$$

Здесь T – некоторый вектор, характеризующий вариант технической реализации СЗИ, T^+, T^0 –допустимое и оптимальное значение вектора T; $C_{доп}$ – допустимые затраты на СЗИ.

Для решения задачи необходимо, прежде всего, сформировать показатель качества функционирования СЗИ $\overline{W}(T)$.

Предотвращенный ущерб выражается в, общем виде, соотношением:

$$\overline{W} = F\left(P_{iугр}; \Delta q_i^{угр}; P_{iугр}^{устр}; i = \overline{1,n}\right). \tag{3}$$

Предотвращенный ущерб за счет ликвидации воздействия *i*-й угрозы:

$$\overline{\omega}_i = P_{iугр} \cdot \Delta q_i^{угр} \cdot P_{iугр}^{устр}; i = \overline{1,n}. \tag{4}$$

При условии независимости угроз и аддитивности их последствий получаем

$$\overline{W} = \sum_{i=1}^{n} P_{iугр} \cdot \Delta q_i^{угр} \cdot P_{iугр}^{устр}. \tag{5}$$

Рассмотрим более подробно сомножители, входящие в (5).

Вероятность появления *i*-й угрозы $P_{iугр}$ определяется статистически и соответствует относительной частоте ее появления

$$P_{iугр} = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i} = \overline{\lambda}_i, \tag{6}$$

где λ_i – частота появления *i*-й угрозы.

Ущерб, приносимый *i*-й угрозой $\Delta q_i^{угр}$, может определяться в абсолютных единицах: экономических потерях, временных затратах, объеме уничтоженной или испорченной информации и т. д.

Однако, практически это сделать весьма затруднительно, особенно на ранних этапах проектирования СЗИ. Поэтому целесообразно вместо абсолютного ущерба использовать относительный ущерб, который, по сути, представляет собой степень опасности *i*-й угрозы для ИС. Степень опасности может быть определена экспертным путем в предположении, что все угрозы для ИС составляют полную группу событий, т. е.

$$0 \le \Delta q_i \le 1;$$
$$\sum_{i=1}^{n} \Delta q_i = 1. \tag{7}$$

Наиболее сложным вопросом является определение вероятности устранения *i*-й угрозы $P_{iугр}^{устр}$ при проектировании системы защиты информации. Сделаем допущение, что эта вероятность определяется тем, насколько полно учтены качественные и количественные требования к СЗИ при их проектировании, т. е.

$$P_{iугр}^{устр} = f_i\left(x_{i1},\ldots,x_{ij},\ldots,x_{im}\right), \tag{8}$$

где x_{ij} – степень выполнения *j*-го требования к СЗИ для устранения *i*-й угрозы, $i = \overline{1,n}; j = \overline{1,m}$.

Пусть первые *k* требований будут количественными $(j = \overline{1,k})$, а остальные $m - k$ – качественными $(j = \overline{k+1,m})$. Степень выполнения *j*-го количественного требования определяется его близостью к требуемому (оптимальному) значению. Для оценки степени выполнения *j*-го количественного требования к

СЗИ удобнее всего использовать его нормированное значение $x_{ij}\left(j=\overline{1,k}\right)$; $0 \le x_{ij} \le 1$. При этом для нормирования удобно использовать функцию вида

$$\bar{x}_{ij} = \frac{x_{ij} - x_{ij}^{нх}}{x_{ij}^{нл} - x_{ij}^{нх}}, \tag{9}$$

где x_{ij} – текущее значение *j*-го требования; $x_{ij}^{нл}, x_{ij}^{нх}$ – наилучшее и наихудшее значения соответственно.

С учетом (9) получаются следующие расчетные соотношения:

– при $x_{ij}^{нл} = x_{ij\max}; x_{ij}^{нх} = x_{ij\min}$:

$$\bar{x}_{ij} = \frac{x_{ij} - x_{ij\min}}{x_{ij\max} - x_{ij\min}}; \tag{10}$$

– при $x_{ij}^{нл} = x_{ij\min}; x_{ij}^{нх} = x_{ij\max}$:

$$\bar{x}_{ij} = \frac{x_{ij\max} - x_{ij}}{x_{ij\max} - x_{ij\min}}. \tag{11}$$

$$\bar{x}_{ij} = \begin{cases} 0, & при \quad x_{ij\min} < x_{ij} < x_{ij\max}, \\ 1, & при \quad x_{ij} = x_{ijopt}, \\ \dfrac{x_{ij} - x_{ij\min}}{x_{ijopt} - x_{ij\min}}, & при \quad x_{ij\min} \le x_{ij} \le x_{ijopt}, \\ \dfrac{x_{ij\max} - x_{ij}}{x_{ij\max} - x_{ijopt}}, & при \quad x_{ijopt} \le x_{ij} \le x_{ij\max}. \end{cases} \tag{12}$$

Степень выполнения *j*-го качественного требования определяется функцией принадлежности к наилучшему значению $\mu(x_{ij})$.

Разложив функцию (8) в ряд Маклорена и ограничившись лишь первыми членами ряда получим:

$$P_{iуp}^{устр} = P_{iуp}^{устр}(0) + \sum_{j=1}^{m} \frac{\partial P_{iуp}^{устр}}{\partial x_{ij}} \cdot x_{ij}, \tag{13}$$

где $P_{iуp}^{устр}(0) = 0$ – вероятность устранения *i*-й угрозы при невыполнении требований к СЗИ;

$\dfrac{\partial P_{iуp}^{устр}}{\partial x_{ij}} = \alpha_{ij}$ – величина, характеризующая степень влияния требования на вероятность устранения *i*-й угрозы (важность выполнения *j*-го требования для устранения *i*-й угрозы).

Очевидно, что

$$0 \le \alpha_{ij} \le 1; \sum_{j=1}^{m} \alpha_{ij} = 1 \text{ для } i = \overline{1,n}. \tag{14}$$

После подстановки в (13) соответствующих значений получим:

$$P_{iуp}^{устр} = \sum_{j=1}^{k} \alpha_{ij} \cdot \bar{x}_{ij} + \sum_{j=k+1}^{m} \alpha_{ij} \cdot \mu\left(x_{ij}\right). \tag{15}$$

Окончательно (5) для оценки величины $\overline{W}$ предотвращенного ущерба принимает вид:

$$\overline{W} = \sum_{i=1}^{n} \sum_{j=1}^{k} \bar{\lambda}_i \cdot \Delta q_i \cdot \alpha_{ij} \cdot \bar{x}_{ij} + \sum_{i=1}^{n} \sum_{j=k+1}^{m} \bar{\lambda}_i \cdot \Delta q_i \cdot \alpha_{ij} \cdot \mu\left(x_{ij}\right). \tag{16}$$

Таким образом, задача синтеза СЗИ в виде (1), (2) сводится к оптимальному обоснованию количественных и качественных требований к СЗИ при допустимых затратах и принимает вид:

$$\text{найти } \max \overline{W}\left(x_{ij};\ i=\overline{1,n};\ j=\overline{1,m}\right) \tag{17}$$

при ограничении $C\left(x_{ij}\right) \le C_{доп};\ i=\overline{1,n};\ j=\overline{1,m}$.

В работе [4] предлагается подход к формальному определению угроз информации.

В соответствии с формулировкой задачи (17) основными этапами ее решения являются:

- сбор и обработка экспертной информации о характеристиках угроз: частоте появления *i*-й угрозы $\overline{\lambda_i}$ и ущербе $\Delta q_i \ \left(i=\overline{1,n}\right)$;
- сбор и обработка экспертной информации для определения важности выполнения *j*-го требования для устранения *i*-угрозы α_{ij} и функции принадлежности $\mu\left(x_{ij}\right),\ \left(i=\overline{1,n};\ j=\overline{1,m}\right)$;
- оценка стоимости СЗИ для конкретного варианта ее реализации, зависящая от степени выполнения требований $C\left(x_{ij};\ i=\overline{1,n};\ j=\overline{1,m}\right)$;
- разработка математической модели и алгоритма выбора рационального варианта построения СЗИ (рационального задания требований) в соответствии с постановкой (17) как задачи нечеткого математического программирования.

III Выводы

В статье рассмотрен метод постановки формальной задачи синтеза системы защиты информации и основные этапы ее решения, а также показатели качества функционирования СЗИ – вероятность появления угроз, вероятность устранения угроз, предотвращенный ущерб за счет ликвидации угроз.

Литература: ***1.*** *Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты.– К.: ООО "ТИД "ДС", 2001.* ***2.*** *НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. // Департамент специальных телекоммуникационных систем и защиты информации Службы безопасности Украины. – Киев, 1999.* ***3.*** *НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. //Департамент специальных телекоммуникационных систем и защиты информации Службы безопасности Украины. – Киев, 1999.* ***4.*** *Антонюк А., Жора В. Моделювання доступу та каналів витоку в інформаційних системах //Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2001. Вип. 3. С. 156–160.*

УДК 681.3.067

ИСПОЛЬЗОВАНИЕ МУЛЬТИАГЕНТНЫХ СИСТЕМ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ КОМПЬЮТЕРНЫХ СЕТЕЙ

Александр Хошаба
Винницкий государственный технический университет

Аннотация: **Определены задачи и основные функции, стоящие перед средствами управления и контроля компьютерными сетями при защите информационных ресурсов. Детально описана структура мультиагентной системы, выполняющей защиту данных в компьютерных сетях.**
Summary: **In article problems and the basic functions which face to control facilities and the control in computer networks at protection of information resources are determined. The structure of multiagent system which carries out protection of the data in computer networks in details is described.**
Ключевые слова: **Защита информационных ресурсов компьютерных сетей, интеллектуальные технологии, мультиагентные системы.**

I Введение

В течение ряда лет в области искусственного интеллекта (ИИ) происходят революционные преобразования. Источниками этих преобразований служат распределенный искусственный интеллект (РИИ)