УДК 004.681

Егоров Ф.И., Тискина Е.О., Хорошко В.А.
Государственный университет информационно-коммуникационных технологий

ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

В современном мире информация и ее обработка играет ключевую роль в управлении и функционировании государств, организаций, компаний и предприятий. Имея доступ к нужной информации, можно правильно оценить текущую ситуацию, принять своевременное решение. Реалии современного мира таковы, что эффективность работы любой структуры (государственной или частной) напрямую зависит от качества и оперативности управления всеми процессами. В сферу управления включаются различные ресурсы – информация, персонал, технологические процессы, техника.

Однако широкое применение информационных технологий немыслимо без повышения внимания к вопросам защиты информации. Информация должна быть доступна только тем, кому она предназначена, и скрыта от сторонних наблюдателей и несанкционированного доступа. Поэтому создание систем, обеспечивающих защиту информации и процедур над ней, оценка качества проектирования и эксплуатации таких систем предполагают решение широкого круга разноплановых задач. Рассмотрим постановки некоторых основных задач защиты информации от несанкционированного доступа.

Определим следующие множества для дальнейшего анализа и исследования задач защиты информации. Множество объектов W - конечное множество элементов $w_1, w_2, ..., w_n$. J - множество индексов объектов: $J = (1, 2, ..., n)$ и при этом объекты – пассивные носители информации. Каждый объект имеет определенный (базовый) уровень защиты $J_0(w_1), \forall i \in J$, тесно связанный с целостностью объекта w_i, т.е. уровень защиты объекта соответствует стоимости $v(w_i)$ информации, содержащейся в нем.

При этом множество методов защиты M - конечное множество элементов $m_1, m_2, ..., m_k$. Под «методами» следует понимать все возможные способы и средства (организационные, технические, программные, организационно-правовые, криптографические и пр.), которые используются для защиты объектов $w_i \in W, i = 1, n$. Совокупность методов, применимых для защиты объектов w_i, назовем их объединением и обозначим

$$\bigcup_{j=1}^{K} m_j(w_i) = M(w_i), i = \overline{1, n}.$$

Обозначим через j -множество индексов всех методов защиты объекта w_i, образующих совокупность $M(w_i) : j = (1, 2, ..., k)$.

Для решения задач защиты информации введем множество подуровневой защиты L - конечное множество элементов $l_1, l_2, ..., l_k$. Каждый подуровень $l_j, 1 \le j \le k$, обеспечивается применением m_j -го метода защиты объекта $w_i \in W$, т.е.

$$\forall w_i \in W i l_j(w_i) \sim m_j(w_i), l_j \in L, m_j \in M, i \in J, j = \overline{1, k}.$$

Мощность множества L совпадает с мощностью множества $M : \|L\| = \|M\|$. Суммарный уровень защиты, обеспечиваемый совокупностью $M(w_i)$ методов защиты объекта должен быть не меньше базового уровня $J_0(w_i)$ защиты объекта w_i:

$$\forall i \in J : J(w_i) = \sum_{j \in J} l_j(w_i) \geq J_0(w_i) \quad (1)$$

Суммирование проводится лишь по тем методам, которые принадлежат объединению $M(w_i)$, используемому для защиты объекта w_i. Выражение (1) и смысловое содержание термина «уровень защиты объекта» определяют принципиальное отличие рассматриваемых здесь задач от задач создания систем защиты, описываемых в [1].

Исходя из выше сказанного, необходимо так же оценить множество стоимостей защиты $s_1, s_2, ..., s_k$. Элемент $s_j \in S, j = \overline{1,k}$ характеризует величину затрат при реализации m_j-го метода защиты объекта $w_i \in W$, и обеспечивающего l_j-й уровень защиты. Мощность множеств M, L и S совпадает: $\|M\| = \|L\| = \|S\|$.

Множество S можно рассматривать как $S = \{S_j^i\}, i = \overline{1,n}; j = 1,k,$ если предполагать, что реализация одного и того же m_j-го метода для каждой пары различных объектов $w_{i1} \neq w_{i2}, i_1 \neq i_2$, имеет различную стоимость:

$$S_j(w_{i1}) \neq S_j(w_{i2}).$$

В этом случае $\|M\| \cdot \|W\| = \|S\|$.

Введем переменную:

$$\chi^j_{(w_i)} = \begin{cases} 1, \textit{если\_применяется\_}m_j - \textit{й\_метод\_защиты} \\ \textit{объекта\_}w_i, \textit{обеспечивающий\_}l_j - \textit{й\_подуровень\_защиты}, 1 \leq j \leq k; \\ 0, \textit{в\_противном\_случае}. \end{cases}$$

Отметим, что

$$\sum_{j=1}^{k} \chi^j(w_i) \leq k. \quad (2)$$

Тогда выражение (1), определяющее уровень защиты объекта, обеспечиваемый совокупностью $M(w_i)$ методов, можно переписать в виде с учетом [2]:

$$J(w_i) = \sum_{j \in J} l_j(w_i) \chi^j(w_i) \geq J_0(w_i), i = \overline{1,n}. \quad (3)$$

Если уровень защиты субъекта (субъекты могут перемещать или изменять содержимое объектов) обозначить через J_c то, с другой стороны, должно также выполнятся условие

$$J_c(w_i) \leq J_c.$$

После определения множеств выделим основные параметры систем защиты информации. Защита объекта $w_i \in W, i = \overline{1,n}$ определяется выбором совокупности $M(w_i)$ методов $m_j(w_i), j = 1,k$, которые характеризуются подуровнем защиты $l_j(w_i)$. Вторая характеристика обеспечения защиты объекта w_i - суммарная стоимость реализации выбранных методов, которая не должна превышать базовой стоимости $S_0(w_i)$ обеспечения защиты объекта. При этом уровень защиты объекта, обеспечиваемый применением выбранной совокупности методов $M(w_i)$ защиты объекта w_i, не должен быть меньше базового уровня защиты объекта $w_i \in W$.

Взлом системы или нарушение системы защиты объекта w_i характеризуется вероятностью взлома каждого метода защиты и всей совокупности методов в целом, суммарной

стоимостью взлома всех методов, а также временными затратами, необходимыми для преодоления всех методов, применяемых для защиты объекта w_i. Суммарная стоимость взлома всех методов, применяемых для защиты объекта w_i, должна быть больше стоимости $v(w_i)$ самого объекта, временные затраты взлома системы защиты объекта должны быть максимальны, они, по крайней мере, должны быть больше $T_0(w_i)$ для базового ограничения временных затрат нападения системы защиты объекта w_i. Только при этих условиях можно считать целесообразным выбор данной совокупности методов защиты объекта w_i.

Наличие взлома m_j-го метода, применяемого для защиты объекта w_i, определяет величину потерь $\hbar_j(w_i)$ для объекта. Суммарная величина потерь при взломе всех методов, применяемых для защиты объекта w_i, не должна превышать стоимости самого объекта $v(w_i)$, - стоимости всей информации, содержащейся в объекте $w_i \in W$.

Эффективность защиты объекта, так же как и системы в целом, существенно зависит от стоимости реализации выбранных методов и средств защиты. Естественно предположить, что чем меньше стоимость реализации системы защиты (при равенстве всех других качественных показателей), тем выше ее эффективность.

Стоимость системы защиты объекта $w_i \in W$, $1 \le i \le n$, определяется суммой

$$\sum_{j=1}^{k} S_j(w_i)\chi^j(w_i),$$

где каждое слагаемое $S_j(w_i)\chi^j(w_i)$ - стоимость реализации $m_j \in M(w_i)$ метода, использованного для защиты объекта w_i. Если какой-либо $m_i(w_i)$-й метод не был использован для защиты объекта w_i, то $\chi^j(w_i) = 0$ и, следовательно, t-е слагаемое суммы равно нулю.

Стоимость защиты объекта должна быть минимизирована, по крайней мере, она не должна превышать определенной величины, скажем $S_0(w_i)$:

$$S(w_i) = \sum_{j=1}^{k} S_j(w_i)\chi^j(w_i) \le S_0(w_i), w_i \in W, i \in J. \tag{4}$$

Для системы в целом это можно записать:

$$S = \sum_{i=1}^{n} S(w_i) = \sum_{i=1}^{n}\sum_{j=1}^{k} S_j(w_i)\chi^j(w_i) \le S_0(w_i), \tag{5}$$

где S_0 - ограничение стоимости для системы.

Обобщим через $S_j^n(w_i)$ и $S_j^э(w_i)$ соответственно стоимости проектирования и эксплуатации m_j-го метода защиты объекта w_i, через $S^n(w_i)$, $S^э(w_i)$, S^n, $S^э$ - соответствующие стоимости проектирования и эксплуатации защиты объекта w_i и системы в целом.

Тогда выражение (4) и (5) примет вид:

$$\begin{aligned} S(w_i) &= \sum_{j=1}^{k} S_j^n(w_i)\chi^j(w_i) + \max_{i\in J} T_0(w_i)\sum_{j=1}^{k} S_j^э(w_i)\chi^j(w_i) = S^n(w_i) + \\ &+ \max_{i\in J} T_0(w_i)\cdot S^э(w_i) \le S_0(w_i), \end{aligned} \tag{6}$$

$w_i \in W, i = \overline{1,n}.$

$$S = S^n + \max_{i\in J} T_0(w_i)\cdot S^э = \sum_{i=1}^{n}\sum_{j=1}^{k} S_j(w_i)\chi^j(w_i) + \max_{i\in J} T_0(w_i)\sum_{i=1}^{n}\sum_{j=1}^{k} S_j^э(w_i)\chi^j(w_i) \le S_0, \quad (7)$$

$w_i \in W, i = \overline{1,n}.$

Здесь $T_0(w_i)$ - максимальное время хранения информации ограниченного использования в объекте w_i, $\max_{i\in J} T_0(w_i)$ - максимальное время нахождения закрытой информации в системе.

Выражение (6) и (7) позволяют сформулировать задачу оптимального выбора методов защиты для каждого конкрétного объекта и для системы в целом.

С другой стороны, стоимость защиты объекта, ограничение на эту стоимость и стоимость самого объекта (стоимость информации, содержащейся в объекте), должны быть связаны между собой: стоимость объекта $v(w_i)$ должна быть больше ограничения на стоимость защиты объекта, т.е. можно записать:

$$v(w_i) \succ S_0(w_i) \ge S(w_i), \forall w_i \in W .$$

Для системы в целом

$$V_c \succ S_0 \ge \sum_{i=1}^{n} S(w_i), \forall i \in J, \quad (8)$$

где V_c - суммарная стоимость информации всех объектов системы:

$$V_c = \sum_{i=1}^{n} v(w_i). \quad (9)$$

Разность $v(w_i) - S(w_i)$ определяет эффективность системы защиты объекта, для системы в целом эффективность определяется разностью $V_c - \sum_{i=1}^{n} S(w_i)$.

Обозначим через $P_j(w_i), j = \overline{1,k}$, вероятность взлома m_j-го метода, использованного для защиты объекта $w_i \in W$. Тогда суммарная вероятность взлома системы защиты объекта w_i, т.е. вероятность преодоления всех методов, примененных для защиты объекта $w_i \in W$, имеет вид:

$$P(w_i) = 1 - \prod_{j=1}^{k}\left[1 - p_j(w_i)\right]\chi^j(w_i), \forall m_i \in W, \quad (10)$$

или для системы в целом, т.к. объекты системы не связаны между собой и представляют независимые события,

$$P = \prod_{i=1}^{n} P(w_i) = \prod_{i=1}^{n}\left[1 - \prod_{j=1}^{k}\left(1 - p_j(w_i)\right)\chi^j(w_i)\right]. \quad (11)$$

Выражения (10) и (11), определяющие вероятности защиты объекта и системы в целом, нужно минимизировать. Это и есть критерий выбора средств и методов защиты.

Теперь обозначим через $t_j(w_i)$ - временные затраты необходимые для взлома m_j-го метода, применимого для защиты объекта w_i, $i = \overline{1,n}$.

Тогда ограничение во взломе всех методов, использованных для защиты объекта w_i, представляется в виде:

$$T_0(w_i) \le \sum_{j=1}^{k} t_j(w_i)\, p_i(w_i)\chi^j(w_i), \forall w_i \in W \quad (12)$$

где $T_0(w_i)$ - максимальное время хранения информации ограниченного использования в объекте w_i.

Для системы, соответственно, имеем выражение:

$$T_0 = \sum_{i=1}^{n}\sum_{j=1}^{k} t_j(w_i)\, p_j(w_i)\, \chi^j(w_i).$$

Если стоимость продолжения m_j-го метода ($m_j \in M$)защиты объекта w_i обозначить через $C_j(w_i)$, то целесообразность обеспечения защиты определяется следующими соотношениями:

$$C(w_i) = \sum_{j=1}^{k} c_j(w_i)\, p_i(w_i)\, \chi^j(w_i) \succ v(w_i) \succ S(w_i), \forall w_i \in W, \quad (13)$$

а для системы должно иметь место

$$C \succ V_c \succ S_0, \quad (14)$$

где С – стоимость преодоления системы защиты всех объектов $w_i \in W$. При этом должны быть учтены ограничения по времени преодоления системы защиты.

Обозначим через $\pi_j(w_i)$ - величину потерь при взломе m_j-го метода, применяемого для защиты объекта w_i. Естественно предполагать, что защита объекта будет целесообразной если суммарная величина потерь при взломе всех методов, применимых для защиты объекта, меньше стоимости самого взлома этих методов:

$$\pi(w_i) = \sum_{j=1}^{k} \pi_j(w_i)\, p_j(w_i)\, \chi^j(w_i) \prec c(w_i). \quad (15)$$

С другой стороны, суммарная величина потерь при взломе всех методов, примененных для защиты объекта $w_i \in W$ не должна превышать стоимости самого объекта:

$$\pi(w_i) \le v(w_i), \forall w_i \in W, \quad (16)$$

если, для системы в целом $\pi_c \le V_c$, где π_c - величина потерь при нарушении системы защиты всех объектов $w_i \in W$, $i = \overline{1,n}$.

Теперь можно выделить $w_i \in W$ объект информационной системы, требующий первоочередных дополнительных мер по защите информации от несанкционированного доступа. Так как V_c - суммарная стоимость информации, содержащейся во всех объектах системы, а $\pi_0(w_i)$ - величина потерь при нарушении системы защиты w_i, то минимум разности:

$$V_c - \pi_0(w_i), i = \overline{1,n} \text{ или}$$

$$\min_{w_i \in W}\left[\sum_{i=1}^{n}\sum_{j=1}^{k} S_j(w_i)\chi^j(w_i) - \sum_{j=1}^{k}\pi_j(w_i)\, p_j(w_i)\chi^j(w_i)\right], \quad (17)$$

определяет номер объекта, потери от взлома методов защиты которого дают максимальную величину и, следовательно, требуют применения дополнительных методов или средств его защиты.

На основании проведенных исследований сформулируем задачи системы защты информации. Будем рассматривать множество элементов:

$\{M_1(w_i), M_2(w_i), ..., M_\sigma(w_i)\}$, где

$$M_\sigma(w_i) = \bigcup_{j=I_\tau} m_j(w_i) \subseteq M(w_i), \tau = \overline{1,\sigma} .$$

Здесь I_τ - подмножество индексов методов защиты объекта, составляющих объединение методов, примененных для защиты объекта w_i и обеспечивающих требуемый уровень его защиты $J(w_i): I_\tau \subseteq J, \forall \tau.$

Таким образом, каждый элемент $M_\tau(w_i)$ $\left(\tau = \overline{1,\sigma}\right)$ представляет собой объединение такого подмножества методов защиты объекта, практическая реализация которых обеспечивает требуемый уровень защиты объекта $w_i \in W$.

Для создания системы защиты объекта $w_i \in W$ $\left(i = \overline{1,n}\right)$ от несанкционированного доступа к информации и к процедурам над ней, сформулируем задачи, которые предполагают оптимизацию по всем элементам [3,4]:

$$M_\tau(w_i) \subseteq M(w_i), \tau = \overline{1,\sigma} .$$

Задача 1. Минимизация стоимости обеспечения защиты объекта $w_i \in W$, $i = \overline{1,n}$, т.е.

$$S(w_i) = \sum_{j=1}^{k} S_j(w_i)\chi^j(w_i) \to \min_{M_\tau(w_i)}, \tau = \overline{1,\sigma},$$

при следующих ограничениях:

$$\sum_{j=1}^{k} \chi_\tau^j(w_i) \le k,$$

$$\sum_{j\in J} I_j(w_i)\chi_\tau^j(w_i) \ge J_0(w_i),$$

$$\sum_{j=1}^{k} S_j(w_i)\chi_\tau^j(w_i) \le S_0(w_i),$$

$$\chi_\tau^j(w_i) = \begin{cases} 1, \\ 0. \end{cases}$$

Более точно задача формируется с учетом неравенства (6), т.е. с раздельным учетом стоимости проектирования и эксплуатации средств и методов, примененных для защиты объекта.

Задача 2. Минимизация эффективности систем защиты объекта $w_i \in W$:

$$v(w_i) - S(w_i) \to \max_{M_\tau(w_i)}$$

при ограничениях задачи 1.

Задача 3. Минимизация вероятности взлома всех методов, используемых для защиты объекта $w_i \in W$:

$$P(w_i) = 1 - \prod_{j=1}^{k} \left(1 - p_j(w_i)\right)\chi^j(w_i) \to \min_{M_\tau(w_i)}$$

при ограничениях принятых при решении задач 1 и 2.

Задача 4. Максимизация стоимости взлома всех методов, использованных для защиты объекта $w_i \in W$:

$$C(w_i) = \sum_{j=1}^{k} c_j(w_i)\, p_j(w_i)\, \chi^j(w_i) \to \max_{M_\tau(w_i)}$$

при ограничениях задачи 1, а также следующих:

$$\sum_{j=1}^{k} t_j(w_i)\, p_j(w_i)\, \chi^j(w_i) \geq T_0(w_i),$$

$$\sum_{j=1}^{k} c_j(w_i)\, p_j(w_i)\, \chi^j(w_i) \succ v(w_i).$$

Задача 5. Минимизация величины потерь от взлома всех методов, использованных для защиты объекта $w_i \in W$:

$$\pi(w_i) = \sum_{j=1}^{k} \pi_j(w_i)\, p_j(w_i)\, \chi^j(w_i) \to \min_{M_\tau(w_i)}$$

при ограничениях принятых в задаче 4, а также ограничения на стоимость взлома системы защиты объекта:

$$\sum_{j=1}^{k} \pi_j(w_i)\, p_j(w_i)\, \chi^j(w_i) \prec c_0(w_i).$$

Решение указанных задач позволит создать приемлемый вариант системы защиты объекта, а решение соответствующей совокупности задач для всего множества объектов W - создать вариант системы защиты информации для системы в целом.

Выбор совокупности методов $m_j \in M$ защиты объекта должен производится с учетом определения всех каналов утечки (через посредство каталога каналов утечки информации) для каждого конкретного объекта $w_i \in W$ с целью их перекрытия. Затем для каждого отдельного метода защиты должны быть определены стоимости проектирования и эксплуатации при реализации этого метода, вероятность и стоимость его взлома. Следующие характеристики, весьма трудные для определения: оценка стоимости объекта, оценки уровней для каждого отдельного метода защиты и уровня защиты самого объекта w_i, а также оценки величины потерь в случае взлома каждого отдельного метода защиты объекта. Временные затраты, необходимые для взлома всех методов, примененных для защиты объекта w_i, могут быть получены через вероятности преодоления каждого из методов и времени, необходимого для реализации одной попытки преодоления каждого метода защиты.

Указанные характеристики представляют собой исходные данные, необходимые для создания и оценки качества системы защиты каждого объекта и́ всей вычислительной системы в целом.

Список литературы

1. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации. – К.: Издательство Юниор, 2003. – 504с.

2. *Ленков С.В., Перегудов Д.А., Хорошко В.А.* // Под ред. В.А. Хорошко. Методы и средства защиты информации. - К.: Арий, 2008. – В 2-х томах.

3. *Егоров Ф.И., Хорошко В.А., Чирков Д.В.* Факторы определяющие технологическую безопасность информации. - //Вісник Східноукраїнського національного університету ім. Даля, №5 (III), 2007. – с.62-64.

4. *Егоров Ф.И., Орленко В.С., Хорошко В.А.* Проектирование сложных информационных сетей. - // Вісник ДУІКТ, том 5, №4, 2007. – с.39-51.

5. *Егоров Ф.И., Хорошко В.А.* Двухкритериальная оптимизация систем защиты информации. - // Сб. науч. Трудов НАУ «Защита информации». – К.: Изд. НАУ, 2007. – с.224-228.

УДК 004:261

Соснін О. В.
Дипломатична Академія України

ПРОБЛЕМИ ТЕОРІЇ І ПРАКТИКИ ЗАСЕКРЕЧУВАННЯ ІНФОРМАЦІЇ

В умовах глобальної інформатизації суспільства реальна безпека держави багато в чому залежить від безпеки її інформаційних ресурсів і технологій. У загальній проблемі забезпечення безпеки інформації питання захисту так званої службової, або конфіденційної інформації, або, як її іноді називають, "інформації з обмеженим доступом" є одним із найважливіших. Це пояснюється, зокрема, тим, що частка конфіденційної інформації в загальному інформаційному потоку являє собою саму значну частину.

Захист національної конфіденційної інформації став одним із головних пріоритетів державної політики, у тому числі й у нашій країні. Віднесення інформації до категорії з обмеженим доступом та її засекречування є важливою складовою теорії і практики захисту інформації.

Розглянемо ознаки, що відрізняють інформацію з обмеженим доступом від відкритої інформації. Вказані ознаки всебічно обґрунтовані у праці [1], серед яких доцільно виділити наступні:

право обмежувати доступ до інформації з обмеженим доступом має тільки її власник та особа (фізична або юридична), яка уповноважена володіти, користуватися, розпоряджатися;

ступінь обмеження доступу та рівень охорони інформації з обмеженим доступом завжди відзначається її важливістю для особи, суспільства, держави;

інформація, що охороняється повинна приносити певну користь власникові та як правило, виправдовувати кошти, що витрачаються на захист такої інформації;

під час створення на основі інформації з обмеженим доступом нової інформації, вона, як правило, включається до масивів інформації, що захищається;

кругообіг інформації з обмеженим доступом здійснюється у сфері, обмеженій режимними заходами;

кругообіг та розсіяння інформації з обмеженим доступом створюють передумови для її уразливості (витоку, розголошення);

старіння інформації з обмеженим доступом, передбачає обов'язковий перегляд ступенів обмеження доступу такої інформації.

Знання та повне уявлення про ознаки що характеризують інформацію з обмеженим доступом як об'єкт захисту служитиме основою для формування складових суб'єктів управління системою захисту інформації, важливою визначальною частиною якої є віднесення відомостей до категорії з обмеженим доступом та її засекречування, встановлення конфіденційності та її засекречування (встановлення конфіденційності).

Віднесення відомостей до інформації з обмеженим доступом та їх засекречування (встановлення конфіденційності) – це практична реалізація об'єктивного закону захисту інформації, а саме : примусового відчуження і усуспільнювання інформації в інтересах суспільної необхідності. В демократичних країнах він всюди реалізується правовими нормами.