УДК 681.3

К.В. КОЛЕСНИКОВ, В.Е. ШАДХИН

Черкасский государственный технологический университет, Украина

СИСТЕМНЫЙ АНАЛИЗ КРИТЕРИЕВ И ПАРАМЕТРОВ ПРОЕКТИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ

В статье рассмотрены критерии и параметры проектирования оптимальной системы защиты. Представлено общее решение задачи проектирования оптимальной системы защиты информации. Предложен метод вычисления коэффициента защищенности, исходя из вероятности появления угроз и вероятности отражения атак.

несанкционированный доступ, коэффициент защищенности

Введение

Надежность вычислительной системы – это свойство системы выполнять возложенные на нее функции в течение заданного промежутка времени. Применительно к системе защиты информации от несанкционированного доступа (НСД) надежность (эффективность защиты) – это свойство системы защиты обеспечивать защиту компьютерной информации от НСД в течение заданного промежутка времени [2].

Постановка задачи. Вопросы оценки эффективности и вопросы проектирования системы защиты тесно связаны, т.к. в их основе лежит единый математический аппарат решения соответствующей оптимизационной задачи [5]. При проектировании системы защиты необходимо решать задачу многокритериальной оптимизации, т.к. система защиты в общем случае характеризуются целым рядом параметров, которые должны учитываться.

1. Критерий и параметры проектирования оптимальной системы защиты

Будем оценивать защищенность системы (Z) количественно в зависимости от стоимости защищаемой информации, вероятности взлома, стоимости самой системы защиты, производительности системы:

$$Z = f(C_{инф}, P_{взл}, Ц_{СЗИ}, П), \quad (1)$$

где $C_{инф}$ – стоимость защищаемой информации; $P_{взл}$ – вероятность взлома; $Ц_{СЗИ}$ – стоимость СЗИ; $П$ – производительность системы.

С учетом введенного понятия защищенности системы оптимизационная задача состоит в обеспечении максимального уровня защищенности (как функции стоимости защищаемой информации и вероятности взлома) при минимальной стоимости системы защиты и минимальном влиянии ее на производительность системы:

$$Z^{opt} = \max Z(C_{инф}, P_{взл}, Ц_{СЗИ}, П). \quad (2)$$

С учетом сказанного может быть сделан важный вывод о многокритериальном характере задачи проектирования системы защиты. При этом, кроме обеспечиваемого уровня защищенности, должен учитываться еще ряд важнейших характеристик системы. Например, обязательно должно учитываться влияние системы защиты на загрузку вычислительного ресурса защищаемого объекта.

В общем случае загрузка вычислительного ресурса определяется количеством прикладных задач, решаемых объектом в единицу времени. [1]

Исходные параметры для задачи проектирования системы защиты, а также возможности сведения задачи к однокритериальной проиллюстрированы на рис. 1.

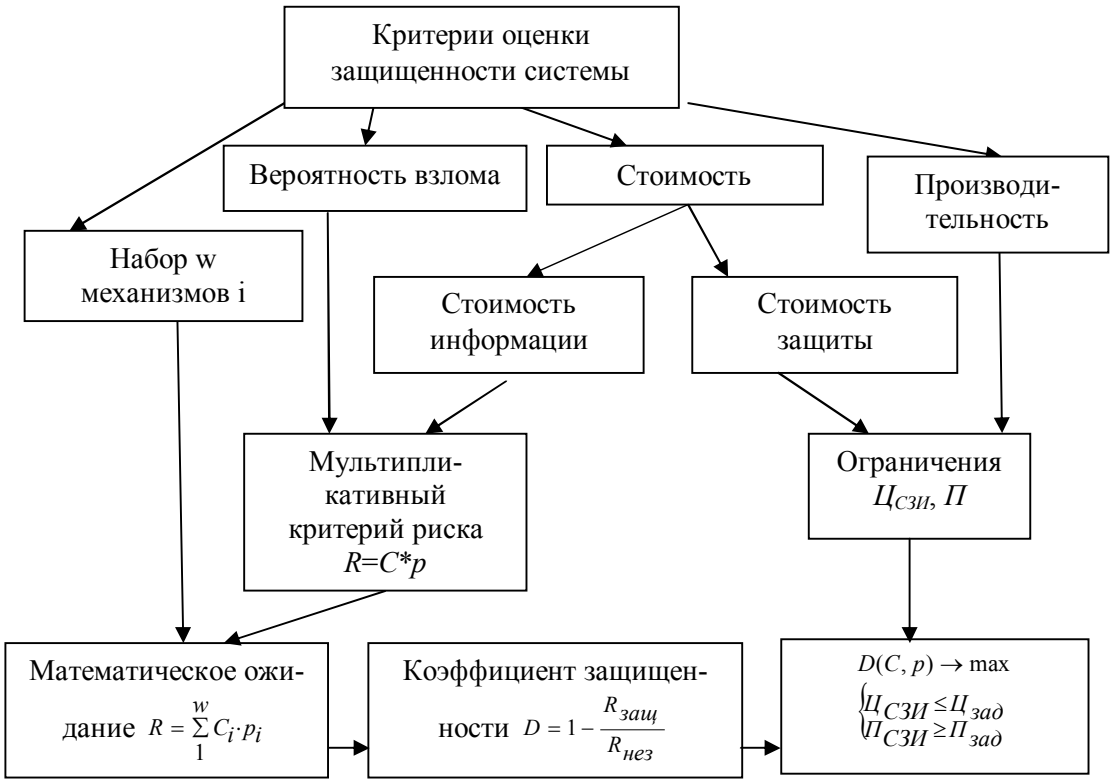

Рис. 1. Критерии оценки защищенности

2. Защищенность системы с точки зрения риска

Рассмотрим защищенность системы с точки зрения риска. Заметим, что использование теории рисков для оценки уровня защищенности на сегодняшний день является наиболее часто используемым на практике подходом. *Риск* (R) – это потенциальные потери от угроз защищенности:

$$R(p) = C_{инф} \cdot p_{взл}. \qquad (3)$$

По существу, параметр риска здесь вводится как мультипликативная свертка двух основных параметров защищенности.

С другой стороны, можно рассматривать риск как потери в единицу времени:

$$R(\lambda) = C_{инф} \cdot \lambda_{взл}, \qquad (4)$$

где $\lambda_{взл}$ – интенсивность потока взломов (под взломом будем понимать удачную попытку несанкционированного доступа к информации).

Эти две формулы связаны следующим соотношением:

$$p_{взл} = \frac{\lambda_{взл}}{\Lambda}, \qquad (5)$$

где Λ – общая интенсивность потока несанкционированных попыток доступа злоумышленниками к информации [1].

3. Основной критерий защищенности. Общее решение задачи проектирования оптимальной системы защиты

В качестве основного критерия защищенности будем использовать *коэффициент защищенности* (D), показывающий относительное уменьшение риска в защищенной системе по сравнению с незащищенной системой:

$$D\% = \left(1 - \frac{R_{защ}}{R_{нез}}\right) \times 100\%, \qquad (6)$$

где $R_{защ}$ – риск в защищенной системе; $R_{нез}$ – риск в незащищенной системе.

Таким образом, в данном случае задача оптимизации выглядит следующим образом:

$$\begin{cases} D(C_{инф}, p_{взл}) \to \max; \\ Ц_{СЗИ} \to \min; \\ П_{СЗИ} \to \max. \end{cases} \quad (7)$$

Для решения этой задачи сведем ее к однокритериальной посредством введения ограничений. В результате получим:

$$\begin{cases} D(C_{инф}, p_{взл}) \to \max; \\ Ц_{СЗИ} \le Ц_{зад}; \\ П_{СЗИ} \ge П_{зад}, \end{cases} \quad (8)$$

где $Ц_{зад}$ и $П_{зад}$ – заданные ограничения на стоимость системы защиты и производительность системы.

Целевая функция выбрана исходя из того, что именно она отражает основное функциональное назначение системы защиты – обеспечение безопасности информации [1].

Производительность системы $П_{СЗИ}$ рассчитывается с применением моделей и методов теории массового обслуживания и теории расписаний (в зависимости от того, защищается ли система оперативной обработки, либо реального времени).

На практике возможно задание ограничения по производительности (влияние на загрузку вычислительного ресурса защищаемой системы) не непосредственно в виде требуемой производительности системы, а как снижение производительности ($dП_{СЗИ}$) информационной системы от установки системы защиты.

В этом случае задача оптимизации будет выглядеть следующим образом:

$$\begin{cases} D(C_{инф}, p_{взл}) \to \max; \\ Ц_{СЗИ} \to \min; \\ dП_{СЗИ} \to \max \end{cases} \quad (9)$$

или после сведения ее к однокритериальной:

$$\begin{cases} D(C_{инф}, p_{взл}) \to \max; \\ Ц_{СЗИ} \le Ц_{зад}; \\ dП_{СЗИ} \ge dП_{зад}, \end{cases} \quad (10)$$

где $Ц_{зад}$ и $dП_{зад}$ – заданные ограничения на стоимость системы защиты и снижение производительности.

Заметим, что именно такой принцип сведения задачи к однокритериальной целесообразен, т.к. в любом техническом задании на разработку системы защиты указывается, в какой мере система защиты должна оказывать влияние на производительность системы. Как правило, внедрение системы защиты не должно снижать производительность системы более чем на 10% [4]. Кроме того, обычно вводится ограничение на стоимость системы защиты.

Если рассчитанное значение коэффициента защищенности (D) не удовлетворяет требованиям к системе защиты, то в допустимых пределах можно изменять заданные ограничения и решить задачу методом последовательного выбора уступок (рассмотрен ниже). При этом задается приращение стоимости и снижение производительности:

$$Ц^*_{зад} = Ц_{зад} + \Delta Ц; \; П^*_{зад} = П_{зад} - \Delta П$$
$$\text{или} \quad (11)$$
$$dП^*_{зад} = dП_{зад} - \Delta dП.$$

В таком виде задача решается в результате реализации итерационной процедуры путем отсеивания вариантов, не удовлетворяющих ограничительным условиям, и последующего выбора из оставшихся варианта с максимальным коэффициентом защищенности.

Теперь выразим коэффициент защищенности через параметры угроз. В общем случае в системе присутствует множество видов угроз. В этих условиях зададим следующие величины:

w – количество видов угроз, воздействующих на систему;

$C_i (i = \overline{1,w})$ – стоимость (потери) от взлома i-го вида;

$\lambda_i (i = \overline{1,w})$ – интенсивность потока взломов i-го вида, соответственно;

$Q_i (i = \overline{1,w})$ – вероятность появления угроз i-го вида в общем потоке попыток несанкционированного доступа к информации, причем $Q_i = \dfrac{\lambda_i}{\Lambda}$;

$p_i(i=\overline{1,w})$ – вероятность отражения угроз i-го вида системой защиты.

Соответственно, для коэффициента потерь от взломов системы защиты имеем:

$$R(p)=\sum_1^w R_i(p)=\sum_1^w C_i\cdot p_{взлі}\ , \qquad (12)$$

где $R_i(p)$ – коэффициент потерь от взлома i-го типа.

Этот коэффициент показывает, какие в среднем потери приходятся на один взлом i-го типа.

Для незащищенной системы

$$p_{угрі}=Q_i,$$

для защищенной системы

$$p_{угрі}=Q_i(1-p_i).$$

Соответственно, для коэффициента потерь от взломов системы защиты в единицу времени имеем:

$$R(\lambda)=\sum_1^w R_i(\lambda)=\sum_1^w C_i\cdot\lambda_{угрі}\ , \qquad (13)$$

где $R_i(\lambda)$ – коэффициент потерь от взломов i-го типа в единицу времени.

Для незащищенной системы $\lambda_{угрі}=\lambda_i$ для защищенной системы $\lambda_{угрі}=\lambda_i\cdot(1-p_i)$.

Соответственно, из (6) имеем:

$$D=1-\frac{\sum_1^w C_i\cdot Q_i\cdot(1-p_i)}{\sum_1^w C_i\cdot Q_i}=1-\frac{\sum_1^w C_i\cdot\lambda_i\cdot(1-p_i)}{\sum_1^w C_i\cdot\lambda_i}. \qquad (14)$$

Если в качестве исходных параметров заданы вероятности появления угроз Q_i, то коэффициент защищенности удобно считать через вероятности появления угроз. Если же в качестве исходных параметров заданы интенсивности потоков угроз λ_i, то, естественно, коэффициент защищенности считается через интенсивность [3].

Заключение

В статье рассмотрены критерии и параметры проектирования оптимальной системы защиты информации. Проведено общее решение задачи проектирования оптимальной системы защиты информации. Очевидно, что при использовании любого математического метода проектирования системы защиты необходимо задавать определенные исходные параметры для оценки защищенности. Однако именно с этим и связаны основные проблемы формализации задачи синтеза системы защиты, что представляет собой широкое поле для дальнейших исследований.

Литература

1. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – С.-Пб.: Наука и техника, 2004. – 384 с.

2. Тимченко А.А. Основи системного проектування та системного аналізу складних об'єктів: Підручник: У двох книгах. Кн. 1. Основи САПР та системног проектування складних об'єктів / За ред. В.І. Бикова. – К.: Либідь, 2000. – 272 с.

3. Норткат С., Купер М., Фирноу М., Фредерик К. Анализ типовых нарушений безопасности в сетях. – М.: Издательский дом «Вильямс», 2001. – 464 с.

4. Домарев В.В. Безопасность информационных технологий. Системный подход. – К.: ООО «ТИД «ДС», 2004. – 992 с.

5. Контроль та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології: Навчальний посібник / А.М. Гуржій, С.Ф. Коряк, В.В. Самсонов, О.Я. Скляров. – Х.: СМІТ, 2004. – 544 с.

Поступила в редакцию 20.02.2006

Рецензент: д-р техн. наук, проф. В.И. Долгов, Харьковский национальный университет радиоэлектроники.