Оценка защищенности информационных систем на основе модели комплекса механизмов защиты

An assessment of information system security based on a model of a complex of protection mechanisms

Ключевые слова: оценка защищенности – security assessment, механизм защиты – the mechanism of protection, рейтинг защищенности – security rating, уровни системы защиты – levels of security system, модель системы защиты – security system model, иерархическая модель – hierarchical model.

В статье рассматривается наиболее полная на настоящий момент количественная оценка уровня защищенности информационной системы, использующая рейтинговые показатели, учитывающие распределение механизмов защиты по уровням иерархической системы защиты.

The article covers the most complete quantitative assessment of the level of information system security up to date, using the rating indicators, which take into account the distribution of the security mechanisms on levels of a hierarchical protection system.

КОНДРАШОВ / KONDRASHOV V.
Валерий Владимирович
аспирант, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург

Официально признаваемой оценкой защищенности информационных систем являются классы защищенности, описание которых приведено в российских и международных стандартах защищенности.

Известные оценки защищенности автоматизированных систем исходят из наличия определенного набора средств и механизмов защиты, методик изготовления, эксплуатации и тестирования, позволяющих отнести то или иное устройство или информационную систему в целом к одному из дискретных уровней защищенности в соответствии с используемыми в данной стране стандартами [1-5].

Для количественной оценки уровня защищенности используют рейтинговые показатели, которые учитывает распределение механизмов защиты по уровням иерархической модели системы защиты информации и изменение вероятности достижения злоумышленником объекта защиты в зависимости от ее уровня [6].

Согласно модели комплекса механизмов защиты [6] уровень защищенности зависит не только от числа механизмов защиты, но и от их расположения в структуре системы защиты информации.

Анализ защищенности проводится в два этапа:

1-й этап – оценка защищенности, обеспечиваемой отдельным механизмом;

2-й этап – оценка защищенности системы защиты информации в целом.

На 1-ом этапе определяется потенциальная защищенность – рейтинг стойкости отдельного механизма защиты. Производят ранжирование механизмов защиты в зависимости от уровня защищенности, который он способен обеспечить.

В наборной модели системы защиты информации ее защищенность оценивают, полагая, что все механизмы защиты равноценны и участвуют в нейтрализации угроз. Для определения рейтинга *Rs* защищенности информационной системы суммируют рейтинги стойкости отдельных механизмов защиты:

$$R_S = \sum_{i=1}^{i} m_i$$

где m_i - рейтинг стойкости i-го механизма защиты.

Структурная модель системы защиты информации учитывает структурные особенности информационной системы, например, наличие средств защиты на следующих уровнях: аппаратном, BIOS, операционной системы, сетевом, СУБД, функционального программного обеспечения (рис. 1).

Механизмы защиты располагаются на уровнях системы защиты информации в соответствии с их назначением. Например, механизм идентификации и аутентификации может быть реализован как на уровне операционной системы, так и на

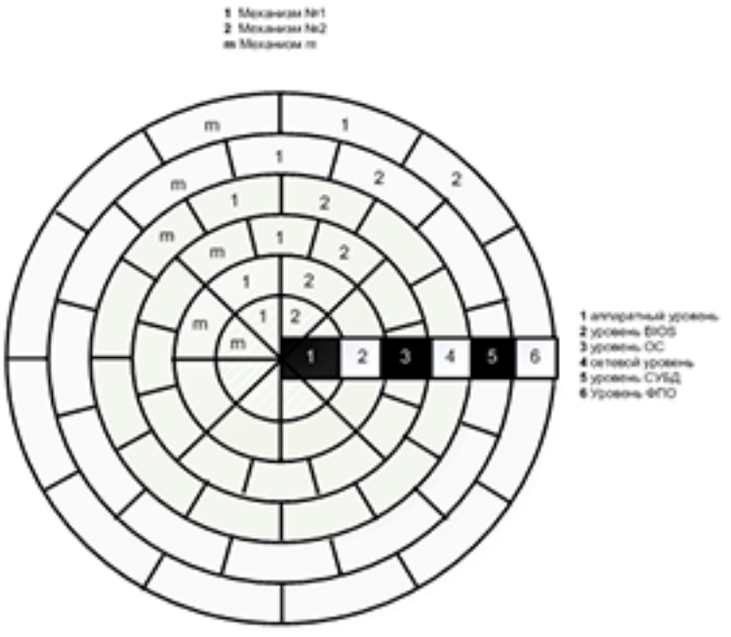

Рис. 1. Структурная модель системы защиты

уровне функционального программного обеспечения.

Если число уровней системы защиты информации равно j, а число различных механизмов защиты составляет i, то можно сформировать матрицу рейтингов стойкости следующего вида:

$$M = \begin{matrix} m_{11} & m_{12} & . & m_{1j} \\ m_{21} & m_{22} & . & m_{2j} \\ . & . & . & . \\ m_{i1} & m_{i2} & . & m_{ij} \end{matrix}$$

Каждый столбец матрицы соответствует уровню системы защиты информации. Элемент матрицы m_{ij} равен 0, если i-й механизм защиты отсутствует на j-м уровне системы защиты информации. Предполагается, что угроза с определенной вероятностью будет нейтрализована некоторым механизмом защиты на одном из уровней системы защиты информации.

Если n – число угроз, i – число механизмов защиты, и $n>i$, то вероятность того, что угроза из множества известных угроз будет нейтрализована i-м механизм защиты:

$$P = \frac{i_j}{n_j}$$

где i_j – число механизмов защиты, а n_j – число угроз, актуальных для j-го уровня системы защиты информации.

Для каждого последующего уровня системы защиты информации число актуальных угроз будет уменьшаться, поскольку некоторые из них будут нейтрализованы на предыдущих уровнях системы защиты информации:

$$n_j = n_{j-1} - i_{j-1}$$

Предполагая, что на всех уровнях число механизмов защиты – максимально возможное и вероятность нейтрализации угрозы на каждом последующем уровне системы защиты информации будет больше, чем на предыдущем. Формируют вектор распределения вероятности нейтрализации угроз по уровням системы защиты информации:

$$P = \begin{matrix} P_1 \\ P_2 \\ \vdots \\ P_j \end{matrix}$$

Поэлементным умножением строк матрицы рейтингов стойкости на вектор распределения вероятностей формируют матрицу защищенности Z:

$$Z = \begin{matrix} m_{11}P_1 + m_{12}P_2 + ... + m_{1j}P_j \\ m_{21}P_1 + m_{22}P_2 + ... + m_{2j}P_j \\ \vdots \\ m_{i1}P_1 + m_{i2}P_2 + ... + m_{ij}P_j \end{matrix}$$

Рейтинг защищенности информационной системы определяют суммой элементов матрицы защищенности Z:

$$R_S = \sum_{i=1}^{i} Z_i$$

Использование предложенной оценки защищенности информационных систем позволяет представлять результаты анализа защищенности в количественной форме, что позволяет использовать рейтинговый показатель в качестве целевой функции для оптимизации распределения механизмов защиты по уровням системы защиты информации (критерий – максимизация рейтинга *Rs*).

К недостаткам следует отнести статичный характер вышеприведенной оценки защищенности информационных систем, не учитывающей такие параметры как ущерб от реализации угроз информационной безопасности и частоту осуществления атак. Кроме того, предположение о снижении количества актуальных угроз по мере приближения к объекту защиты не всегда справедливо, например, для внутрисистемных попыток несанкционированного доступа.

Литература

1. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Часть 1. Введение и общая модель. – Госстандарт России, Москва, 2002;

2. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. – Госстандарт России, Москва, 2002;

3. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. – Госстандарт России, Москва, 2002;

4. *Девянин П.Н.* и др. Теоретические основы компьютерной безопасности. – М.: «Радио и Связь», 2000;

5. Common Criteria for Information Technology Security Evaluation. Version 2.2. Revision 256. Part 1: Introduction and general model. – January 2004;

6. *Суханов А.В., Суханов В.А.* Оценка защищенности информационных систем по методологии Общих Критериев. – Журнал научных публикаций аспирантов и докторантов, №5, май 2008.