УДК 681.324

ПРИМЕНЕНИЕ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

С.С. Химка, Н.Е. Губенко
Донецкий национальный технический университет

У статті описується розробка концептуальної та імітаційної моделі системи захисту інформації, розглядаються головні критерії захищеності та надаються результати проведення імітаційного експерименту.

Введение

Согласно официальному подходу, описаному в [1], [4] эффективность защиты информации определяется классом защищенности автоматизированной системы (АС). Класс защищенности, в свою очередь, определяет набор механизмов защиты (МЗ), которые должны быть реализованы в АС. Такой подход к оценке эффективности защиты информации не позволяет учитывать ни качество самих МЗ, констатируя лишь факт их наличия или отсутствия, ни изменение условий функционирования системы защиты информации (СЗИ). Примерами таких изменений могут служить модификация аппаратной и программной среды, изменение условий информационного взаимодействия объектов и субъектов защиты, числа пользователей системы, возникновение информационных конфликтов в АС.

Описание концептуальной модели СЗИ

В работе [2] приведены методы и методики, позволяющие выполнять количественную оценку защищенности информации при использовании СЗИ. Как правило, количественная защищенность информации оценивается определенным набором вероятностных показателей, основным из которых является некий интегральный показатель. В статье [2] для обоснования методики оценки защищенности информации разработана теоретическая модель СЗИ от несанкционированного доступа (НСД). Ее можно представить в виде схемы, изображенной на рисунке 1.

СЗИ имеет вид сетевой модели, состоящей из набора средств защиты S_i. На вход средств защиты поступают потоки запросов несанкционированного доступа (НСД) $V(t)$, определяемые моделью нарушителя на множестве потенциальных угроз $\{U_i\}$. Каждое из

средств защиты отвечает за защиту от угрозы определенного типа и использует соответствующий защитный механизм. Задача средства защиты - распознать угрозу и заблокировать несанкционированный запрос.

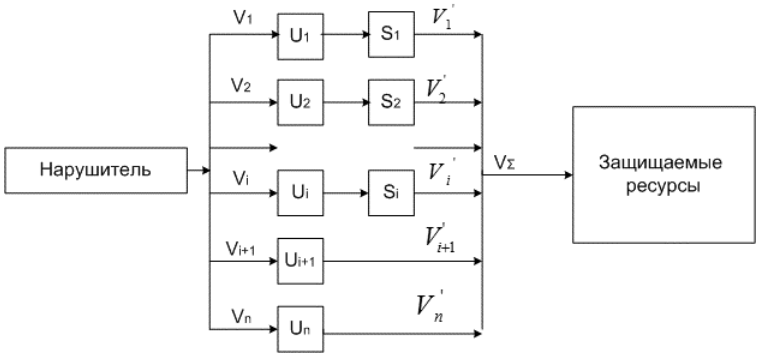

Рис. 1. Модель системы защиты информации от несанкционированного доступа

В результате функционирования системы защиты исходный поток НСД разрежается с вероятностями $p_i(y)$ и образует выходной поток $V_i^{'}(t)$. На рисунке видно, что для m входных потоков отсутствуют средства защиты, это отражает факт неполного закрытия системой защиты всех возможных каналов проявления угроз.

Каждое средство (механизм) защиты характеризуется вероятностью пропуска НСД – q и, соответственно, вероятностью обеспечения защиты (отражения НСД) $p = 1 - q$.

Нарушитель характеризуется вектором интенсивностей $\lambda = \{\lambda_1, \lambda_2, \dots \lambda_{i+m}\}$ попыток реализации соответствующих угроз $U_1 \dots U_{i+m}$.

Согласно [3], для того, чтобы реализовать системный подход к обеспечению информационной безопасности необходимо применять методы моделирования систем и процессов защиты информации. В модели должны быть отражены существенные свойства моделируемого объекта или процесса, а также математическое или логическое описание его компонентов.

Целью моделирования должен являться поиск оптимальных комбинаций механизмов защиты и оценка эффективности использования методов защиты.

В [2] описана вероятностная модель системы защиты информации с использованием теории массового обслуживания. Следовательно целесообразно использовать при построении имитационной модели средства моделирования СМО. К таким

средствам можно отнести язык имитационного моделирования GPSS.

Разработка имитационной модели СЗИ

Представим математическую модель СЗИ, показанную на рисунке 1 в виде функциональных блоков, объединенных в три группы, соответствующие трем основным объектам моделируемой системы: «Нарушитель», «СЗИ» и «Защищаемые ресурсы». Модель показана на рисунке 2

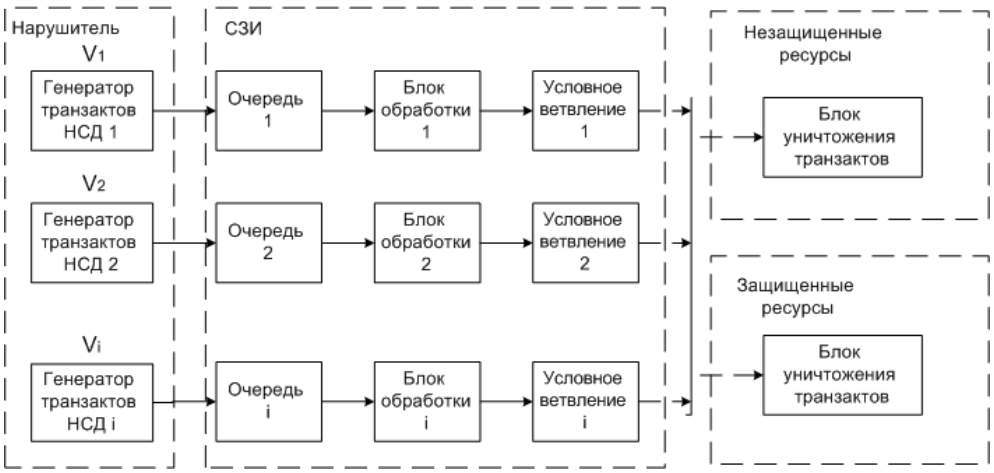

Рис. 2. Имитационная модель СЗИ от НСД

У первого блока - «Нарушитель» - нет входного воздействия, его задача генерация потока (потоков) запросов НСД (транзактов) с заданной интенсивностью λ.

Блок «СЗИ» имитирует процесс реагирования СЗИ на запросы НСД. Функциональные элементы этого блока имитируют очереди запросов НСД и задержки на обслуживание и т.д. Основной же задачей функционирования этого блока является отсеивание запросов НСД с определенной (заданной) вероятностью. На выходе блока образуется разреженный поток запросов НСД, имеющий интенсивность λ'.

Последний блок модели – «Защищаемые ресурсы» – не выполняет самостоятельных функций и используется в имитационной модели для уничтожения запросов НСД.

Для оценки степени защищенности автоматизированной системы от НСД используются следующие показатели: вероятность защиты - $Z(t)$; среднее время между пропущенными НСД - T_n; интенсивностью потока пропущенных НСД - $H(t)$.[2]

Если рассматривать вероятность обеспечения защиты как вероятность отсутствия несанкционированных запросов к информации

на выходе средств защиты, то ее значение можно определить по формуле:

$$Z(t) = 1 - F(t) \quad (1)$$

где $F(t)$ - функция распределения случайной величины T_n, Эта величина показывает время между двумя соседними пропусками НСД. $Z(t)$ является интегральным показателем защищенности информации и показывает вероятность того, что за время t не будет пропущено ни одной попытки НСД.

Если рассматривать суммарный поток НСД как поток, распределенный по закону Пуассона[2], то для вычислений оценки защищенности можно использовать следующая формула:

$$Z(t) = e^{-\sum_{i=1}^{n} \lambda_i q_i t} \quad (2)$$

Тогда, интенсивность потока пропущенных запросов НСД определется формулой:

$$H(t) = \sum_{i=1}^{n} \lambda_i q_i t \quad (3)$$

Алгоритм работы имитационной модели имеет следующий вид. Генератор транзактов генерирует с заданной интенсивностью запрос НСД. Запрос поступает в очередь. Если механизм защиты свободен, запрос НСД поступает на обслуживание на время $t_{ЗД}$. После этого он отсеивается или пропускается в систему, образуя поток пропущенных запросов НСД. Отсеивание или пропуск запросов НСД происходит с заданными вероятностями.

Для построения модели использовался язык программирования GPSS. Возможность проявления угрозы рассматривается как случайное событие. Пусть время между запросами НСД распределяется по экспоненциальному закону, а средняя интенсивность потока - 60 с. Тогда, приняв допущение, что время обработки запроса составляет 1 с, и с вероятностью 0,9 запрос будет нейтрализован, можем промоделировать систему на протяжении 100000 с. В итоге получены следующие результаты: интенсивность потока пропущенных запросов H=0,01, среднее время между пропусками запросов: $\tau_{нсд}$=593 секунды.

На рисунке 3 представлены график зависимости интегрального показателя защищенности от времени – Z(t) и график функции распределения F(t) случайной величины $\tau_{нсд}$.

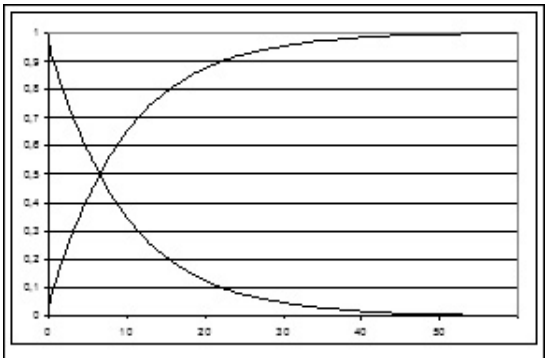

Рис. 3. Графики $F(t)$ и $Z(t)$, полученные экспериментально

Выводы

В ходе проведения исследований рассмотрены показатели эффективности системы защиты и построена имитационная модель системы защиты с использованием языка имитационного моделирования GPSS. Произведен ручной расчет и построены графики таких показателей, как интегральный показатель защищенности $Z(t)$ и функция распределения $F(t)$, найден средний интервал времени $\tau_{нсд}$ между соседними пропусками НСД. После этого проведен эксперимент и получены экспериментальные значения показателя защищенности $Z(t)$, средней интенсивности потока пропущенных НСД H и среднего интервала времени $\tau_{нсд}$ между соседними пропусками НСД. В результате можно сделать вывод, что значения, полученные в ходе имитационного моделирования, подтверждают теоретические расчеты. Следовательно, подтверждается адекватность имитационной модели.

Литература

1. Закон України №121 від 23.04.2002 «Про заходи щодо захисту конфіденційної і відкритої інформації, що циркулює в автоматизованій системі Міністерства»
2. Карпов В.В. Вероятностная модель оценки защищенности средств вычислительной техники с аппаратно-программным комплексом защиты информации от несанкционированного доступа. // Программные продукты и системы. - 2003. - №1. – С. 31
3. Девянин П.Н., Михальский О.О. и др. Теоретические основы компьютерной безопасности. - М.: Радио и связь, 2000.
4. Зегжда Дмитрий Петрович. Принципы и методы создания защищенных систем обработки информации : Дис. д-ра техн. наук : 05.13.19 : Санкт-Петербург, 2002 380 с. РГБ ОД, 71:04-5/168-4
5. Гостехкомиссия России. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования по защите информации. - М.: 1992.

Получено 28.05.09