А.А. Пономарёв
Аспирант кафедры информационной безопасности в управлении
Удмуртского государственного университета

МОДЕЛЬ НАДЕЖНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056.53

Разработана модель надежности системы защиты информации (СЗИ), которая позволяет вычислять характеристики СЗИ, используя аппарат теории массового обслуживания.

Под надежностью системы защиты будем понимать свойство СЗИ выполнять возложенные на неё функции заданный промежуток времени[1]. Учитывая специфику анализируемой области, а именно рассматривая вопросы защиты информации различными программными и аппаратными средствами, можно говорить, что для СЗИ понятие отказ должно трактоваться шире, чем при рассмотрении любого другого технического средства. Так как с отказом связан не только переход СЗИ в состояние неработоспособности, но и обнаружение в СЗИ уязвимостей. Так же следует учитывать, что поскольку функцией СЗИ является противодействие заданному множеству угроз, то в модели СЗИ следует учитывать наличие и активность действий злоумышленника.

СЗИ являются сложными системами с множеством недетерминированных факторов, и модель их функционирования может строиться только с некоторым уровнем абстракции.

Осуществление злоумышленником попыток несанкционированного доступа (НСД), отказы СЗИ, появление уязвимостей в СЗИ, интенсивность проверок функционирования СЗИ, интенсивность устранения уязвимостей, интенсивность создания новой информации в организации можно представить как простейший поток событий. Тогда СЗИ может рассматриваться как система массового обслуживания с состояниями полученными изменением трех признаков: u(0,1) – система не уязвима (уязвимости не известны) или система с известной уязвимостью; v(0,1) – СЗИ

работоспособна или отказ; k(0,1)– есть попытка НСД или нет. В таком случае СЗИ может быть представлена следующим образом рисунок 1.

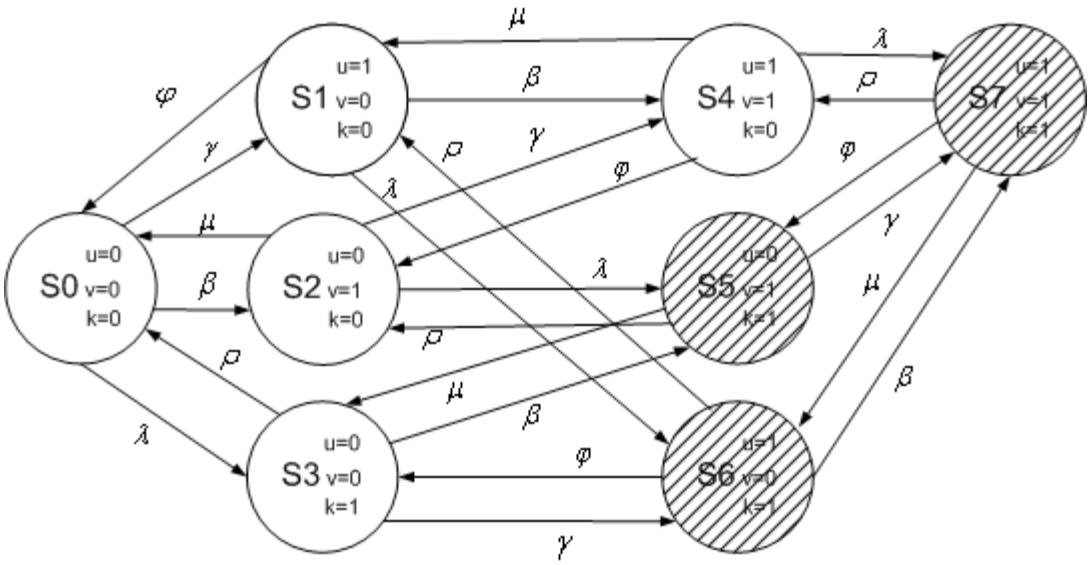

Рисунок 1. Модель надежности СЗИ

На рисунке 1 S1,S2…S7 состояния системы, полученные изменением признаков u, v, k под действием простых потоков событий параметры простых потоков, которые могут трактоваться как интенсивности: λ – интенсивность попыток НСД; β – интенсивность отказов СЗИ; γ – интенсивность нахождения уязвимостей в СЗИ; μ – интенсивность проверки функционирования СЗИ с приведением её в работоспособное состояние; φ – интенсивность устранение уязвимостей; ρ – интенсивность создание новой информации.

Анализ модели показанной на рисунке 1 позволяет вычислять следующие характеристики СЗИ: коэффициент надежности, параметр потока отказов, среднее время преодоления СЗИ злоумышленником, среднее время восстановления[2].

Для нахождения вероятностей состояний составим систему линейных алгебраических уравнений относительно стационарных вероятностей p_i, $i = 0, 1, 2, \ldots, 8$:

$$\begin{cases} -p_0(\gamma+\lambda+\beta)+p_1\varphi+p_2\mu+p_3\rho=0 \\ -p_1(\varphi+\beta+\lambda)+p_0\gamma+p_4\mu+p_6\rho=0 \\ -p_2(\mu+\gamma+\lambda)+p_0\beta+p_4\varphi+p_5\rho=0 \\ -p_3(\beta+\gamma+\rho)+p_0\lambda+p_5\mu+p_6\varphi=0 \\ -p_4(\lambda+\mu+\varphi)+p_1\beta+p_2\gamma+p_7\rho=0 \\ -p_5(\mu+\gamma+\rho)+p_2\lambda+p_3\beta+p_7\varphi=0 \\ -p_6(\varphi+\beta+\rho)+p_1\lambda+p_3\gamma+p_7\mu=0 \\ -p_7(\varphi+\mu+\rho)+p_4\lambda+p_5\gamma+p_6\beta=0 \end{cases} \quad (1)$$

Система уравнений (1) является однородной, и должна решаться вместе с условием нормировки: $\sum_{i=0}^{7} p_i = 1$. Решить систему (1) можно программным средством Microsoft Excel, функцией «Поиск решения».

Пример. Рассмотрим задачу выбора межсетевого экрана (МЭ) для организации, допустим встроенный в операционную систему МЭ, обеспечивает следующие характеристики: λ (интенсивность попыток НСД) = 1 в день; β (интенсивность отказа МЭ) = 0,003 в день; γ (интенсивность нахождения уязвимостей в МЭ) = 0,0328 в день; μ (интенсивность проверок функционирования МЭ с приведением его в рабочее состояние) = 0,0328 в день; φ (интенсивность устранения уязвимостей) = 0,0328 в день; ρ (интенсивность создания новой информации) = 1 в день. Аппаратный МЭ обеспечивает следующие характеристики: λ = 1 в день; β = 0,0003 в день; γ = 0,00328 в день; μ = 0,0328 в день; φ = 0,0328 в день; ρ = 1 в день.

Среднее время преодоления программного МЭ с приведенными выше параметрами будет составлять 14 дней, а время преодоления аппаратного МЭ 155 дней. Графики зависимости времени преодоления от интенсивности появления уязвимостей для программного и аппаратного МЭ показаны на рисунке 2.

Среднее время преодоления СЗИ должно быть больше времени актуальности защищаемой информации. Время актуальности информации зависит от того какая информации обрабатывается: оперативная, тактическая или стратегическая.

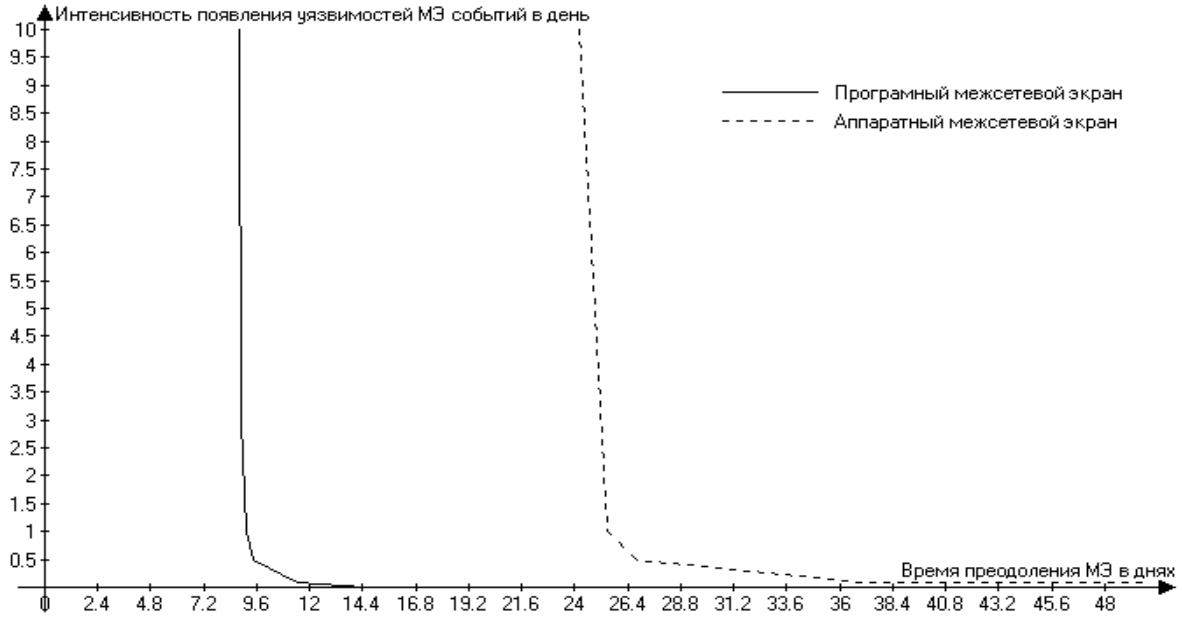

Рисунок 2. Зависимость времени преодоления МЭ от уязвимостей в МЭ

Из полученных результатов можно утверждать, что изменение одного из параметров имеет сильное влияние на время преодоления СЗИ только до определенных значений, затем значения остальных параметров не дают быстро изменяться времени преодоления СЗИ. Таким образом, модель позволяет не только вычислять среднее время преодоления СЗИ, но и обосновать математически регламенты обслуживания оборудования отвечающего за защиту информации на предприятии.

Библиографический список

1. Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. Наука и техника, Санкт-Петербург, 2004

2. Пловко А. М., Гуров С. В. Основы теории надежности. Практикум. – СПб.: БХВ-Петербург, 2006.

A.A. Ponomarev

MODEL OF RELIABILITY OF INFORMATION PROTECTION SYSTEM

Abstract. The article is devoted to the received model information security system which allows calculating average time of overcoming by the intruder, using the theory of mass service.