УДК 519.8

МОДЕЛЬ ЗАЩИТЫ МНОГОКАНАЛЬНЫХ АВТОМАТИЗИРОВАННЫХ КОМПЛЕКСОВ ОТ DDOS-АТАК

В.А. Минаев
доктор технических наук, профессор
Московский государственный технический университет им. Н. Э. Баумана
E-mail: m1va@yandex.ru

И.Д. Королев
доктор технических наук, профессор
Краснодарское высшее военное училище им. генерала армии С. М. Штеменко
E-mail: pi_korolev@mail.ru

М. П. Сычев
доктор технических наук, профессор
Московский государственный технический университет им. Н. Э. Баумана
E-mail: mpsichov@sm.bmstu.ru

О.В.Петрова
кандидат технических наук, доцент
Краснодарское высшее военное училище им. генерала армии С. М. Штеменко
E-mail: Odi16.na@gmail.com

Аннотация.Моделируется система защиты автоматизированных информационных систем (АИС) от DDoS-атак. Осуществляется постановка задачи распределения потока заявок в системе многоканального обслуживания с различной пропускной способностью каналов. Приводятся формулы для расчета предельных вероятностей отказа системы при установившемся режиме обработки поступающих заявок.

Ключевые слова: автоматизированная информационная система, моделирование системы защиты, система массового обслуживания.

SECURITY MODEL OF MULTI-CHANNEL AUTOMATED SYSTEMS FROM DDOS-ATTACKS

V.A. Minaev, I.D. Korolev, M.P. Sychev, O.V.Petrova

Abstract. The system of automated information systems (AIS) protection from DDoS-attacks is simulated. The problem of the flow of applications allocation in the system of multi-channel service with different channel capacity is formulated. The formulas for calculating the maximum probability of the system failure in the steady-state processing of incoming applications are given.

Keywords: automated system, modeling, protection system, queuing system.

Введение

Сегодня одним из распространенных видов компьютерных атак на АИС, приводящих к отказу в обслуживании, являются DDoS-атаки [3 - 10]. Поэтому вопросы защиты от них автоматизированных информационных систем (АИС) при их взаимодействии с сетями

общего доступа представляются весьма актуальными. В работе рассматривается новая модель защиты за счет выявления и применения ее синергетических свойств.

Система защиты должна полностью контролировать не только внутренние процессы АИС, но и внешние, связанные с передачей данных по каналам связи. Причем речь идет не только об обеспечении защиты канала связи криптографическими средствами, но и об оптимальном управлении каналами для безотказного обслуживания удаленных пользователей [6-8]. Это позволяет максимально защитить АИС от компьютерных атак типа «отказ в обслуживании» по минимальной стоимости.

Очевидно, что одиночный канал обслуживания при большой интенсивности воздействии злоумышленника на АИС делает её работу неэффективной [3-5]. Предположим, что многопроцессорное, многоканальное аппаратное обеспечение АИС, как “обслуживающего прибора”, полностью справляется с потоками заявок.

Постановка задачи

Рассмотрим систему защиты АИС от DDoS-атак, которая обладает основным защищенным каналом передачи информации и двумя запасными. Применение трех независимых каналов повышает информационную связность АИС с удаленными пользователями, а, следовательно – доступность АИС и устойчивость ее функционирования [4,5]. Оценку надежности функционирования будем вычислять через показатели отказа в обслуживании АИС после осуществления DDoS-атак.

Пусть имеется подсистема защиты АИС, состоящая из внешнего процесса, обеспечивающего информационное взаимодействие с удаленными абонентами, и внутреннего, обеспечивающего безопасную обработку и хранение данных в АИС. Будем считать, что безотказность работы в АИС на ее внутреннем уровне всегда обеспечивается. Основное внимание уделим обеспечению безотказной работы в АИС на уровне внешнего процесса, описываемого в следующем виде:

$$\Pi_{\text{внешн}} = \langle \mathrm{B}, \mathrm{A}_n, \rangle;\ n = 1,2,3;$$

где: *B* – система распределения заявок по каналам;

A_1 – основной канал с пропускной способностью μ_0;

A_2, A_3 – резервные каналы с пропускными способностями μ_1 и μ_2, соответственно;

Введём допущение: при включении запасных каналов их иерархия определяется случайным образом, при этом каналы выбираются последовательно, в прямом порядке, освобождаясь также поочередно, в обратном порядке.

Получение заявок будем рассматривать как простейший поток событий со следующими параметрами [1, 2]:

λ – плотность потока (среднее число событий, приходящееся в единицу времени);

$F(t) = 1 - e^{-\lambda t}$ – закон распределения вероятности появления одного события за время *t*;

$P_0(t) = e^{-\lambda t}$ – вероятность того, что за время t не появится ни одна заявка.

В каналах происходит обработка поступивших заявок, причем время обработки заявки ($m_{iобр}$) распределено по показательному закону [1-3]:

$$g(t) = \mu_i . e^{\mu_i \cdot t}, (i=0, 1, 2);$$

$$\mu_i = {}^{1}/_{m_{iобр}}, (i=0, 1, 2).$$

Итак, будем рассматривать систему защиты АИС как трехканальную СМО с отказами, причём обработка запросов на каждом канале происходит с различной интенсивностью μ_i; *i=0, 1, 2*. Имеем следующие состояния системы: 0 – свободны все каналы; 1 – занят первый канал; 2 – заняты первые 2 канала; 3 – заняты все 3 канала.

Найдем вероятность безотказной работы рассматриваемой системы защиты.

Решение задачи

Определим вероятности состояния системы в каждый из моментов времени

$$P_0(t), P_1(t), P_2(t), P_3(t), \quad (1)$$

при условии

$$\sum_{k=0}^{3} P_k(t)=1.$$

Составим дифференциальные уравнения для состояний системы (1).

1. Зафиксируем момент времени *t* и найдем вероятность того, что в момент времени $t+\Delta t$ система будет находиться в состоянии *0*. Это возможно при:

A – в момент *t* система находилась в состоянии *0* и за промежуток времени Δt не переходит в другое состояние;

B – в момент *t* система находилась в состоянии *1* и за промежуток времени Δt переходит в состояние *0*.

$$P_0(t) + P_0(t + \Delta t) = P(A) + P(B). \quad (2)$$

Вероятность события *A* равна:

$$P(A) = P_0(t) \cdot e^{-\lambda \cdot \Delta t} \approx P_0(t) \cdot (1 - \lambda \cdot \Delta t). \quad (3)$$

Вероятность события B равна:

$$P(B) = P_1(t) \cdot \mu_0 \cdot \Delta t\,. \quad (4)$$

Подставим в формулу вероятности нахождения системы в состоянии *0* значения из формул (3), (4) [1]:

$$P_0(t+\Delta t) = P_0(t)\cdot(1-\lambda\cdot\Delta t) + P_1(t)\cdot\mu_0\cdot\Delta t,$$

$$P_0(t+\Delta t) + P_0(t) = -P_0(t)\cdot\lambda\cdot\Delta t + P_1(t)\cdot\mu_0\cdot\Delta t.$$

Разделим обе части на Δt, и при t→0 перейдем к дифференциальному уравнению:

$$\frac{\partial P_0(t)}{\partial t} = -P_0(t)\cdot\lambda + P_1(t)\cdot\mu_0. \quad (5)$$

2. Далее зафиксируем момент времени *t* и найдем вероятность того, что в момент времени *t*+Δ*t* система будет находиться в состоянии *1*. Это возможно при:

A – в момент *t* система находилась в состоянии *1* и за промежуток времени Δt не перешла в другое состояние.

B – в момент *t* система находилась в состоянии *2* и за промежуток времени Δ*t* перешла в состояние *1*.

C – в момент t система находилась в состоянии 3 и за промежуток времени Δ*t* перешла в состояние *1*.

$$P_1(t+\Delta t) = P(A) + P(B) + P(C), \quad (6)$$

$$P(A) = P_1(t)\cdot e^{-(\lambda+\mu_0)\cdot\Delta t} \approx P_1(t)\cdot(1-(\lambda+\mu_0)\cdot\Delta t), \quad (7)$$

$$P(B) = P_2(t)\cdot(1-e^{-\mu_1\cdot\Delta t}) \approx P_2(t)\cdot\mu_1\cdot\Delta t, \quad (8)$$

$$P(C) = P_0(t)\cdot e^{-\lambda\cdot\Delta t} \approx P_0(t)\cdot\lambda\cdot\Delta t. \quad (9)$$

Подставим в формулу вероятности (6) значения из формул (7-9) [1]:

$$P_1(t+\Delta t) = P_1(t)\cdot(1-(\lambda+\mu_0)\cdot\Delta t) + P_2(t)\cdot\mu_1\cdot\Delta t + P_0(t)\cdot\lambda\cdot\Delta t$$

Переходя к дифференциальному уравнению, получим:

$$P_1(t+\Delta t) = P_1(t)\cdot(1-(\lambda+\mu_0)\cdot\Delta t) + P_2(t)\cdot\mu_1\cdot\Delta t + P_0(t)\cdot\lambda\cdot\Delta t$$

$$\frac{\partial P_1(t)}{\partial t} = -P_1(t)\cdot(\lambda+\mu_0) + P_2(t)\cdot\mu_1 + P_0(t)\cdot\lambda \quad (10)$$

3. Теперь зафиксируем момент времени t и найдем вероятность того, что в момент времени *t*+Δ*t* система будет находиться в состоянии 2. Опуская промежуточные вычисления, аналогично получим дифференциальное уравнение:

$$\frac{\partial P_2(t)}{\partial t} = -P_2(t)\cdot(\lambda+\mu_1) + P_3(t)\cdot\mu_2 + P_1(t)\cdot\lambda. \quad (11)$$

4. Наконец, по аналогии получим дифференциальное уравнение:

$$\frac{\partial P_3(t)}{\partial t} = -P_3(t)\cdot\mu_2 + P_2(t)\cdot\lambda. \quad (12)$$

Таким образом, получаем систему дифференциальных уравнений (5, 10, 11, 12) [1]:

$$\begin{cases} \frac{\partial P_0(t)}{\partial t} = -P_0(t)\cdot\lambda + P_1(t)\cdot\mu_0 \\ \frac{\partial P_1(t)}{\partial t} = -P_1(t)\cdot(\lambda+\mu_0) + P_2(t)\cdot\mu_1 + P_0(t)\cdot\lambda \\ \frac{\partial P_2(t)}{\partial t} = -P_2(t)\cdot(\lambda+\mu_1) + P_3(t)\cdot\mu_2 + P_1(t)\cdot\lambda \\ \frac{\partial P_3(t)}{\partial t} = -P_3(t)\cdot\mu_2 + P_2(t)\cdot\lambda \end{cases} \quad (13)$$

Из (13) найдем предельные вероятности состояний системы в установившемся режиме [1]:

$$P_0 = \frac{\mu_0\mu_1\mu_2}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}, \quad (14)$$

$$P_1 = \frac{\lambda\mu_1\mu_2}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}, \quad (15)$$

$$P_2 = \frac{\lambda^2\mu_2}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}, \quad (16)$$

$$P_3 = \frac{\lambda^3}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}. \quad (17)$$

Вероятность отказа системы при заданном порядке обработки поступающих заявок определяется по формуле (17).

Рассмотрим полное множество гипотез о порядке выбора каналов при поступлении заявок для обработки:

$Г_1$ – пока не занят канал A_1 заявки поступают на него, если он занят, заявки поступают на A_2, если и A_2 занят, то заявки поступают на A_3;

$Г_2$ – пока не занят канал A_1 заявки поступают на него, если он занят, заявки поступают на A_3, если и A_3 занят, то заявки поступают на A_2;

$Г_3$ – пока не занят канал A_2 заявки поступают на него, если он занят, заявки поступают на A_1, если и A_1 занят, то заявки поступают на A_3;

$Г_4$ – пока не занят канал A_2 заявки поступают на него, если он занят, заявки поступают на A_3, если и A_3 занят, то заявки поступают на A_1;

$Г_5$ – пока не занят канал A_3 заявки поступают на него, если он занят, заявки поступают на A_1, если и A_1 занят, то заявки поступают на A_2;

$Г_6$ – пока не занят канал A_3 заявки поступают на него, если он занят, заявки поступают на A_2, если и A_2 занят, то заявки поступают на A_1.

Т.к. заявки распределяются по каналам с различными вероятностями появления каждой гипотезы $P(Г_i)$, то по формуле полной вероятности:

$$P_{\text{отк}} = \sum_{i=1}^{6} P(Г_i)\cdot P_{\text{отк}Г_i}, \quad (18)$$

где $P_{откГ_i}$ - вероятность отказа системы при принятии i-ой гипотезы.

$P_{откГ_i}$ рассчитаем, используя формулу (17) и учитывая порядок нумерации каналов:

$$P_{откГ_1} = \frac{\lambda^3}{\mu_0\mu_1\mu_2+\lambda\mu_1\mu_2+\lambda^2\mu_2+\lambda^3}, \quad (19)$$

$$P_{откГ_2} = \frac{\lambda^3}{\mu_0\mu_1\mu_2+\lambda\mu_1\mu_2+\lambda^2\mu_0+\lambda^3}, \quad (20)$$

$$P_{откГ_3} = \frac{\lambda^3}{\mu_0\mu_1\mu_2+\lambda\mu_0\mu_2+\lambda^2\mu_2+\lambda^3}, \quad (21)$$

$$P_{откГ_4} = \frac{\lambda^3}{\mu_0\mu_1\mu_2+\lambda\mu_0\mu_2+\lambda^2\mu_0+\lambda^3}, \quad (22)$$

$$P_{откГ_5} = \frac{\lambda^3}{\mu_0\mu_1\mu_2+\lambda\mu_1\mu_0+\lambda^2\mu_1+\lambda^3}, \quad (23)$$

$$P_{откГ_6} = \frac{\lambda^3}{\mu_0\mu_1\mu_2+\lambda\mu_1\mu_0+\lambda^2\mu_0+\lambda^3}. \quad (24)$$

Подставив формулы (19-24) в формулу нахождения полной вероятности отказа системы (18), получим:

$$P_{отк} = \lambda^3\left(\frac{P(\Gamma_1)}{\mu_0\mu_1\mu_2+\lambda\mu_1\mu_2+\lambda^2\mu_2+\lambda^3} + \frac{P(\Gamma_2)}{\mu_0\mu_1\mu_2+\lambda\mu_1\mu_2+\lambda^2\mu_0+\lambda^3} + \frac{P(\Gamma_3)}{\mu_0\mu_1\mu_2+\lambda\mu_0\mu_2+\lambda^2\mu_2+\lambda^3} + \frac{P(\Gamma_4)}{\mu_0\mu_1\mu_2+\lambda\mu_0\mu_2+\lambda^2\mu_0+\lambda^3} + \frac{P(\Gamma_5)}{\mu_0\mu_1\mu_2+\lambda\mu_1\mu_0+\lambda^2\mu_0+\lambda^3} + \frac{P(\Gamma_6)}{\mu_0\mu_1\mu_2+\lambda\mu_0\mu_1+\lambda^2\mu_1+\lambda^3}\right) \quad (25)$$

Покажем для простых случаев, как оценивать параметры потока заявок, когда необходимо подключать запасные защищенные каналы [4,5]. Для этого рассмотрим вначале работу только основного канала [6,7], т.е. одноканальную систему массового обслуживания с отказами. В этом случае вероятность отказа рассчитывается по формуле:

$$P_{отк} = \frac{\frac{\lambda}{\mu_1}}{1+\frac{\lambda}{\mu_1}} = \frac{\lambda}{\mu_1+\lambda}. \quad (26)$$

Для АИС допустимой вероятностью отказа является значение, не превышающее 0,05 [8,10]. Найдем максимальное допустимое значение λ, при котором обеспечивается безотказная работа основного канала:

$$P_{отк} \le 0{,}05,$$

$$\frac{\lambda}{\mu_1+\lambda} \le 0{,}05,$$

$$\lambda \le \frac{\mu_1}{19}. \quad (27)$$

Таким образом, при значениях потока заявок, превышающего условие (27), система защиты не может обеспечить безотказную работу АС и необходимо подключать запасной канал A_2 [9,10].

Найдем вероятность отказа данной системы при включении запасного канала A_2. Для этого рассмотрим двухканальную СМО с отказами. Введем состояния: 0 – свободны все каналы; 1 – занят первый канал; 2 – заняты два канала.

Исходя из рассуждений, описанных выше, найдем вероятность отказа данной системы:

$$\begin{cases} 0 = -P_0\lambda + P_1\mu_0 \\ 0 = -P_1(\lambda + \mu_0) + P_2\mu_1 + P_0\lambda \\ 0 = -P_2\mu_1 + P_1\lambda \\ \sum_{k=0}^{2} P_k = 1 \end{cases}, \quad (28)$$

$$P_1 = \frac{P_0\lambda}{\mu_0}. \quad (29)$$

$$P_2 = \frac{P_0\lambda^2}{\mu_0\mu_1}, \quad (30)$$

$$P_0 = \frac{\mu_0\mu_1}{\mu_0\mu_1 + \lambda\mu_1 + \lambda^2}. \quad (31)$$

Подставим значение из (31) в уравнения (29), (30):

$$P_1 = \frac{\lambda\mu_1}{\mu_0\mu_1 + \lambda\mu_1 + \lambda^2},$$

$$P_2 = \frac{\lambda^2}{\mu_0\mu_1 + \lambda\mu_1 + \lambda^2}. \quad (32)$$

Найдем максимальное допустимое значение потока заявок, при котором обеспечивается безотказная работа основного и одного запасного каналов:

$$P_{отк} \leq 0{,}05,$$

$$\frac{\lambda^2}{\mu_0\mu_1 + \lambda\mu_1 + \lambda^2} \leq 0{,}05,$$

$$38 \cdot \lambda^2 - \lambda \cdot \mu_1 - \mu_1 \cdot \mu_0 \leq 0 \quad (33)$$

Находя и исследуя корни (33), находим:

$$\lambda \leq \frac{\mu_1}{38}\left(1 + \sqrt{1 + 76 \cdot \frac{\mu_0}{\mu_1}}\right. \quad (34)$$

Таким образом, при значениях параметров потока, не удовлетворяющих условию (34), система защиты не может обеспечить безотказную работу АИС, и необходимо подключать второй запасной канал обработки информации A_3.

Выводы

1. Чтобы в ходе реализации DDoS-атак на АИС избежать отказы в обслуживании потока заявок, необходимо заблаговременно реагировать на изменения последнего, адаптивно подстраивая общую пропускную способность каналов автоматизированных комплексов в соответствии, например, с (19) - (25) при трехканальной системе.

2. Подобным же образом возможно производить расчеты при большем числе каналов. В случае возникновения сложностей при аналитическом представлении вероятностей отказа, возможно построение имитационной модели системы защиты АИС [11, 12].

3. Для предварительных расчетов ограничений потоков применительно к простым системам массового автоматизированного обслуживания целесообразно использовать соотношения (27) и (34).

ЛИТЕРАТУРА

1. *Вентцель Е.С.* Теория вероятностей: Учебник. 11-е изд., стереотипное. М.: КНОРУС, 2010. 664 с.
2. *Матвеев В.Ф., Ушаков В.Г.* Системы массового обслуживания: Учебное пособие. М.: Изд-во МГУ, 1984. 242 с.
3. *Коценяк М.А., Кулешов И.А., Лаута О.С.* Устойчивость информационно-телекоммуникационных сетей. СПб: Изд-во Политехнического университета, 2013. 93 с.
4. *Богово А.В. Игнатов В.В.* Эффективность систем военной связи и методы ее оценки: Монография. СПб: ВАС, 2006. 183 с.
5. *Боговик А.В. Игнатов В.В.* Теория управления в системах военного назначения: Учебник. СПб: ВАС, 2008. 460 с.
6. *Королев И.Д., Петрова О.В.* Разработка модели защиты информации, обрабатываемой в вычислительных сетях, от компьютерных атак // Известия вузов. Северокавказский регион. Технические науки. 2006. №1. – С. 68-73.
7. *Королев И.Д., Петрова О.В., Сураев А.С.* Разработка модели защиты информации, обрабатываемой в вычислительных сетях, от компьютерных атак // Сборник трудов. Краснодар: ФВАС, 2011. – С. 34-40.
8. *Королев И.Д., Петрова О.В., Малышев Д.В., Пунин К.В., Шайков И.Н.* Модель защищенности комплекса средств автоматизации специального назначения // Телекоммуникации. 2016. № 9. – С. 41-44.
9. *Королев И.Д., Петрова О.В., Исупов А.Б., Юрков В.А.* Моделирование процесса функционирования телекоммуникационной сети в условиях программно-аппаратных воздействий // Научный журнал КубГАУ. 2012. №81(07). С. 2-12.
10. *Королев И.Д., Петрова О.В., Пугин К.В., Мухортов В.В., Солодовников А.С.* Определение параметров защищенности АСУ, работающей в условиях информационного противоборства // Свидетельство о государственной регистрации программы для ЭВМ № 2016611851, Российская Федерация. Зарегистрировано в реестре программ для ЭВМ 11.02.2016.
11. *Фисун А.П., Касилов А.Г., Фисенко В.Е., Минаев В.А., Афанасьев В.В., Митяев В.В., Фисун Р.А., Джевага К.А., Кожухов С.А.* Развитие методологических основ информатики и информационной безопасности систем: Депонированная рукопись. Дата депонирования: 07.07.2004, №: 1165-В2004. М.: ВИНИТИ, 2004. 253 с.

12. *Чекалин А.А., Скрыль С.В., Минаев В.А.* Комплексный технический контроль эффективности мер безопасности систем управления в органах внутренних дел: Учебное пособие для высших учебных заведений МВД России. Часть 2. Практические аспекты технической разведки и комплексного технического контроля. М.: Научно-техническое издательство "Горячая линия-Телеком", 2006. 205 с.

УДК 004.94

СУПЕРЭВМ И ОПЕРАЦИОННЫЕ СИСТЕМЫ НОВОГО ПОКОЛЕНИЯ

А.С. Моляков
кандидат технических наук
Российский государственный гуманитарный университет
E-mail: andrei_molyakov@mail.ru

Аннотация. Автор ответил на следующие четыре конкретных вопроса: какие новые угрозы информационной безопасности исходят непосредственно от суперкомпьютеров, какие суперкомпьютеры в этом плане наиболее опасны, какие новые возможности обеспечения кибербезопасности могут предоставить суперкомпьютеры, суперкомпьютеры какого типа для этого лучше подходят. Проиллюстрированы подходы к организации обеспечения национальной кибербезопасности, а также создания сил и средств ведения кибервойн.

Ключевые слова: СуперЭВМ, кибербезопасность, ОС нового поколения, массово-мультитредовый модуль, высокоэффективный маршрутизатор.

SUPERCOMPUTERS AND NEXT GENERATION OPERATION SYSTEMS

A.S. Molyakov

Annotation. The author answered the following four specific questions: what new information security threats come directly from supercomputers, which supercomputers are most dangerous in this regard, what new cybersecurity opportunities supercomputers can provide, what kind of supercomputers are better suited for this. Approaches to the organization of national cyber security, as well as the creation of forces and means of conducting cyberwars, are illustrated in this article.

Keywords: Supercomputers, cybersecurity, next generation OS, massive-multithreaded module, hi-speed router.

Применение суперкомпьютеров с новой архитектурой, в частности, массово-мультитредовой требует определённых знания и умения. Это исследуется сейчас в ведущих центрах. По линии массово-мультитредовых архитектур выделяется Центр CASS-MT Северо-западной тихоокеанской национальной лаборатории (PNNL) Министерства энергетики США, где исследуются возможности массово-мультитредовых архитектур и ведётся разработка программного обеспечения для них. В финансировании и организации работ участвует разведсообщество США. В проекте участвуют PNNL, фирма Cray, Лаборатория Sandia и технологический университет Джорджии [1, 2].