Модель системы защиты многоканальных автоматизированных комплексов от ddos атак с учетом освобождения по мере обработки каналов

И.Д. Королев, О.В. Петрова, И.О. Овчаренко, Д.В. Леонов

Краснодарское высшее военное училище им. генерала армии С.М. Штеменко

Аннотация: Рассматривается решение задачи поиска вероятностной характеристики нахождения многоканальной системы безопасности в конкретных состояниях функционирования при обмене информацией с сетями общего доступа. Актуальность данной проблемы заключается в том, что один защищенный канал не может обеспечить достаточную пропускную способность, особенно в условиях, когда рассматриваются большие потоки ложной информации, посылаемой на защищаемый ресурс оппонентом и не своевременность подключения запасных каналов может привести к потере важной информации, поступающей в систему. Выполнение стоящей перед системой защиты задачи возможно только при использовании многоканальной системы.
В работе приведен анализ принципов работы многоканальной системы защиты. Анализ показал, что для решения задачи обеспечения безопасной связи с внешним ресурсом через сети общего доступа целесообразно использовать многоканальную систему с разной пропускной способностью каналов, при этом должен быть определен основной канал и запасные, которые подключаются к работе при невозможности основным каналом обрабатывать все поступающие заявки с вероятностью 0,95. В данной модели учитывается, что каналы заполняются иерархически, а освобождаются по мере обработки поступивших заявок.
Целью данной работы является нахождение условия включения запасных защищенных каналов обработки информации путем оценки вероятности безотказной работы автоматизированной информационной системы при возникновении большой нагрузки на защищенный канал передачи информации с особой спецификацией. Для достижение данной цели в работе применяется рассмотрение подсистемы защиты как многоканальной СМО с разной пропускной способностью каналов.
Ключевые слова: автоматизированная система, моделирование, подсистема защиты, система массового обслуживания, вероятностная оценка.

Сегодня одним из распространенных видов компьютерных атак на АИС, приводящих к отказу в обслуживании, являются DDoS-атаки [1]. Поэтому вопросы защиты от них автоматизированных информационных систем (АИС) при их взаимодействии ее с сетями общего доступа представляются весьма перспективными. В данной статье рассматривается новая модель защиты за счет выявление 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 [2]. 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 ее работу неэффективной [3]. Предположим, что многопроцессорное, многоканальное аппаратное обеспечение АИС, как “обслуживающего прибора”, полностью справляется с потоками заявок.

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]. 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 [5]. Основное внимание уделим обеспечению безотказной работы в АИС на уровне внешнего процесса, описываемого в следующем виде:

$$\Pi_{внешн} = \langle B, A_n, \rangle;\ n = 1,2,3;$$

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.

Введем допущение: каналы выбираются последовательно, в прямом порядке, освобождаясь по мере обработки заявок.

Получение заявок будем рассматривать как простейший поток событий со следующими параметрами [6]:

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 ($m_{i\text{обр}}$) распределено по показательному закону [7]:

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

$$\mu_i = 1/m_{i\text{обр}}, (i=0, 1, 2).$$

Итак, будем рассматривать систему защиты АИС как трехканальную СМО с отказами, причем обработка запросов на каждом канале происходит с разной интенсивностью μ_i: ($i=0, 1, 2$).

Найдем значение плотности потока заявок, при которой необходимо подключать запасные защищенные каналы обработки информации [8] и вероятность безотказной работы рассматриваемой системы защиты.

Для этого рассмотрим данную систему при работе только одного основного канала [9].

Тогда мы можем рассмотреть данную подсистему защиты как одноканальную систему массового обслуживания с отказами. Тогда вероятность отказа считается по формуле:

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

Так как для автоматизированной системы специального назначения допустимой вероятностью отказа является значение, не превышающее 0,05 [10], то мы можем найти максимальное допустимое значение плотности потока заявок, при котором обеспечивается надежное безотказное состояние основного канала:

$$P_{\text{отк}} \leq 0{,}05 \quad (2)$$

$$\frac{\lambda}{\mu_1+\lambda} \leq 0{,}05 \quad (3)$$

$$\frac{0{,}95\lambda - 0{,}05\mu_1}{\mu_1+\lambda} \leq 0 \quad (4)$$

Так как $\lambda \succ 0$ и $\mu_1 \succ 0$, то получаем:

$$0{,}95\lambda - 0{,}05\mu_1 \leq 0 \quad (5)$$

$$\lambda \leq \frac{\mu_1}{19} \quad (6)$$

Таким образом при значениях плотности потока заявок не удовлетворяющим условию (37), система защиты не может обеспечить безотказную работу АИС и необходимо подключать запасной канал обработки информации A_2 [11].

Найдем вероятность отказа данной системы при включении запасного канала A_2 (рис.1).

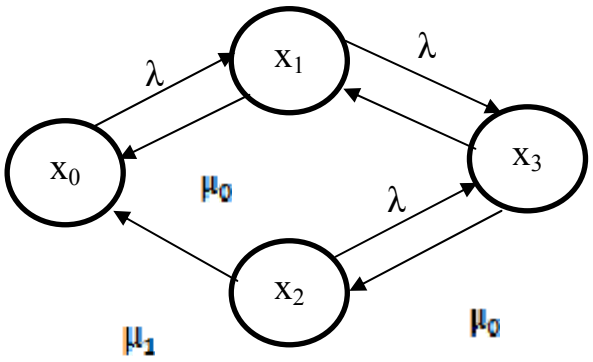

Рис. 1 - Вероятность отказа данной подсистемы при включении запасного канала A_2.

Для этого рассмотрим следующие состояния системы:

x_0 – свободны все каналы;

x_1 – занят первый канал;

x_2 – занят второй канал.

x_3 – заняты 2 канала.

Определим вероятности состояния системы в каждый из моментов времени *t*

$$P_0(t),\ P_1(t),\ P_2(t),\ P_3(t), \tag{7}$$

при условии

$$\sum_{k=0}^{3} P_k(t) = 1 \tag{8}$$

Составим дифференциальные уравнения для состояний системы (7).

1. Зафиксируем момент времени t и найдем вероятность того, что в момент времени $t+\Delta t$ система будет находиться в состоянии x_0. Это возможно при:

A – в момент t система находилась в состоянии x_0 и за промежуток времени Δt не переходит в другое состояние;

B – в момент t система находилась в состоянии x_1 и за промежуток времени Δt переходит в состояние x_0.

C – в момент t система находилась в состоянии x_2 и за промежуток времени Δt переходит в состояние 0.

$$P_0(t) + P_0(t+\Delta t) = P(A) + P(B) + P(C) \quad (9)$$

Вероятность события A равна:

$$P(A) = P_0(t) \cdot e^{-\lambda \cdot \Delta t} \approx P_0(t) \cdot (1 - \lambda \cdot \Delta t) \quad (10)$$

Вероятность события B равна:

$$P(B) = P_1(t) \cdot \mu_0 \cdot \Delta t \quad (11)$$

Вероятность события C равна:

$$P(C) = P_2(t) \cdot \mu_1 \cdot \Delta t \quad (12)$$

Подставим в формулу вероятности нахождения системы в состоянии x_0 значения из формул (10-12) [12]:

$$P_0(t+\Delta t) = P_0(t) \cdot (1 - \lambda \cdot \Delta t) + P_1(t) \cdot \mu_0 \cdot \Delta t + P_2(t) \cdot \mu_1 \cdot \Delta t \quad (13)$$

$$P_0(t+\Delta t) + P_0(t) = -P_0(t) \cdot \lambda \cdot \Delta t + P_1(t) \cdot \mu_0 \cdot \Delta t + P_2(t) \cdot \mu_1 \cdot \Delta t \quad (14)$$

Разделим обе части на Δt, и при $t \to 0$ перейдем к дифференциальному уравнению:

$$\frac{\partial P_0(t)}{\partial t} = -P_0(t) \cdot \lambda + P_1(t) \cdot \mu_0 + P_2(t) \cdot \mu_1 \quad (15)$$

2. Далее зафиксируем момент времени t и найдем вероятность того, что в момент времени $t+\Delta t$ система будет находиться в состоянии x_1. Это возможно при:

A – в момент t система находилась в состоянии x_1 и за промежуток времени Δt не перешла в другое состояние.

B – в момент t система находилась в состоянии x_3 и за промежуток времени Δt перешла в состояние x_1.

C – в момент t система находилась в состоянии x_0 и за промежуток времени Δt перешла в состояние x_1.

$$P_1(t+\Delta t) = P(A) + P(B) + P(C) \quad (16)$$

$$P(A) = P_1(t) \cdot e^{-(\lambda+\mu_0)\cdot\Delta t} \approx P_1(t) \cdot (1 - (\lambda+\mu_0)\cdot\Delta t) \quad (17)$$

$$P(B) = P_3(t) \cdot (1 - e^{-\mu_1\cdot\Delta t}) \approx P_3(t) \cdot \mu_1 \cdot \Delta t \quad (18)$$

$$P(C) = P_0(t) \cdot e^{-\lambda\cdot\Delta t} \approx P_0(t) \cdot \lambda \cdot \Delta t \quad (19)$$

Подставим в формулу вероятности (10) значения из формул (17-19) [1]:

$$P_1(t+\Delta t) = P_1(t) \cdot (1 - (\lambda+\mu_0)\cdot\Delta t) + P_3(t) \cdot \mu_1 \cdot \Delta t + P_0(t) \cdot \lambda \cdot \Delta t \quad (20)$$

Переходя к дифференциальному уравнению, получим:

$$P_1(t+\Delta t) = P_1(t) \cdot (1 - (\lambda+\mu_0)\cdot\Delta t) + P_3(t) \cdot \mu_1 \cdot \Delta t + P_0(t) \cdot \lambda \cdot \Delta t \quad (21)$$

$$\frac{\partial P_1(t)}{\partial t} = -P_1(t) \cdot (\lambda+\mu_0) + P_3(t) \cdot \mu_1 + P_0(t) \cdot \lambda \quad (22)$$

3. Теперь зафиксируем момент времени t и найдем вероятность того, что в момент времени $t+\Delta t$ система будет находиться в состоянии x_2. Опуская промежуточные вычисления, аналогично получим дифференциальное уравнение:

Отсюда аналогично переходим к дифференциальному уравнению:

$$\frac{\partial P_2(t)}{\partial t} = -P_2(t)\cdot(\lambda+\mu_1)+P_3(t)\cdot\mu_0 \quad (23)$$

4. Наконец, по аналогии получим дифференциальное уравнение для состояния x_3:

$$\frac{\partial P_3(t)}{\partial t} = -P_3(t)\cdot(\mu_1+\mu_0)+P_2(t)\cdot\lambda+P_1(t)\cdot\lambda \quad (24)$$

Таким образом, получаем систему дифференциальных уравнений (8, 15, 22, 23, 24) [1]:

$$\begin{cases} \frac{\partial P_0(t)}{\partial t} = -P_0(t)\cdot\lambda + P_1(t)\cdot\mu_0 + P_2(t)\cdot\mu_1 \\ \frac{\partial P_1(t)}{\partial t} - -P_1(t)\cdot(\lambda+\mu_0)+P_2(t)\cdot\mu_1+P_0(t)\cdot\lambda \\ \frac{\partial P_2(t)}{\partial t} = -P_2(t)\cdot(\lambda+\mu_1)+P_3(t)\cdot\mu_0 \\ \frac{\partial P_3(t)}{\partial t} = -P_3(t)\cdot(\mu_1+\mu_0)+P_2(t)\cdot\lambda+P_1(t)\cdot\lambda \\ P_0(t)+P_1(t)+P_2(t)+P_3(t)=1 \end{cases} \quad (25)$$

Из (25) найдем предельные вероятности состояний системы в установившемся режиме:

$$P_0 = \frac{\mu_0\mu_1(\mu_0+\mu_1)}{\lambda^2(\lambda+\mu_1+\mu_0)+\lambda\mu_1(\lambda+\mu_0+\mu_1)+\mu_0\mu_1(\mu_0+\mu_1)} \quad (26)$$

$$P_1 = \frac{\lambda\mu_1(\lambda+\mu_0+\mu_1)}{\lambda^2(\lambda+\mu_1+\mu_0)+\lambda\mu_1(\lambda+\mu_0+\mu_1)+\mu_0\mu_1(\mu_0+\mu_1)} \quad (27)$$

$$P_2 = \frac{\lambda^2\mu_0}{\lambda^2(\lambda+\mu_1+\mu_0)+\lambda\mu_1(\lambda+\mu_0+\mu_1)+\mu_0\mu_1(\mu_0+\mu_1)} \quad (28)$$

$$P_3 = \frac{\lambda^2(\lambda+\mu_1)}{\lambda^2(\lambda+\mu_1+\mu_0)+\lambda\mu_1(\lambda+\mu_0+\mu_1)+\mu_0\mu_1(\mu_0+\mu_1)} \quad (29)$$

Найдем максимальное допустимое значение плотности потока заявок, при котором обеспечивается надежное безотказное состояние основного и одного запасного каналов:

$$P_{отк} \leq 0{,}05 \tag{30}$$

$$\frac{\lambda^2(\lambda+\mu_1)}{\lambda^2(\lambda+\mu_1+\mu_0)+\lambda\mu_1(\lambda+\mu_0+\mu_1)+\mu_0\mu_1(\mu_0+\mu_1)} \leq 0{,}05 \tag{31}$$

Так как знаменатель больше нуля, получаем:

$$0{,}95\lambda^2 + (0{,}9\mu_1 - 0{,}05\mu_0)\lambda^2 - 0{,}05(\mu_0+\mu_1)\mu_1\,\lambda -$$

$$-0{,}05\mu_0\mu_1(\mu_0+\mu_1) \leq 0 \tag{32}$$

Так, при известных μ_0 и μ_1 мы можем найти значение плотности потока заявок, при которой два канала не могут обеспечить безотказную работу АИС и необходимо подключать второй запасной канал обработки информации A_3. Для автоматизированной системы специального назначения допустимой вероятностью отказа является значение не большее 0,05.

В качестве примера рассмотрим следующие, возможные варианты интенсивностей плотности потока заявок и интенсивностей обработки запросов на каждом канале:

пусть система защиты АИС от DDoS атак, обладает основным защищенным каналом передачи информации и двумя запасными, при этом интенсивности обработки заявок на каналах различны и равны 0,6, 0,5, 0,4 соответственно, определим значение плотности потока заявок при которой необходимо подключать первых запасной канал и второй запасной канал.

Для нахождения значения плотности потока заявок при которой для того, чтобы система могла обеспечить бесперебойную работу с вероятностью 0,95 необходимо подключать первый запасной канал, воспользуемся формулой (6), (32):

$$\lambda \leq \frac{0,6}{19} \quad (33)$$

$$\lambda \leq 0,03158 \quad (34)$$

Получаем, что при значении $\lambda > 0,03158$, необходимо подключать запасной канал.

Подставив $\mu_0 = 0,6$, и $\mu_1 = 0,5$ в формулу (32), получим:

$$0,95\lambda^3 + 0,42\lambda^2 - 0,0275\lambda - 0,0165 \leq 0 \quad (35)$$

Найдем корни кубического уравнения методом Виета-Кардано и преобразуем уравнение (35):

$$(\lambda + 0,40908)(\lambda + 0,22322)(\lambda - 0,1902) \leq 0 \quad (36)$$

Решая неравенство методом интервалом, учитывая, что $\lambda > 0$:

$$0 < \lambda \leq 0,1902 \quad (37)$$

Получаем, что критическое значение плотности потока заявок при работе первого запасного канала более чем в 6 раз выше критического значения при работе основного канала. При $\lambda > 0,1902$ необходимо подключать второй запасной канал.

Таким образом, была выведена формула нахождения критических значений плотности потока заявок, при которых необходимо подключать запасные каналы передачи информации, что позволяет правильно реагировать при возникновении угрозы отказа системы в доступе легитимным пользователям.

В перспективе развития данной темы планируется найти вероятность отказа подсистемы защиты автоматизированной информационной системы специального назначения при работе всех запасных каналов, описать систему поддержки принятия решений при выборе канала для обработки очередной

заявки, построение имитационной модели подсистемы защиты и статистическое подтверждение значения вероятности отказа.

Литература

1. Венцель Е.С. Теория вероятностей. 2010. 628 с.

2. Матвеев В.Ф., Ушаков В.Г. Системы массового обслуживания. МГУ: 1984. 246 с.

3. Коценяк М.А., Кулешов И.А., Лаута О.С. Устойчивость информационно-телекоммуникационных сетей. СПб.: Политех, 2013. 92 с.

4. Боговик А.В., Игнатов В.В. Эффективность систем военной связи и методы ее оценки. СПб.: ВАС, 2006. 183 с.

5. Боговик А.В., Игнатов В.В. Теория управления в системах военного назначения. СПб.: ВАС, 2008. 460 с.

6. Леонов Д.В. Анализ проблем системы защиты информации защищаемой государством // Наука вчера, сегодня, завтра / Сб. ст. по материалам XLIV междунар. науч.-практ. конф. № 3. Новосибирск: АНС «СибАК», 2017. 85 с.

7. Леонов Д.В. Методика системного анализа системы защиты сведений охраняемых государством // Естественные и математические науки в современном мире / Сб. ст. по материалам LII междунар. науч.-практ. конф. № 3. Новосибирск: АНС «СибАК», 2017. 57 с.

8. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. Криптография: 1999. 123 с.

9. Banks J., Carson J., Nelson B., Nicol D. Discrete-event system simulation. New Jersey: Prentice Hall, 2000. 140 p.

10. Elliott M.R. Buyer’s guide simulation . IEE Solutions, 2000. 165 p.

11. Зотов А.И., Гриценко В.В. Надежностная модель частичного отказа в технической системе // Инженерный вестник Дона, 2019, №2. URL: ivdon.ru/ru/magazine/archive/n2y2019/5759.

12. Андрианов А.В., Зикий А.Н., Давтян А.Д. Генератор частотно-модулированных сигналов // Инженерный вестник Дона, 2019, №2. URL: ivdon.ru/ru/magazine/archive/n2y2019/5722.

References

1. Vencel' E.S. Teorija verojatnostej [Probability theory]. 2010. 628 p.

2. Matveev V.F., Ushakov V.G. Sistemy massovogo obsluzhivanija [Queuing systems]. MGU: 1984. 246 p.

3. Kocenjak M.A., Kuleshov I.A., Lauta O.S. Ustojchivost' informacionno-telekommunikacionnyh setej [Stability of information and telecommunication network]. SPb.: Politeh, 2013. 92 p.

4. Bogovik A.V., Ignatov V.V. Jeffektivnost' sistem voennoj svjazi i metody ee ocenki [The effectiveness of military communication systems and methods of its evaluation]. SPb.: VAS, 2006. 183 p.

5. Bogovik A.V., Ignatov V.V. Teorija upravlenija v sistemah voennogo naznachenija [Control Theory in Military Systems]. SPb.: VAS, 2008. 460 p.

6. Leonov D.V. Nauka vchera, segodnja, zavtra. Sb. st. po materialam XLIV mezhdunar. nauch.-prakt. konf. № 3. Novosibirsk: ANS «SibAK», 2017. 85 p.

7. Leonov D.V. Estestvennye i matematicheskie nauki v sovremennom mire. Sb. st. po materialam LII mezhdunar. nauch.-prakt. konf. № 3. Novosibirsk: ANS «SibAK», 2017. 57 p.

8. Nechaev V.I. Jelementy kriptografii. Osnovy teorii zashhity informacii [Elements of cryptography. Fundamentals of Information Security Theory]. Kriptografija: 1999. 123 p.

9. Banks J., Carson J., Nelson B., Nicol D. Discrete-event system simulation. New Jersey: Prentice Hall, 2000. 140 p.

10. Elliott M.R. Buyer’s guide simulation. IEE Solutions, 2000. 165 p.

11. Zotov A.I., Gricenko V.V. Inzenernyj vestnik Dona, 2019, №2. URL: ivdon.ru/ru/magazine/archive/n2y2019/5759.

12. Andrianov A.V., Zikij A.N., Davtjan A.D. Inzenernyj vestnik Dona, 2019, №2. URL: ivdon.ru/ru/magazine/archive/n2y2019/5722.