Способ оценки защищенности автоматизированной информационной системы специального назначения от DDoS-атак на основе теоретико-эмпирического подхода

О.В. Петрова, И.Д. Королев, Д.М. Крюков, В.Л. Колесников

Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М.Штеменко

Аннотация: Рассматривается модель, реализующая способ оценки защищенности автоматизированной информационной системы специального назначения, учитывающая в качестве эмпирической составляющей не только интенсивность нагрузки на систему, но и количество каналов как средство защиты информации от DDoS-атак на основе объединения двух подходов к оценке защищенности. Для построения модели применяется переход от теоретической модели с использованием эмпирических состояний и непрерывным временем к модели с дискретным временем. Использование предложенной модели оценки защищенности автоматизированной информационной системы специального назначения позволяет применять как эмпирические значения, полученные в результате измерений или моделирования, так и теоретическую базу для моделирования средств защиты информации в условиях воздействия DDoS-атак с учетом их характеристик, которые будут отражаться функцией дохода и выбором оптимального режима функционирования автоматизированной информационной системы специального назначения в дискретные моменты времени. При синтезе двух моделей был устранен недостаток статичности характера оценки защищенности автоматизированной информационной системы специального назначения, учтена интенсивность компьютерных атак типа DDoS, которая динамично меняет как параметры, оценивающие средства защиты, так и вероятности пребывания системы в критических состояниях.
Ключевые слова: автоматизированная система, моделирование, оценка защищенности, система массового обслуживания, вероятностная оценка, DDoS-атака.

Рассмотрим модель оценки защищенности автоматизированной информационной системы специального назначения (далее АИС СН) в условиях воздействия DDoS-атак, которая обладает основным защищенным каналом обработки заявок и одним (двумя) запасным [1,2]. Оценка защищенности вычисляется через показатели времени восстановления АИС СН после осуществления DDoS-атак. Модель оценки защищенности АИС СН от DDoS-атак с одним резервным каналом представлена графом состояний на рис. 1, где X_0 – свободны все каналы; X_1 – занят первый канал; X_2 – заняты оба канала.

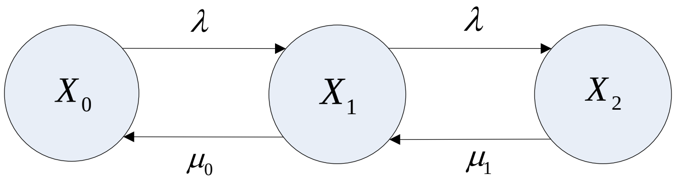

Рис. 1 – Модель оценки защищенности АИС СН с одним резервным каналом

Система алгебраических уравнений, описывающих вероятности пребывания системы в рассматриваемых состояниях для стационарного режима, имеет следующий вид [1, 3]:

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

где P_0 – вероятность пребывания системы в состоянии X_0, P_1 –в состоянии X_1, P_2 –в состоянии X_2, вычисляемые по формулам (1 – 3)[1, 3]:

$$P_0 = \frac{\mu_1\mu_0}{\mu_1\mu_0 + \mu_1\lambda + \lambda^2}, \quad (1)$$

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

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

Для оценки защищенности АИС СН с одни резервным каналом в дискретные моменты времени выделяются два основных уровня, представленных на рис. 2: защищенный уровень, соответствующий состоянию системы S_1={ X_0, X_1 }, незащищенный уровень S_2={ X_2 }, или же, S_1={ X_0 } и S_2={ X_1, X_2 }:

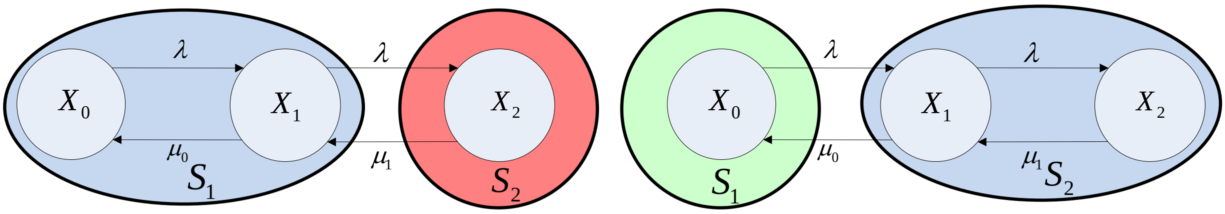

Рис. 2 – Процесс разбиения на состояния S_1 и S_2 модели оценки защищенности АИС СН с одним резервным каналом

Тогда в определенные моменты времени АИС СН может находиться в одном из двух состояний S_1 или S_2, которые формируют несовместные события, представленные на рис. 3:

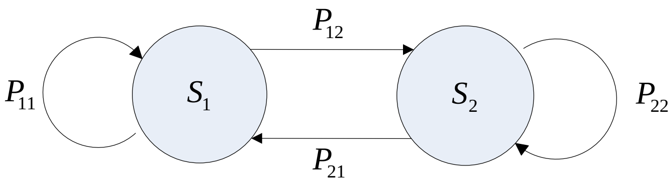

Рис. 3 – Модель оценки защищенности АИС СН с резервными каналами с проверкой в дискретные моменты времени

Для оценки защищенности АИС СН с резервными каналами с проверкой в дискретные моменты времени обозначим: через p_{11} – вероятность того, что система останется в состоянии S_1 (защищенном состоянии), p_{12} – вероятность того, что система из состояния S_1 перейдет в состояние S_2, p_{21} – вероятность того, что система перейдет из состояния S_2 в состояние S_1, а p_{22} – вероятность того, что система останется в состоянии S_2 (незащищенном состоянии).

Предположим, что в любой период времени, когда АИС СН находится в защищенном состоянии, мы получаем «доход» t_0 за счет того, что не будет затрат времени на восстановление и, следовательно, система будет это время работать, за период до очередной проверки. Под данным доходом будем понимать число, пропорциональное количеству времени с коэффициентом больше единицы между самими периодами проверки. В указанных предположениях, для данной системы рассмотрим два случая:

1. $\mu_0 \rangle\rangle \mu_1$. При этом восстановление занимает t_1 часов, $t_{0>t1}$. В этом случае существует две альтернативы: первая S_1={ X_0, X_1 } и S_2={ X_2 }, тогда $p_{11} = P_0 + P_1$, $p_{12} = P_2$; вторая S_1={ X_0 } и S_2={ X_1, X_2 }, где $p_{22} = P_1 + P_2$, $p_{21} = P_0$.

$\mu_0 \langle\langle \mu_1$. При этом восстановление занимает t_2 часов, $t_0>t_2\geq t_1$. В этом случае, также существует две альтернативы: первая S_1={ X_0 } и S_2={ X_1, X_2 }, тогда $p_{11} = P_0$, $p_{12} = (1 - p_{11}) = P_1 + P_2$; вторая S_1={ X_0, X_1 } и S_2={ X_2 }, тогда $p_{22} = P_2$, $P_2 = (1 - p_{22}) = P_0 + P_1$.

Таким образом, существуют два состояния, 1 и 2, и два решения, зависящие от значения μ_0 и μ_1 с разными временными показателями восстановления системы – значениями дохода в случае перехода ее в незащищенное состояние. Матрицы данной модели представлены далее:

$$P(f) = \begin{bmatrix} p_{11} & 1 - p_{11} \\ 1 - p_{22} & p_{22} \end{bmatrix} = \begin{bmatrix} P_0 + P_1 & P_2 \\ P_0 & P_1 + P_2 \end{bmatrix}, r(f) = \begin{bmatrix} t_0 \\ -t_1 \end{bmatrix};$$

$$P(g) = \begin{bmatrix} p_{11} & 1 - p_{11} \\ 1 - p_{22} & p_{22} \end{bmatrix} = \begin{bmatrix} P_0 & P_1 + P_2 \\ P_0 + P_1 & P_2 \end{bmatrix}, r(g) = \begin{bmatrix} t_0 \\ -t_2 \end{bmatrix},$$

где $P(f)$ – матрица вероятностей перехода системы в состояния S_1 и S_2 для случая, когда $\mu_0 \rangle\rangle \mu_1$; $P(g)$ – матрица вероятностей перехода системы в состояния S_1 и S_2 для случая, когда $\mu_0 \langle\langle \mu_1$; $r(f)$ – вектор временных показателей дохода системы при переходе из состояний S_1 и S_2 при $\mu_0 \rangle\rangle \mu_1$; $r(g)$ – вектор временных показателей на восстановления системы из состояний S_1 и S_2 при $\mu_0 \langle\langle \mu_1$.

Модели оценки защищенности АИС СН при массированном воздействии DDoS-атак с двумя резервными каналами соответствует граф состояний, представленный на рис. 4 [2]:

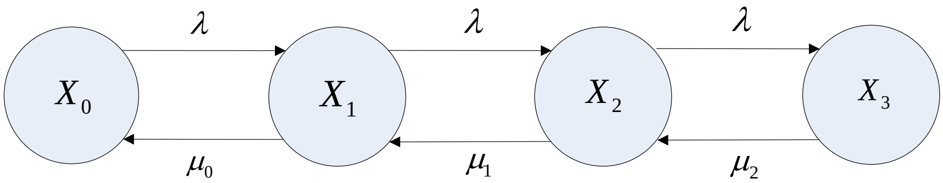

Рис. 4 – Модель оценки защищенности АИС СН с двумя резервными каналами

Модель, представленная на рисунке 4, учитывает следующее допущение – все каналы в системе включаются и освобождаются последовательно. Тогда определим состояния системы: X_0 – свободны все каналы; X_1 – занят первый (основной) канал; X_2 заняты первые 2 канала (основной и первый резервный); X_3 – заняты все 3 канала (основной и два резервных) [2].

Система алгебраических уравнений, описывающая вероятности нахождения данной АИС СН в рассматриваемых состояниях для стационарного режима функционирования имеет следующий вид [2, 3]:

$$\begin{cases} 0 = -P_0\lambda + P_1\mu_0, \\ 0 = -P_1(\lambda + \mu_0) + P_2\mu_1 + P_0\lambda, \\ 0 = -P_2(\lambda + \mu_1) + P_1\lambda + P_3\mu_2, \\ 0 = -P_3\mu_2 + P_2\lambda, \\ \sum_{k=0}^{3} P_k = 1, \end{cases}$$

где P_0 – вероятность нахождения системы в состоянии X_0; P_1 – вероятность пребывания системы в состоянии X_1; P_2 – вероятность пребывания системы в состоянии X_2; P_3 – вероятность пребывания системы в состоянии X_3, которые вычисляем по формулам (4 – 7) [2, 3];

$$P_0 = \frac{\mu_0\mu_1\mu_2}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}, \qquad (4)$$

$$P_1 = \frac{\lambda\mu_1\mu_2}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}, \qquad (5)$$

$$P_2 = \frac{\lambda^2\mu_2}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}, \quad (6)$$

$$P_3 = \frac{\lambda^3}{\mu_0\mu_1\mu_2 + \lambda\mu_1\mu_2 + \lambda^2\mu_2 + \lambda^3}. \quad (7)$$

Для оценки защищенности АИС СН с двумя резервными каналами в дискретные моменты времени также выделяются два основных уровня: защищенный уровень, соответствующий состоянию системы S_1={ X_0, X_1, X_2 } и незащищенный уровень S_2={ X_3 }, или же S_1={ X_0 } и S_2={ X_1, X_2, X_3 }. Тогда в определенные моменты времени АИС СН может находиться в одном из двух состояний S_1 или S_2. (см. рис. 3).

Для оценки защищенности АИС СН с двумя резервными каналами с проверкой в дискретные моменты времени обозначим: p_{11} – вероятность того, что система останется в состоянии S_1 (защищенном состоянии), p_{12} – вероятность того, что система из состояния S_1 перейдет в состояние S_2, p_{21}– вероятность того, что система перейдет из состояния S_2 в состояние S_1, и p_{22} – вероятность того, что система останется в состоянии S_2 (незащищенном состоянии).

Предположим, что аналогично модели оценки защищенности АИС СН с одним резервным каналом, в любой момент времени, когда система находится в защищенном состоянии, будем считать, что получаем «доход» t_0 за период между проверками [4-6]. В указанных предположениях, для данной системы рассмотрим два случая:

1. $\mu_1 \rangle\rangle \mu_2$. При этом восстановление системы будет занимать t_1 часов, t_0>t_1. В этом случае первая альтернатива состоит в том, что S_1={ X_0, X_1, X_2 } и S_2={ X_3 }, тогда $p_{11} = P_0 + P_1 + P_2$, $p_{12} = (1 - p_{11})$; вторая альтернатива состоит в том, что S_1={ X_0 }, а S_2={ X_1, X_2, X_3 }, тогда $p_{22} = P_1 + P_2 + P_3$, $p_{21} = (1 - p_{22})$.

2. $\mu_1 \langle\langle \mu_2$. При этом восстановление занимает t_2 часов, $t_0 > t_2 \geq t_1$. В этом случае первая альтернатива состоит в том, что $S_1=\{X_0\}$, а $S_2=\{X_1, X_2, X_3\}$, тогда $p_{11} = P_0$, $p_{12} = (1-p_{11})$; а вторая $S_1=\{X_0, X_1, X_2\}$ и $S_2=\{X_3\}$, $p_{22} = P_3$, $p_{21} = (1-p_{22})$.

Таким образом, существуют два состояния, 1 и 2, и два решения, зависящие от значения μ_1 и μ_2 с разными временными показателями восстановления системы в случае перехода ее в незащищенное состояние [7, 8]. Матрицы для данной модели представлены ниже:

$$P(f) = \begin{bmatrix} p_{11} & 1-p_{11} \\ 1-p_{22} & p_{22} \end{bmatrix} = \begin{bmatrix} P_0 + P_1 + P_2 & P_3 \\ P_0 & P_1 + P_2 + P_3 \end{bmatrix}, r(f) = \begin{bmatrix} t_0 \\ -t_1 \end{bmatrix};$$

$$P(g) = \begin{bmatrix} p_{11} & 1-p_{11} \\ 1-p_{22} & p_{22} \end{bmatrix} = \begin{bmatrix} P_0 & P_1 + P_2 + P_3 \\ 1-P_3 & P_3 \end{bmatrix}, r(g) = \begin{bmatrix} t_0 \\ -t_2 \end{bmatrix},$$

где $P(f)$ – матрица вероятностей перехода системы в состояния S_1 и S_2 для случая, когда $\mu_1 \rangle\rangle \mu_2$; $P(g)$ – матрица вероятностей перехода системы в состояния S_1 и S_2 для случая, когда $\mu_1 \langle\langle \mu_2$; $r(f)$ – вектор временных показателей дохода системы при переходе из состояний S_1 и S_2, при $\mu_1 \rangle\rangle \mu_2$; $r(g)$ – вектор временных показателей восстановления системы – времени перехода из состояний S_1 и S_2 при $\mu_1 \langle\langle \mu_2$. Таким образом, средний доход, при различных альтернативных возможностях пребывания системы – *j*, можно рассчитать по формуле (8), с учетом формирования стратегий *i*:

$$r_i^k = \sum_{j=1}^{2} p_{ij}^k r_{ij}^k, \tag{8}$$

где r_{ij}^k – координаты вектора временных показателей на восстановления системы при переходе из состояния S_1 и S_2 [4, 9, 10]. Рассмотрим пример оценки защищенности АИС СН с одним резервным каналом каналом с проверкой в дискретные моменты времени. Исходные данные для расчета характеристик представлены в таблице № 1.

Таблица № 1

Оценка защищенности АИС СН при работе основного и первого резервного каналов обработки заявок

Оценка защищенности	Интенсивность входящего потока	Интенсивность обработки		P_0	P_1	P_2
		1–й канал	2–й канал			
Низкая	0.3	0.45	0.15	0,333	0,222	0,445
Низкая	0.3	0.35	0.45	0,412	0,353	0,235

Интенсивность входящего потока λ=0,3, интенсивность обработки заявки системой на основном канале μ_1=0,45 и μ_2=0,15. Допустим, что в этих условиях, если система останется в состоянии S_1 система проработает промежуток времени t_0=60 минут, а если перейдет в состояние S_2, то потребуется ее восстановление с временными затратами равными t_1=45 минут. Рассчитаем значение вероятностей нахождения системы в состояниях X_0, X_1, X_2 в соответствии с (1 – 3).

Используя предложенную модель, с учетом того, что $\mu_0 \rangle\rangle \mu_1$, получаем следующие значения вероятностей: $p_{11}=P_0+P_1$=0,333, а в состоянии $p_{22}=P_1+P_2$=0,667. Тогда матрицы данной системы будут иметь вид:

$$P(f)=\begin{bmatrix} 0.555 & 0.445 \\ 0.333 & 0.667 \end{bmatrix}, r(f)=\begin{bmatrix} 60 \\ -45 \end{bmatrix}.$$

Если интенсивность обработки заявки системой на основном канале μ_1=0,35 и μ_2=0,45, и, система останется в состоянии S_1, то система гарантированно не откажет в течение времени t_0=50 минут, а если перейдет в состояние S_2, то потребуется ее восстановление с временными затратами равными t_0=15 минут. Тогда, в соответствии с (1 – 3):

$$P_0=\frac{0,35\cdot 0,45}{0,35\cdot 0,45+0,45\cdot 0,3+0,3^2}\approx 0,412;$$

$$P_1 = \frac{0,45 \cdot 0,3}{0,35 \cdot 0,45 + 0,45 \cdot 0,3 + 0,3^2} \approx 0,353;$$

$$P_2 = \frac{0,3^2}{0,35 \cdot 0,45 + 0,45 \cdot 0,3 + 0,3^2} \approx 0,235,$$

с учетом того, что $\mu_0 \langle\langle \mu_1$, получаем следующие значения вероятностей: p_{11}=P_0=0,412, а в состоянии p_{22}=P_2=0,235. Тогда матрицы данной системы будут иметь вид:

$$P(g) = \begin{bmatrix} 0.412 & 0.588 \\ 0.765 & 0.235 \end{bmatrix}, r(g) = \begin{bmatrix} 60 \\ -15 \end{bmatrix}.$$

Пример расчета представлен в таблице № 2.

Таблица № 2

Средний доход системы при различных альтернативных возможностях с учетом формирования стратегий

i	j	p_{i1}^k	p_{i2}^k	r_{i1}^k	r_{i2}^k	$r_i^k = \sum_{j=1}^{2} p_{ij}^k r_{ij}^k$
1	1 2	0,45	0,15	60	-45	20,25
2	1	0,35	0,45	50	-15	10,825

Вывод: использование предложенной модели оценки защищенности АИС СН позволяет применять как эмпирические значения, полученные в результате измерений или моделирования, так и теоретическую базу для моделирования средств защиты информации в условиях воздействия DDoS-атак с учетом их характеристик, которые будут отражаться функцией дохода и выбором оптимального режима функционирования АИС СН в дискретные моменты времени.

При синтезе двух моделей был устранен недостаток статичности характера оценки защищенности АИС СН, учтена интенсивность компьютерных атак типа DDoS, которая динамично меняет как параметры, оценивающие средства защиты, так и вероятности пребывания системы в критических состояниях.

Литература

1. Королев И.Д., Петрова О.В., Овчаренко И.О. Моделирование системы защиты многоканальных автоматизированных комплексов // Вестник Российского нового университета. 2019. С. 3-10.

2. Королев И.Д., Петрова О.В., Овчаренко И.О. Модель системы защиты многоканальных автоматизированных комплексов от DDoS–атак с учетом освобождения по мере обработки каналов // Инженерный вестник Дона, 2019, № 7. URL:ivdon.ru/ru/magazine/archive/N7y2019/6080.

3. Вентцель Е.С., Овчаров Л.А. Теория вероятностей. 5-е изд. М.: ЮСТИЦИЯ, 2018. С. 596–628.

4. Майн Х., Осаки С. Марковские процессы принятия решений, под редакцией Бусленко Н.П. М.: Главная редакция физико-математической литературы издательства «Наука», 1977. 176 с.

5. Суханов А.И., Оценки защищенности информационных систем // Журнал научных публикаций аспирантов и докторантов, 2008. URL: jurnal.org/articles/2008/inf33.html (дата обращения: 09.03.2020).

6. Mine, H. and Sh. Osaki, 1970. Markovian Decision Processes. New York: American Elsevier Publishing Company Inc.

7. Privault, N., 2018. Understanding Marcov Chains. Examples and Applications. Springer.

8. Cobb, G.W., 2018. What is Markov Chain Monte Carlo and why it Matters. MCMC.

9. Metcalfe, A., D. Green, T. Greenfield and M. Mansor, 2019. Statistics in Engineering. CRC Press.

10. Xin-She Yang and Xing-Shi He, 2019. Mathematical Foundations of NatureInspired Algorithms. Springer.

References

1. Korolev I.D., Petrova O.V., Ovcharenko I.O., Vestnik Rossiyskogo novogo universiteta. 2019.

2. Korolev I.D., Petrova O.V., Ovcharenko I.O., Inzhenernyj vestnik Dona (Rus), 2019, № 7 URL: ivdon.ru/ru/magazine/archive/N7y2019/6080.

3. Venttsel' YE.S., Ovcharov L.A. Teoriya veroyatnostey. Moscow: YUSTITSIYA, 2018. p. 596–628.

4. Mayn KH., Osaki S. Markovskiye protsessy prinyatiya resheniy [Markovian decision processes], pod redaktsiyey Buslenko N.P. M.: Glavnaya redaktsiya fiziko-matematicheskoy literatury izdatel'stva «NaukA», 1977. 176 p.

5. Sukhanov A.I., Zhurnal nauchnykh publikatsiy aspirantov i doktorantov, 2008. URL: jurnal.org/articles/2008/inf33.html

6. Mine, H. and Sh. Osaki, 1970. Markovian Decision Processes. New York: American Elsevier Publishing Company Inc.

7. Privault, N., 2018. Understanding Marcov Chains. Examples and Applications. Springer.

8. Cobb, G.W., 2018. What is Markov Chain Monte Carlo and why it Matters. MCMC.

9. Metcalfe, A., D. Green, T. Greenfield and M. Mansor, 2019. Statistics in Engineering. CRC Press.

10. Xin-She Yang and Xing-Shi He, 2019. Mathematical Foundations of NatureInspired Algorithms. Springer.