УДК 343.985 DOI: 10.26102/2310-6018/2020.31.4.020

Статистический алгоритм обнаружения угроз компьютерной безопасности

И.В. Милосердов, В.А. Малышев
Санкт-Петербургский институт информатики и автоматизации Российской академии наук,
Санкт-Петербург, Российская Федерация

Аннотация: Рассматривается задача синтеза статистического алгоритма, построенного в подклассе дискретно-непрерывных случайных процессов предназначенного для прогнозирования и обнаружения начала DDos атаки по анализу изменений интенсивности принимаемого трафика. Для анализа и выявления угроз безопасности компьютерных сетей существуют системы мониторинга, ориентированные на анализ трафика, пакетов и протоколов. Все эти системы являются уязвимыми. Атаке подлежат практически все уровни модели OSI объекта, под которым понимается какого либо типа сервера или выбранные приложения, но первым признаком начинающейся атаки является аномальное поведение входного трафика. К перспективным методам обеспечения безопасности КС можно отнести методы, основанные на выявлении отклонений по изменениям вероятностных параметров данных. Их суть заключается в определении изменений статистических характеристик потоков данных. Разработанный алгоритм позволяет не только обнаружить угрозу безопасности сети, но и прогнозировать возможности начала DDos атаки, удобен для применения на нижних уровнях модели OSI, например, для обнаружения интенсивности трафика и его отклонений Информация, выдаваемая разработанным алгоритмом, носит вероятностный характер, поэтому, она может быть комплексироваться с результатами получаемыми другими методами обнаружения угроз безопасности компьютерной сети.

Ключевые слова: компьютерная сеть, угроза безопасности, дискретно-непрерывные случайные процессы, мониторинг безопасности, рекуррентный алгоритм

Для цитирования: Милосердов И.В., Малышев В.А. Статистический алгоритм обнаружения угроз компьютерной безопасности. *Моделирование, оптимизация и информационные технологии.* 2020;8(4). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=866 DOI: 10.26102/2310-6018/2020.31.4.020

Statistical algorithm for detecting computer security threats

I.V. Miloserdov, V.A. Malyshev
St. Petersburg Institute of Informatics and Automation of the Russian Academy of Sciences, Saint Petersburg, Russian Federation

Abstract: The problem of synthesis of a statistical algorithm constructed in a subclass of discrete-continuous random processes designed to predict and detect the beginning of a DDos attack by analyzing changes in the intensity of received traffic is considered. To analyze and identify threats to the security of computer networks, there are monitoring systems that focus on analyzing traffic, packets, and protocols. All of these systems are vulnerable. Almost all levels of the object's OSI model, which is defined as any type of server or selected applications, are subject to attack, but the first sign of an attack is abnormal behavior of input traffic. Promising techniques to ensure safety of the COP include methods based on the detection of the deviation by the change of probabilistic data parameters. Their essence is to determine changes in the statistical characteristics of data flows. The developed algorithm allows not only detecting a network security threat, but also.

Keywords: computer network, security threat, discrete-continuous random processes, security monitoring, recurrent algorithm

Для цитирования: Miloserdov I.V., Malyshev V.A. Statistical algorithm for detecting computer security threats. *Modeling, optimization and information technology.* 2020;8(4). Available from: https://moitvivt.ru/ru/journal/pdf?id=866 DOI: 10.26102/2310-6018/2020.31.4.020 (In Russ).

Введение

Современные компьютерные сети (КС) становятся неотъемлемой частью деятельности человека практически во всех сферах жизни. Развиваются и повсеместно внедряются существующие варианты КС. В ближайшее время ожидается интенсивное внедрение концепции КС «физических предметов», оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой, называемых технологией IoT. Рассматривается организация таких сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека.

Вместе с тем, неуклонно растет количество угроз безопасности КС (БКС), увеличивается количество киберпреступлений. По заявлениям ведущих компаний, работающих в сфере компьютерной безопасности, общее количество распределенных атак, направленных на отказ в обслуживании (Distributed Denial of Service (DDos)), за 2019 год выросло примерно в полтора раза. Рост рынка IoT означает, что злоумышленники при желании могут эксплуатировать уязвимые устройства. Нарушения функционирования КС вызванное деструктивными воздействиями, как показывает анализ, приводит к значительному материальному ущербу и эта тенденция, в настоящее время, только усиливается. Особенно опасный характер приобретают распределенные атаки, направленные на отказ в обслуживании, которым в настоящее время свойственно большое разнообразие.

Для анализа и выявления угроз БКС существуют системы мониторинга, ориентированные на анализ трафика, пакетов и протоколов. Все эти системы являются уязвимыми. В настоящее время, к наиболее популярным методам обнаружения деструктивных воздействий на КС, можно отнести методы, в основе которых лежит количественный анализ возрастающей при атаке сетевой нагрузки [1-9]. В этих методах используется анализ соотношения принятых и отправленных пакетов; учет количества пакетов, их тип и количество запросов [1]; учет количества пакетов из различных подсетей [2, 3]; группировка входящих запросов по подсетям и их сравнение [4, 5]; учет количества скачков трафика до подсетей для фильтрации пакетов с ложным адресом отправителя [6]; разделение проходящего трафика на потоки на основе величины «поражающего воздействия» [7]; проверка легитимности трафика по протоколам соответствующих уровней модели OSI: TCP, ICMP, UDP [8, 9].

К перспективным методам обеспечения безопасности КС можно отнести методы, основанные на выявлении отклонений по изменениям вероятностных параметров данных. Их суть заключается в определении изменений статистических характеристик потоков данных [8, 10, 11].

Недостатком перечисленных методов мониторинга является их нацеленность на мощные атаки, в то время как их чувствительность к атакам средней и малой мощности недостаточно высокая [12]. Кроме того, разработанные методы не предусматривают возможностей обеспечения БКС в целом и комплексирования всей имеющейся информации.

В условиях высокой неопределенности и разнообразия угроз, возможных рисков для своевременного обнаружения и предотвращения деструктивных воздействий на КС необходимо наличие эффективных средств и методов мониторинга состояния сетей, позволяющего обеспечить их защиту. В связи с этим, разработка новых методов мониторинга и своевременного обнаружения производимых атак на КС является достаточно актуальной задачей.

Целью работы является разработка единой модели мониторинга БКС, критерием эффективности для которой является максимум апостериорной плотности вероятности распределенных атак, направленных на отказ в обслуживании.

Синтез алгоритма мониторинга безопасности компьютерной сети

Распределенные атаки, направленные на отказ в обслуживании сетей, действуют практически на всех уровнях модели OSI взаимодействия открытых систем. На уровне «Прикладной» модели OSI воздействию подвергаются протоколы FTP, HTTP, POP3, SMTP и шлюзы, которые их используют; на «Представительском» уровне Протоколы сжатия и кодирования данных (ASCII, EBCDIC); на «Сеансовом» протоколы входа/выхода (RPC, PAP); на «Транспортном» протоколы TCP, UDP; на «Сетевом» протоколы IP, ICMP, ARP, RIP и роутеры, которые их используют; на «Канальном» уровне Протоколы 802.3, 802.5, а также контроллеры, точки доступа и мосты, которые их используют; на «Физическом» протоколы 100BaseT, 1000 Base-X, а также концентраторы, розетки и патч-панели, которые их используют. В связи с этим, для мониторинга ВС на предмет атак необходим совместный мониторинг протоколов и пакетов, передающихся между узлами сети, а также интенсивности проходящего трафика и его изменений. На Рисунке 1 показана блок-схема системы мониторинга КС совместно с системой управления БКС. КС представлена в виде сетевых и оконечных устройств представленных категорией «Объекты» и связей между ними.

В качестве объектов мониторинга выбраны сетевые категории, отражающие анализ трафика, протоколов и пакетов, и обобщенные категории объектов сети, отражающие их состояния – подверженность вредоносным воздействиям имеющегося на них программного обеспечения. Особенностью модели мониторинга является наличие системы оценки и прогноза состояния КС. По данным поступающим с системы наблюдения и анализа в этом блоке строится модель обработки информации системы мониторинга, статистического прогноза и предупреждения об имеющихся угрозах БКС.

Для построения модели предупреждения об угрозах БКС необходимо построить динамические модели или сценарии развития атак, проводимых на узлы сети. Такие параметрические модели, в виде стохастических разностных уравнений можно построить методами статистической обработки трафика поступающего на объекты ВС. Сценариев развития атаки на КС, в общем случае может быть несколько, но для простоты описания метода синтеза выберем один сценарий стационарной сети и один сценарий атаки. Динамика параметров сети в стационарных условиях (отсутствии а Если в момент времени t_k сеть подвергнута атаке, то считаем ее состояние s_k=2, а вектор непрерывнозначных параметров представляет собой сумму параметров КС в стационарном состоянии и параметров помех $x_k^{(1)} + x_k^{(2)}$.

так), описывается дискретным состоянием сети s_k=1 к моменту времени t_k (t_{k+1} = $t_k+\Delta t; k = \overline{0, K}$), при этом вектор $x_k^{(1)}$ описывает непрерывнозначные параметры сети.

Рисунок 1 – Модель системы мониторинга и управления безопасной компьютерной сетью
Figure 1 – Model of a secure computer network monitoring and management system

Тогда наблюдаемый в сети процесс может быть задан векторным уравнением вида:

$$z_k = \overline{C}(s_k)\bar{x}_k + n_k, \quad \overline{C}^T(s_k) = \begin{bmatrix} 1 \\ \lambda_k \end{bmatrix}, \quad \bar{x}_k = \begin{bmatrix} x_k^{(1)} \\ x_k^{(2)} \end{bmatrix}; \qquad (1)$$

где λ_k – случайный параметр равный 1 если сеть в момент времени t_k подвержена атаке (s_k=2) и 0 если атак на ВС нет; n_k – дискретная последовательность случайных величин определяющих точность наблюдаемых (вычисляемых) параметров.

Считаем, что начальное распределение вектора $\hat{\bar{x}}_0$ является гауссовым с известной матрицей ковариации $\hat{\mathrm{R}}_0$.

Для простоты можно принять, что n_k имеет нормальное распределение, нулевое математическое ожидание и дисперсию Q.

Считаем, что модели сетевой динамики заданы в виде стохастических разностных уравнений вида:

$$\bar{x}_{k+1} = A(s_{k+1}, s_k)\bar{x}_k + \xi_k; \quad \boldsymbol{\xi}_k^{\,T} = \begin{bmatrix} \xi_k^{(1)} & \xi_k^{(2)} \end{bmatrix}; \quad A(s_{k+1}, s_k) = \begin{bmatrix} \alpha_k^{(1)} & 0 \\ 0 & \alpha_k^{(2)} \end{bmatrix}; \qquad (2)$$

где $A(s_{k+1}, s_k)$ – переходная матрица, описывающая динамику стационарного состояния сети с помощью коэффициента $\alpha_k^{(1)}$ и динамику атаки с помощью коэффициента $\alpha_k^{(2)}$; ξ_k - последовательности не зависимых формирующих гауссовых величин, с нулевым средним и матрицей ковариаций G_k.

Считаем, что начальное распределение вектора $\hat{\bar{x}}_0$ является гауссовым с известной матрицей ковариации $\hat{\mathrm{R}}_0$.

Наличие или отсутствие атаки в рассматриваемой модели определяется коэффициентом λ_k ($k = \overline{0, K}$). Априорные сведения об этом коэффициенте определяются возможностью атаки и ее продолжительностью. Считая, что переходы могут быть описаны Пуассоновскими потоками, априорные сведения о дискретной последовательности s_k задаются начальным распределением состояний $P_0(s_0 = 1)$, $P_0(s_0 = 2)$ и вероятностями переходов между состояниями. Переход из состояния $s_k = 1$ в состояние $s_k = 2$ определяется интенсивностью ν_{12}, а возвращение к стационарному режиму интенсивностью ν_{21}. Поэтому можно принять, что вероятность перехода на каждом дискете времени k:

$$q_{12} = \nu_{12}\Delta t; q_{21} = \nu_{21}\Delta t. \quad (3)$$

Таким образом, задача синтеза рекуррентного алгоритма обнаружения атаки на КС, по критерию максимальной вероятности может быть сформулирована следующим образом.

Имеется уравнение наблюдений (1), динамика рекуррентных последовательностей задана выражением (2). Заданы начальные распределения вектора $\bar{x}_o$ и случайной величины λ_0. Заданы априорные вероятности переходов между состояниями системы. Требуется по поступающим измерениям (1) определить оценку состояния КС по критерию максимума апостериорной плотности вероятности.

Вывод алгоритма приводится в [13], сам алгоритм состоит из априорной и апостериорной частей и блока начальных условий.

Блок прогноза, для рассматриваемых начальных условий:

$$\tilde{P}_{k+1}^{(j)} = q_{ij}\hat{P}_k^{(i)} + (1 - q_{ji})\hat{P}_k^{(i)}; \quad (4)$$

$$\tilde{\bar{x}}_{k+1}^{(i)} = \hat{x}_k^{(i)} + \left(\tilde{P}_{k+1}^{(i)}\right)^{-1}\tilde{P}_{k+1}^{(j)}\left(\hat{x}_k^{(i)} - \hat{x}_k^{(j)}\right); \quad (5)$$

$$\tilde{R}_{k+1}^{(i)} = \hat{R}_k^{(i)} + \left(\tilde{P}_k^{(i)}\right)^{-1}\tilde{P}_k^{(j)}\left[\hat{R}_k^{(i)} - \hat{R}_k^{(j)} + \left(\hat{x}_k^{(i)} - \hat{x}_k^{(j)}\right)^2\right]; \quad (6)$$

где $(i, j) = \overline{1,2}$; $(i \neq j)$; $\tilde{x}_{k+1}$, $\tilde{R}_{k+1}$ – вектор априорных оценок параметров сети и его ковариационная матрица предсказанные на момент времени t_{k+1}; $\tilde{P}_{k+1}^{(i)}$ - скалярная оценка априорной вероятности состояния $s_{k+1} = i$; $\hat{x}_k$, $\hat{R}_k$, $\hat{P}_k^{(i)}$ - апостериорные оценки соответствующих параметров, полученные на текущий момент времени.

Апостериорная часть:

$$h_k^{(1)} = \left(\tilde{R}_k^{(1)} + Q\right)^{-0.5}\exp\left(-0.5\left(z_k - \tilde{x}_k^{(1)}\right)^2\left(\tilde{R}_k^{(1)} + Q\right)^{-1}\right); \quad (7)$$

$$h_k^{(2)} = \left(\tilde{R}_k^{(1)} + \tilde{R}_k^{(2)} + Q\right)^{-0.5} \exp\left(-0.5\left(z_k - \tilde{x}_k^{(1)} - \tilde{x}_k^{(2)}\right)^2 \left(\tilde{R}_k^{(1)} + \tilde{R}_k^{(2)} + Q\right)^{-1}\right); \quad (8)$$

$$\hat{P}_k^{(i)} = \frac{\tilde{P}_k^{(i)} h_k^{(i)}}{\sum_{j=1}^{2} \tilde{P}_k^{(j)} h_k^{(j)}}; \quad (9)$$

$$\hat{x}_k^{(1)} = \tilde{x}_k^{(1)} + \tilde{R}_k^{(1)}\left(\tilde{R}_k^{(1)} + Q\right)^{-1}(z_k - \tilde{x}_k^{(1)}); \quad (10)$$

$$\hat{x}_k^{(2)} = \tilde{x}_k^{(2)} + \tilde{R}_k^{(2)}\left(\tilde{R}_k^{(1)} + \tilde{R}_k^{(2)} + Q\right)^{-1}(z_k - \tilde{x}_k^{(1)} - \tilde{x}_k^{(2)}). \quad (11)$$

Алгоритм (4) – (11) удобен для применения на нижних уровнях модели OSI, например, для обнаружения интенсивности трафика и его отклонений. Но если информация об атаках поступает с верхних уровней модели OSI в статистически обработанном виде, возможно полное комплексирование этой информации на основе байесовского правила. При этом, уравнение (9) приводится к виду:

$$\hat{P}_k^{(i)} = \frac{\tilde{P}_k^{(i)} h_k^{(i)} \pi_k^{(i)}}{\sum_{j=1}^{2} \tilde{P}_k^{(j)} h_k^{(j)} \pi_k^{(j)}}, \quad (12)$$

где $\pi_k^{(i)}$ – вероятность того, что сеть находится в состоянии $s_{k+1} = i$ поступившая с верхних уровней модели и полученная другими методами.

Результаты

Обнаружение воздействий на КС по изменениям трафика было проведено по рассмотренному алгоритму при следующих начальных условиях: $\Delta t = 10$ с, $K=10^3$, $x_0^{(1)} = 7.8$ Мбит, $\hat{x}_0^{(2)} = 10$ Мбит, $\hat{R}_0^{(1)} = 25$ Мбит^2, $\hat{R}_0^{(2)} = 50$ Мбит^2, $Q = 10^2$ Мбит^2, $G=100$ Мбит^2, $\lambda_0 = 0$, $\hat{P}_0^{(1)} = 1$, $\hat{P}_0^{(2)} = 0$.

На Рисунке 2 показаны нормированные значения интенсивности трафика $c1_i$ (непрерывная линия) и его изменений $n1_i$ (пунктирная линия) без воздействия атаки и после ее воздействия.

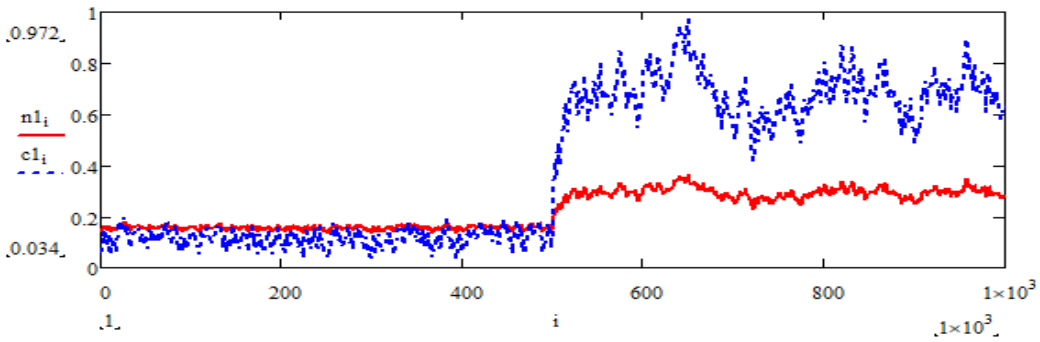

Рисунок 2 – Нормированные к единице графики интенсивности трафика и его изменений в стационарном состоянии и при DDos атаке

Figure 2 – Normalized to one graph of traffic intensity and its changes in the stationary state and during a DDos attack

По приведенному алгоритму (4) – (11) проводилось обнаружение атаки. На Рисунке 3 показана вероятность обнаружения угрозы деструктивного вмешательства $P2_i$.

Из Рисунка видно, что вероятность обнаружения увеличивается в рассматриваемых условиях до уровня 0.5 за несколько шагов. Следует отметить, что синтезированный алгоритм работает в условиях, когда интенсивность трафика не меняется, но меняются его статистические параметры, такие как ковариационная матрица. Интенсивность переходов между состояниями, может регулироваться системой управления БКС.

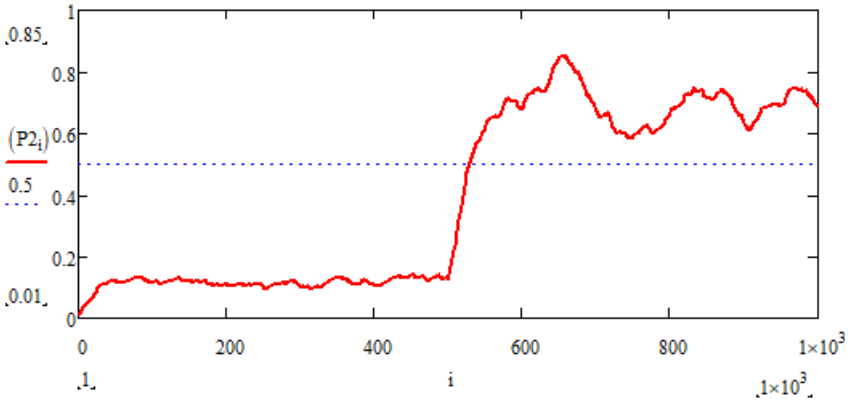

Рисунок 3 – Оценка апостериорной вероятности обнаружения атаки
Figure 3 – Estimation of the posteriori probability of detecting an attack

Выводы

В настоящее время отсутствуют универсальные и гарантированные методы обеспечения БКС. Количество атак на КС и несанкционированных взломов сайтов и платежных систем с каждым годом увеличивается, и по прогнозам специалистов эта тенденция будет только усиливаться. Задача поиска новых методов обеспечения БКС является достаточно актуальной.

Предложен новый метод синтеза алгоритма мониторинга КС позволяющий обнаруживать и предупреждать о сетевых угрозах. В основе метода синтеза лежит теория оптимальной фильтрации дискретно-непрерывных случайных процессов. Метод позволяет по интенсивности проходящего трафика и его изменениям определять вероятность атак, направленных на отказ в обслуживании. Кроме того, синтезированный алгоритм позволяет в текущем времени проводить комплексирование информации, поступающей от измерителей, работающих на других принципах, если эта информация прошла статистическую обработку. Комплексирование измерителей, работающих на различных принципах и уровнях модели OSI может дать качественный скачек в задаче мониторинга КС с целью обеспечения ее безопасности.

Рассмотрен пример применения алгоритма обнаружения угроз БКС на модели имитирующей появление атаки, направленной на отказ системы в обслуживании.

Следует отметить, что для более точной настройки алгоритма необходима его апробация на реальной КС и наличие набора статистических данных по применявшимся DDos атакам.

ЛИТЕРАТУРА

1. Cabrera, J.B.D. *Proactive detection of distributed denial of service attacks using mib traffic variables – a feasibility study* I J.B.D. Cabrera, L. Lewis, X. Qin et al. II Proc.of International Symposium on Integrated Network Management. Seattle, 14–18 May. 2001. Piscataway: IEEE, 2001:609– 622.

2. Ioannidis, J. *Implementing Pushback: Router-Based Defense Against DDoS Attacks* I J. loannidis, S.M. Bellovin II Proc. of Symposium of Network and Distributed Systems Security (NDSS). San Diego, 6-8 February. 2002: 57-71.
3. Manajan, R. *Controlling High Bandwidth Aggregates in the Network* : ICSI Technical Report I R. Manajan, S.M. Bellovin, S. Floyd et al. - ICSI, 2001: 16.
4. CoIIins, M. An *Empirical Analysis of Target-Resident DoS Filters* I M. Collins, M.K. Reiter If Proc. of 2004 IEEE Symposium on Security and Privacy (S&P'04). Oakland, May 9 –12, 2004. Piscataway : IEEE, 2004: 103–114.
5. Krishnamurthy, B. *On network-aware clustering of Web clients* I B. Krishnamurthy, J. Wang II Proc. of ACM SIGCOMM 2000. Stockholm 28 August – 1 September, 2000. [USA]: ACM publishing, 2000:97–110.
6. Jin, C. *Hop-count filtering: An effective defense against spoofed DDoS traffic* I C. Jin, H. Wang, K.G. Shin II Proc. of 10th ACM Conference on Computer and Communications Security. Washington, October 27-30, 2003. [USA] : ACM publishing, 2003:30-41.
7. Xuan, D. A Gateway-Based *Defense System for Distributed DoS Attacks in High Speed Networks* I D. Xuan, R. Bettati, W. Zhao II Proc.of 2nd IEEE SMC Information Assurance Workshop. West Point, NY, June, 2001. - Piscataway : IEEE, 2001:212-219.
8. Kang, J. *Protect E-Commerce against DDoS Attacks with Improved DWARD Detection System* I J. Kang, Z. Zhang, J. Ju II Proc. of 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service. HongKong, 29 March-1 April, 2005. Piscataway : IEEE, 2005:100-105.
9. Mirkovic, J. A *Taxonomy of DDoS Attacks and Defense Mechanisms / J.Mirkovic, P. Reiher II ACM SIGCOMM Computer Communications Review*. 2004;34(2):643-666.
10. Li, M. *Decision Analysis of Statistically Detecting Distributed Denial-of Service Flooding* Attacks I M. Li, C Chi, W. Jia et al. II International Journal of Information Technology and Decision Making. 2003;2(3):397-405.
11. Peng, T. *Proactively Detecting DDoS Attack Using Source IP Address Monitoring* I T. Peng, C. Leckie, R. Kotagiri II Networking 2004. Athens, Greece, May 9-14, 2004. Berlin : Springer, 2004;3042:771-782.
12. Терновой О.С., Шатохина А.С. *Методика обнаружения уязвимостей к DDoS-атакам систем управления контентом на примере системы Wordpress.* М: «Известия Алтайского государственного университета». 2012;1/2(71):104–108.
13. В.А. Бухалев *Распознавание, оценивание и управление в системах со случайной скачкообразной структурой*. М.: Наука «Физматлит», 1996:287.

REFERENCES

1. Cabrera, J.B.D. *Proactive detection of distributed denial of service attacks using mib traffic variables – a feasibility study* I J.B.D. Cabrera, L. Lewis, X. Qin et al. II Proc.of International Symposium on Integrated Network Management. Seattle, 14–18 May. 2001. Piscataway: IEEE, 2001:609– 622.
2. Ioannidis, J. *Implementing Pushback: Router-Based Defense Against DDoS Attacks* I J. loannidis, S.M. Bellovin II Proc. of Symposium of Network and Distributed Systems Security (NDSS). San Diego, 6-8 February 2002. 2002:57-71.
3. Manajan, R. *Controlling High Bandwidth Aggregates in the Network*: ICSI Technical Report I R. Manajan, S.M. Bellovin, S. Floyd et al. ICSI, 2001:16.
4. CoIIins, M. An *Empirical Analysis of Target-Resident DoS Filters* I M. Collins, M.K. Reiter If Proc. of 2004 IEEE Symposium on Security and Privacy (S&P'04). Oakland, May 9 –12, 2004. Piscataway : IEEE, 2004:103–114.

5. Krishnamurthy, B. *On network-aware clustering of Web clients* I B. Krishnamurthy, J. Wang II Proc. of ACM SIGCOMM 2000. Stockholm 28 August – 1 September, 2000. [USA]: ACM publishing, 2000:97–110.
6. Jin, C. *Hop-count filtering: An effective defense against spoofed DDoS traffic* I C. Jin, H. Wang, K.G. Shin II Proc. of 10th ACM Conference on Computer and Communications Security. Washington, October 27-30,2003. [USA] : ACM publishing, 2003:30-41.
7. Xuan, D. A Gateway-Based *Defense System for Distributed DoS Attacks in High Speed Networks* I D. Xuan, R. Bettati, W. Zhao II Proc. of 2nd IEEE SMC Information Assurance Workshop. West Point, NY, June, 2001. Piscataway : IEEE, 2001:212-219.
8. Kang, J. *Protect E-Commerce against DDoS Attacks with Improved DWARD Detection System* I J. Kang, Z. Zhang, J. Ju II Proc. of 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service. HongKong, 29 March - 1 April, 2005. Piscataway : IEEE, 2005:100-105.
9. Mirkovic, J. A *Taxonomy of DDoS Attacks and Defense Mechanisms / J.Mirkovic, P. Reiher II ACM SIGCOMM Computer Communications Review*. 2004;34(2):643-666.
10. Li, M. *Decision Analysis of Statistically Detecting Distributed Denial-of Service Flooding* Attacks I M. Li, C Chi, W. Jia et al. II International Journal of Information Technology and Decision Making. 2003;2(3):397- 405.
11. Peng, T. *Proactively Detecting DDoS Attack Using Source IP Address Monitoring* I T. Peng, C. Leckie, R. Kotagiri II Networking 2004. Athens, Greece, May 9-14, 2004. Berlin : Springer. 2004;3042:771-782.
12. Ternovoy O.S., Shatokhina A.S. *Method of detecting vulnerabilities to DDoS attacks of content management systems on the example of the Wordpress system*/ Ternovoy O. S., Izvestiya Altaiskogo gosudarstvennogo universiteta. 2012;1/2(71):104-108.
13. Bukhalev V.A. *Recognition, evaluation and control in systems with random jump structure* /M.: Nauka "Fizmatlit". 1996:287.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATIONS ABOUT AUTHORS

Милосердов Игорь Васильевич, д.т.н, профессор, Санкт Петербургский институт информатики и автоматизации Российской академии наук, Санкт-Петербург, Российская Федерация
e-mail: ig.milos@yandex.ru

Igor V. Miloserdov, Dr. Sci. (Tech), professor, Saint Petersburg Institute of Informatics and automation of the Russian Academy of Sciences, Saint Petersburg, Russian Federation.

.

Малышев Владимир Александрович, д.т.н, профессор, ВУНЦ ВВС «Военно-воздушная академия им. проф. Н.Е Жуковского и Ю.А. Гагарина», Воронеж, Российская Федерация
e-mail: vamalyshev@list.ru

Vladimir A. Malyshev, Dr. Sci. (Tech)., professor, MESC AF «Air Force Academy named after prof. N.E. Zhukovsky and Y.A. Gagarin", Voronezh, Russian Federation