МУЛЬТИСЕРВИСНЫЕ СЕТИ: ДИСКРЕТНАЯ РИСК-МОДЕЛЬ HTTP-ФЛУДА

***Калашников Андрей Олегович**, доктор технических наук, г. Москва*
***Бурса Максим Васильевич**, г. Воронеж*
***Остапенко Григорий Александрович** , доктор технических наук, профессор, г. Воронеж*

В данной работе рассматриваются вопросы оценки риска реализации распределенных атак типа «HTTP–флуд» на мультисервисные сети с использованием дискретных риск–оценок. Производятся оценки риска мультисервисных сетей, имеющих в своем составе как один web–сервер, так и их множество при реализации на них синхронных и асинхронных атак

***Ключевые слова**: риск, дискретизация, HTTP–флуд, мультисервисные сети*

MULTISERVICE NETWORKS: DISCRETE RISK MODEL HTTP-FLOOD

***Andrey Kalashnikov**, Doctor of technical sciences, Moscow*
***Maksim Bursa**, Voronezh*
***Grigoriy Ostapenko**, Doctor of technical sciences, Professor, Voronezh*

This paper discusses the issues of risk assessment implementation of distributed attacks such as «HTTP–flood» on multiservice networks using discrete risk assessments. Risk assessment carried out multi–service networks, having in its composition as a web–server and a lot of them in implementing them synchronous and asynchronous attacks

***Keywords**: risk, sampling, HTTP–flood, multiservice networks*

Атаки типа «HTTP-флуд» являются весьма популярным средством нарушения доступности информации. Согласно данным, предоставленным организациями Prolexic и Akamai, количество данных атак за последние полтора года составляет 10-20% от общего количества DDoS-атак [1]. Они направлены на web-серверы, которые зачастую входят в состав мультисервисных сетей (МСС). Из анализа особенностей МСС можно сделать вывод о том, что обеспечение их отказоустойчивости является существенным моментом с точки зрения безопасности, так как нарушение функционирования одной из услуг, предоставляемых сетью, влияет на другие неопределенным образом.

Из всего вышесказанного следует необходимость повышения защищенности web-серверов МСС от атак типа «HTTP-флуд». Одним из важнейших этапов процесса повышения защищенности объектов различного характера является оценка риска реализации той или иной угрозы [2-5]. Данная оценка проводится для определения правильных и своевременных мероприятий по повышению защиты, а также выбора средств, способных обеспечить оптимальный уровень защищенности объекта.

Стартовым этапом риск-анализа систем различного характера обычно [2-5] является определение аналитического вида функции риска реализации атак на отдельный компонент этой системы. Отсюда необходимо получить аналитический вид ущерба, который получает компонент системы при реализации атаки, а также определить, на основании статистических данных, вид закона распределения и шаг дискретизации переменной риска.

Ущерб от реализации конкретной атаки задается функцией ущерба, которая должна учитывать специфику конкретно взятой атаки, а закон распределения ущерба определяется с помощью одного из критериев проверки гипотезы о принадлежности полученных статистических данных за

определенный период времени теоретическому закону распределения.

Получим аналитический вид функции ущерба при реализации атак типа «HTTP-флуд» на web-сервер МСС.

Атаки типа «HTTP-флуд» направлены на приведение ресурса сети в недоступное состояние, при котором легитимные пользователи не могут получить необходимую им информацию. Сила атаки определяется количеством вредоносных запросов, которые попадают на атакуемый web-сервер МСС, подвергающийся данной атаке [1].

Поступающее жертве количество HTTP-запросов зачастую переменно. Оно определяется как намерениями злоумышленника, так и количеством легитимных пользователей, обращающихся к атакуемому ресурсу сети [1].

Таким образом, когда в определенный промежуток времени t_0, суммарное количество запросов к атакуемому ресурсу МСС превышает его производительность $x_{\text{пр}}$, то он переходит в недоступное состояние, так как более не в состоянии обработать поступающий на него наплыв информации [1]. Суммарное количество запросов к ресурсу при реализации атаки типа HTTP-флуд возможно определить следующим образом [4]:

$$x_\Sigma = \xi \cdot x_b + x_l = \left(\left(\frac{k_{\text{исх}} + k_{\text{з}} - k_n}{k_{\text{исх}}}\right)(t - t_0)x_b + x_l\right),$$

где:

x_b –количество запросов, поступающих от ботнета, подконтрольного злоумышленнику при реализации атаки;

$\xi = \left(\frac{k_{\text{исх}}+k_{\text{з}}-k_n}{k_{\text{исх}}}\right)$ – коэффициент распространения ботнета, который характеризует степень увеличения или сокращения количества хостов-зомби в подконтрольной злоумышленнику сети с момента начала атаки t_0;

$k_{исх}$ – количество хостов-зомби в ботнете злоумышленника на момент начала атаки t_0;

$k_{\text{з}}$ – количество захваченных хостов-зомби в ботнете злоумышленника с момента начала атаки t_0;

k_{n} – количество потерянных хостов-зомби в ботнете злоумышленника с момента начала атаки t_0;

x_l – переменная, характеризующая количество запросов к атакуемому ресурсу, поступающих от легитимных пользователей в промежуток времени реализации атаки.

Следовательно, функция ущерба для ресурса МСС, подвергающегося атаке, принимает следующий вид:

$$U(t) = \left(\left(\frac{k_{\text{исх}} + k_{\text{з}} - k_n}{k_{\text{исх}}}\right)(t - t_0)x_b + x_l - x_{\text{пр}}\right)(t - t_0).$$

Как было установлено в [5], плотность вероятности ущерба от реализации атак типа «HTTP-флуд» определяется гамма-плотностью вероятности наступления ущерба.

Зная плотность вероятности наступления ущерба, становится возможным определение шага дискретизации функции риска.

Определение шага дискретизации t при оценке риска компонента МСС возможно с использованием двух оценок. Первая задается следующим выражением:

$$max(\Delta t) = \frac{1}{2 \cdot f_{max}} = \frac{1}{2 \cdot f(t^*)}.$$

$$(\Delta t) \le \left(T_{\text{ср}} - t^*\right),$$

где:

$T_{\text{ср}} = \int_0^\infty t \cdot f(t)dt,$

$f(t) = \frac{t^{c-1}\lambda^c \cdot exp(-\lambda t)}{\Gamma(c)}$ – плотность вероятности гамма-распределения [6],

c-коэффициент, определяющий продолжительность реализации атаки типа «HTTP-флуд»,

λ- коэффициент, определяющий интенсивность реализации атаки типа «HTTP-флуд»,

t^* – мода плотности вероятности гамма-распределения.

а вторая:

$$(\Delta t) \le min\left\{\left(T_{\text{ср}} - t^*\right), \frac{1}{2 \cdot f(t^*)}\right\}.$$

Найдем $T_{\text{ср}}$, t^* и $f(t^*)$для гамма-плотности вероятности наступления ущерба.

Для поиска t^* необходимо взять производную от плотности вероятности по времени и приравнять ее нулю:

$$\frac{df(t)}{dt} = \frac{d}{dt}\left(\frac{t^{c-1}\lambda^c \cdot exp(-\lambda t)}{\Gamma(c)}\right) =$$

$$\frac{\lambda^c}{\Gamma(c)}\left((c-1)t^{c-2}exp(-\lambda t) + t^{c-1}(-\lambda) \cdot exp(-\lambda t)\right) =$$

$$\frac{\lambda^c exp(-\lambda t)}{\Gamma(c)} \cdot \left((c-1)t^{c-2} + t^{c-1}(-\lambda)\right) = 0,$$

откуда:

$$c - 1 = \lambda t.$$

Следовательно, мода плотности вероятности $f(t)$ выглядит следующим образом:

$$t^* = \frac{c-1}{\lambda},$$

а пик функции:

$$f_{max} = f(t^*) = \left(\frac{\left(\frac{c-1}{\lambda}\right)^{c-1}\lambda^c \cdot exp\left(-\lambda\left(\frac{c-1}{\lambda}\right)\right)}{\Gamma(c)}\right) =$$

$$\left(\frac{(c-1)^{c-1}\lambda \cdot exp(1-c)}{\Gamma(c)}\right).$$

В свою очередь, $T_{ср}$:

$$T_{ср} = \int_0^{\infty} t \cdot \frac{t^{c-1}\lambda^c \cdot exp(-\lambda t)}{\Gamma(c)} dt.$$

Для решения данного интеграла необходимо свести подынтегральное выражение к гамма-функции, которая определяется следующим выражением [7]:

$$\Gamma(c) = \int_0^{\infty} t^{c-1} exp(-t) dt,$$

следовательно:

$$T_{ср} = \int_0^{\infty} \frac{t^c \lambda^c \cdot exp(-\lambda t)}{\Gamma(c)} dt = \frac{1}{\Gamma(c)} \int_0^{\infty} t^{c+1-1} \lambda^{c+1-1} \cdot exp(-\lambda t) dt.$$

Далее введем замену переменных $y=\lambda t$, получим:

$$T_{ср} = \frac{1}{\lambda \cdot \Gamma(c)} \int_0^{\infty} y^{c+1-1} \cdot exp(-y) dt = \frac{\Gamma(c+1)}{\lambda \cdot \Gamma(c)} = \frac{c \cdot \Gamma(c)}{\lambda \cdot \Gamma(c)} = \frac{c}{\lambda}.$$

Тогда $max(\Delta t)$:

$$max(\Delta t) = \frac{\Gamma(c)}{2(c-1)^{c-1} \cdot \lambda \cdot exp(1-c)}.$$

Таким образом, получаем, что Δt может определяться одним из двух способов:

$$(\Delta t) \le \frac{1}{\lambda},$$

либо:

$$(\Delta t) \le min\left\{\frac{1}{\lambda}, \frac{\Gamma(c)}{2(c-1)^{c-1} \cdot \lambda \cdot exp(1-c)}\right\}.$$

Также, немаловажным является задание количества шагов дискретизации, оценить которое можно определить следующим образом:

$$n \ge [\lambda] + 1,$$

где $[.]$ – оператор взятия целой части.

Для компонентов МСС, подвергающихся атакам типа «HTTP-флуд» примем:

$$\Delta t = \frac{1}{2 \cdot f_{max}} = \frac{\Gamma(c)}{2(c-1)^{c-1} \cdot \lambda \cdot exp(1-c)}.$$

Тогда:

$$n \ge \left[\frac{2(c-1)^{c-1} \cdot \lambda \cdot exp(1-c)}{\Gamma(c)}\right] + 1. \quad (1)$$

На рисунке 1 представлена зависимость плотности вероятность гамма распределения от изменения параметра c.

Полученный в выражении (1) результат согласуется с эмпирическими данными, приведенными на рисунке 1, где при увеличении параметра с область значений функции возрастает.

В соответствии с представленными выше результатами, огибающая функции риска web-сервера МСС, подвергающегося атаке типа «HTTP-флуд» имеет вид:

$$Risk(t) = U(t) f(t)(t) = \left(\left(\xi(t-t_0)x_b + x_l - x_{пр}\right)(t-t_0)\right) \frac{\lambda^c}{\Gamma(c)} t^{c-1} e^{-\lambda t}(t).$$

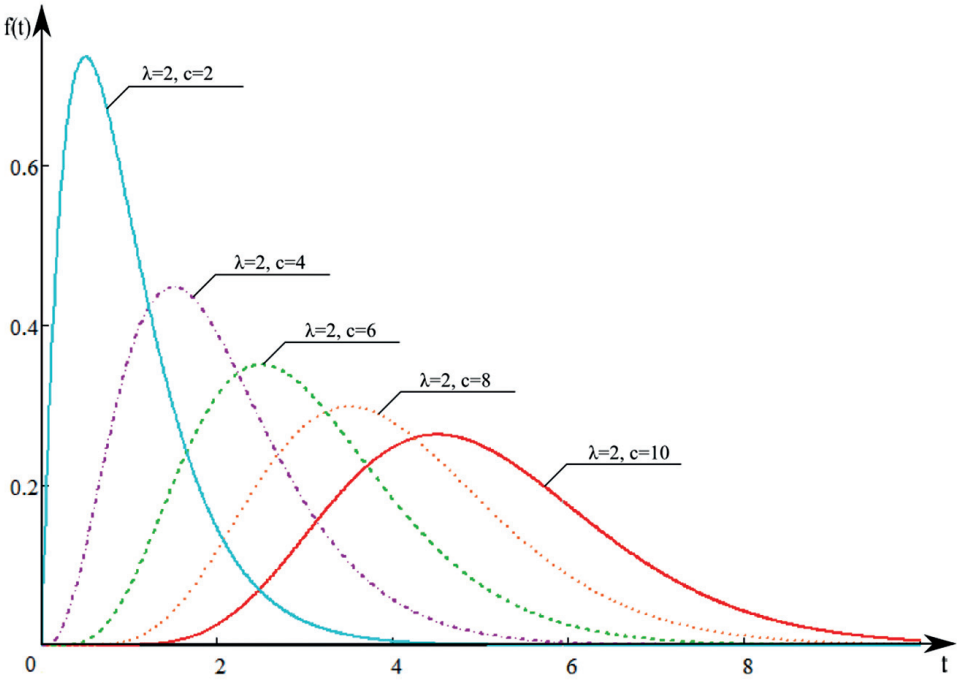

***Рис. 1** – График зависимости плотности гамма-распределения от параметра c*

Для дальнейших выкладок необходимо пронормировать ущерб. Нормированный ущерб для атак типа «HTTP-флуд» выглядит следующим образом:

$$\acute{U}(t) = \frac{U(t)}{(x_b + x_l)(t_{max} - t_0)^2} = \frac{(\xi(t - t_0)x_b + x_l - x_{\text{пр}})(t - t_0)}{(x_b + x_l)(t_{max} - t_0)^2}.$$

где t_{max} – мода функции риска [5].

А функция риска в заданном интервале $[t_1;t_2]$ функционирования сети:

$$Risk[t_1; t_2] = \sum_{\acute{k}=t_1+t}^{t_2} \acute{U}(\acute{k}) f(\acute{k}) \left(\frac{1}{n}\right) =$$

$$\sum_{\acute{k}=t_1+t}^{t_2} \left(\frac{(\xi(\acute{k} - t_0)x_b + x_l - x_{\text{пр}})(\acute{k} - t_0)}{(x_b + x_l)(t_{max} - t_0)^2}\right) \frac{\lambda^c}{\Gamma(c)} \acute{k}^{c-1} e^{-\lambda \acute{k}} \left(\frac{1}{n}\right),$$

где $\acute{k} = \frac{k}{n}, t_2 > t_1$.

Вышеприведенное выражение позволяет определить уровень риска web-сервера МСС в произвольном временном интервале $[t_1;t_2]$ реализации атак типа «HTTP-флуд» на него.

На основании полученных результатов становится возможным произвести аналитические оценки риска реализации синхронных и асинхронных атак данного типа на МСС, содержащую в своем составе более одного web-сервера [2-3].

Оценки будут производиться с учетом того, что ущербы, возникающие в отдельных компонентах МСС, слабо зависят друг от друга, что позволяет найти общий ущерб МСС как сумму ущербов, возникающих в конкретно взятых ее компонентах. Графически, процесс определения интервала оценки риска для МСС, состоящей из двух web-серверов представлен на рисунке 2, где изображены кривые огибающей функции риска при t_1=20 и t_2=30 для настроек двух web-серверов:

на рисунке а) ξ=0,9, x_b=4000, x_l=1500, $x_{\text{пр}}$=1700, t_0=4, c=3, λ=0,1;

на рисунке б) ξ=1,05, x_b=8000, x_l=1000, $x_{\text{пр}}$=5200, t_0=4, c=6, λ=0,3.

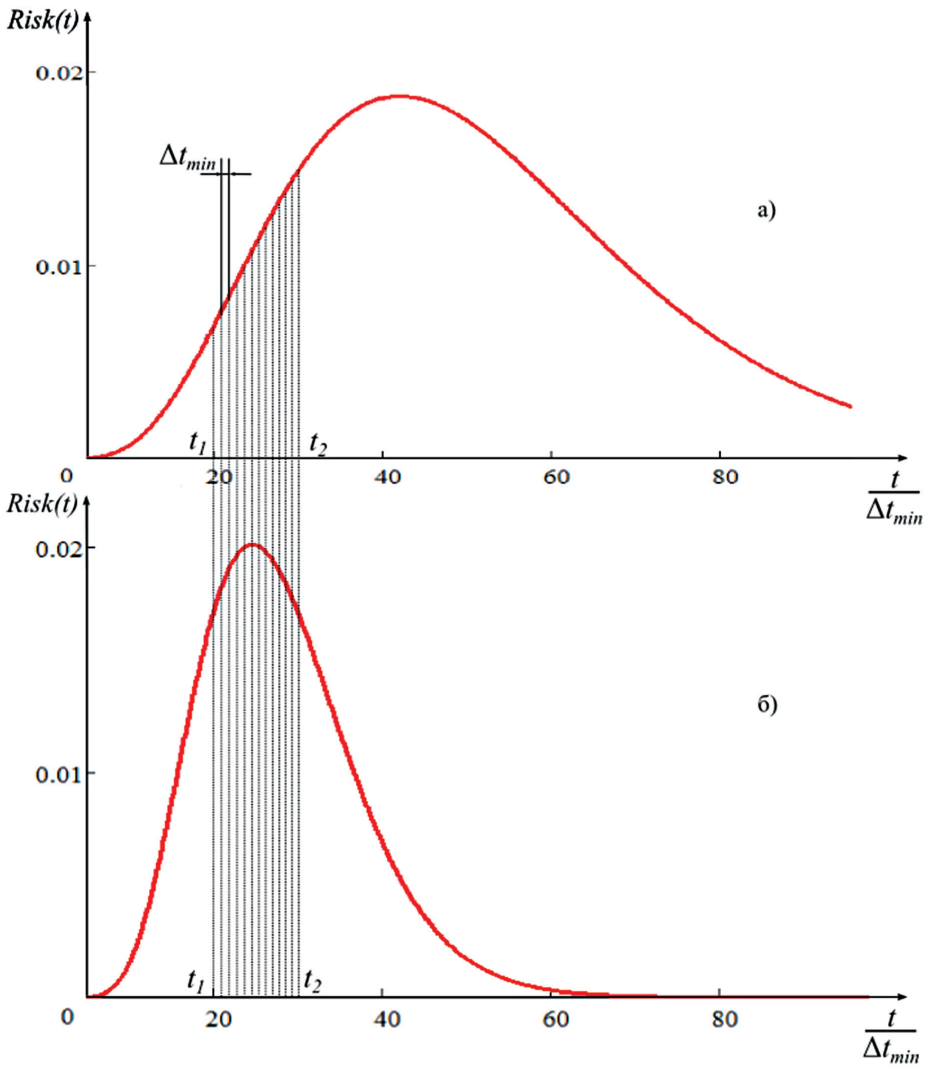

***Рис. 2** –Процесс определения интервала оценки риска МСС, состоящей из двух web-серверов*

Таким образом, при реализации синхронных атак на web-серверы МСС, состоящую из m компонент, может быть предложено следующее выражение:

$$Risk_{\Sigma}^{(CA)} = \sum_{\acute{k}=t_1+\Delta t_{min}}^{t_2} \left[\left[\sum_{i=1}^{m} \acute{U}_i(\acute{k})\right] \cdot \left[\prod_{i=1}^{m} f_i(\acute{k}) \cdot \left(\frac{1}{n_{max}}\right)\right]\right] =$$

$$\sum_{\acute{k}=t_1+\Delta t_{min}}^{t_2} \left[\begin{array}{c}\left[\sum_{i=1}^{m}\left(\left(\frac{\xi_i(\acute{k}-t_0)x_{b_i}+x_{l_i}-x_{\text{пр}_i}}{(x_{b_i}+x_{l_i})(t_{max}-t_0)^2}\right)(\acute{k}-t_0)\right)\right]\times \\ \times\left[\prod_{i=1}^{m}\left(\frac{\lambda^{c}}{\Gamma(c)}\acute{k}^{c-1}e^{-\lambda t}\right)\times\left(\frac{1}{n_{max}}\right)\right]\end{array}\right],$$

а при реализации асинхронных атак:

$$Risk_{\Sigma}^{(AA)} = \sum_{\acute{k}=t_1+\Delta t_{min}}^{t_2} \left[\sum_{i=1}^{m} \acute{U}_i(\acute{k})\, f_i(\acute{k})\left(\frac{1}{n_{max}}\right)\right] =$$

$$\sum_{\acute{k}=t_1+\Delta t_{min}}^{t_2}\left(\sum_{i=1}^{m}\left(\left(\frac{\left(\xi_i(\acute{k}-t_{0_i})x_{b_i}+x_{l_i}-x_{\text{пр}_i}\right)(\acute{k}-t_{0_i})}{(x_{b_i}+x_{l_i})(t_{max}-t_{0_i})^2}\right)\left(\frac{\lambda^{c}}{\Gamma(c)}\acute{k}^{c-1}e^{-\lambda t}\right)\left(\frac{1}{n_{max}}\right)\right)\right),$$

где: $\acute{k} = \frac{k}{n_{max}}, t_2 > t_1,$

m – количество web-серверов в составе МСС,

Δt_{min} – минимальный из шагов дискретизации m компонент МСС,

n_{max}=$max(n_1,...n_{\text{m}})$ – максимальное значение из различных количеств шагов дискретизации m компонент МСС.

Таким образом, в данной работе были предложены аналитические выражения функции ущерба, шага дискретизации и функции риска при реализации одной и множества асинхронных или синхронных атак типа «HTTP-флуд» на web-серверы МСС.

Полученные оценки представляются удобной базой для оценки и последующего управления рисками МСС, имеющим в своем составе web-сервер и подвергающимся атакам типа «HTTP-флуд».

Литература:

1. Сайт компании «Akamai» [Электронный ресурс]. – Режим доступа: http://www.akamai.com.
2. Остапенко, Г.А. Информационные риски в социальных сетях. [Текст]: монография /Г.А. Остапенко, Л.В. Паринова, В.И. Белоножкин, И.Л. Батаронов, К.В. Симонов; под ред. чл.-корр. РАН Д. А. Новикова. – Воронеж: Издательство «Научная книга». 2013. – 160 с.
3. Дешина, А.Е. Управление информационными рисками мультисерверных систем при воздействии DDOS –атак [Текст] / А.Е. Дешина, М.В. Бурса, А.Г. Остапенко, А.О. Калашников, Г.А. Остапенко; под ред. чл.-корр. РАН Д.А. Новикова. – Воронеж: Научная книга, 2014. – 160 с.
4. Бурса, М.В. HTTP-флуды информационно- телекоммуникационных систем: оценка рисков и управление защищенностью [Текст] / М.В. Бурса, А.Г. Остапенко, А.О. Калашников // Сборник трудов конференции «XII всероссийское совещание по проблемам управления ВСПУ-2014» Институт проблем управления им. В.А. Трапезникова РАН. 2014. С. 9150-9153.
5. Бурса М.В. Аналитическая оценка пика функции риска для компонентов информационно-телекоммуникационных систем, подвергающимся атакам типа HTTP-флуд / М.В. Бурса // Информация и безопасность. 2014. № 2. – С. 232-235
6. Бочаров, П.П. Теория вероятностей. Математическая статистика [Текст] / П.П. Бочаров, А.В. Печинкин. – М.: ФИЗМАТЛИТ, 2005. – 296 с.
7. Виленкин, Н.Я. Специальные функции и теория представлений групп [Текст] / Н.Я. Виленкин – М.: Наука, 1965. – 588 с.

References:

1. Sayt kompanii «Akamai» [Elektronnyiy resurs]. – Rezhim dostupa: http://www.akamai.com.
2. Ostapenko, G.A. Informatsionnyie riski v sotsialnyih setyah. [Tekst]: monografiya /G.A. Ostapenko, L.V. Parinova, V.I. Belonozhkin, I.L. Bataronov, K.V. Simonov; pod red. chl.-korr. RAN D. A. Novikova. – Voronezh: Izdatelstvo «Nauchnaya kniga». 2013. – 160 p.
3. Deshina, A.E. Upravlenie informatsionnyimi riskami multiservernyih sistem pri vozdeystvii DDOS –atak [Tekst] / A.E. Deshina, M.V. Bursa, A.G. Ostapenko, A.O. Kalashnikov, G.A. Ostapenko; pod red. chl.-korr. RAN D.A. Novikova. – Voronezh: Nauchnaya kniga, 2014. – 160 p.
4. Bursa, M.V. HTTP-fludyi informatsionno- telekommunikatsionnyih sistem: otsenka riskov i upravlenie zaschischennostyu [Tekst] / M.V. Bursa, A.G. Ostapenko, A.O. Kalashnikov // Sbornik trudov konferentsii «XII vserossiyskoe soveschanie po problemam upravleniya VSPU-2014» Institut problem upravleniya im. V.A. Trapeznikova RAN. 2014. P. 9150-9153.
5. Bursa M.V. Analiticheskaya otsenka pika funktsii riska dlya komponentov informatsionno-telekommunikatsionnyih sistem, podvergayuschimsya atakam tipa HTTP-flud / M.V. Bursa // Informatsiya i bezopasnost. 2014. # 2. – P. 232-235
6. Bocharov, P.P. Teoriya veroyatnostey. Matematicheskaya statistika [Tekst] / P.P. Bocharov, A.V. Pechinkin. – M.: FIZMATLIT, 2005. – 296 p.
7. Vilenkin, N.Ya. Spetsialnyie funktsii i teoriya predstavleniy grupp [Tekst] / N.Ya. Vilenkin – M.: Nauka, 1965. – 588 p.