BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 2, Number 354 (2015), 55 – 60

THE FORMALIZED MODELS OF LINEAR TYPE FOR DIFFERENTIATION OF DOS ATTACKS ON THE BASIS OF THE WEIGHT FACTORS METHOD

Shangytbayeva G.A.[1], Karpinski M.P.[2], Zhumagulova A.A.[3]

E-mail: gul_janet@mail.ru, mkarpinski@ath.bielsko.pl, alia_zha@mail.ru

[1] Kazakh National Technical University named after K. I. Satpayev, Almaty, Kazakhstan;
[2] Academy of Technologies and the Humanities in Bielsko-Biala, Bielsko-Biala, Poland;
[3] K. Zhubanov Aktobe Regional State University, Kazakhstan

Keywords: formalized mathematical model, client – server model, DOS – attacks, DDOS – attacks, DRDoS – attacks.

Abstract. This article discusses the DoS/DDoS/DRDoS tasks of attacks on the client – services model of communication. In the analysis results of classification of DoS/DDoS/DRDoS – attacks the formalized mathematical models is offered. They allow to define a level of influence of indexes of attacks to a computer network. These structured formalized mathematical models allow to consider structure of a network on the basis of big percent of a measure of influence of each type of attack. It gives the chance to effectively protect an information system taking into account information on threats. Based on classification of information threats, characteristic for attacks such as DoS/DDoS/DRDoS, the formalized models of a linear type of attack for differentiation of attacks on the basis of the weight factors method are offered. By these indexes and coefficients it is possible to define the main types of threats in computer systems. This allows to efficiently design information protection system based on information threats.

УДК 004.75: 004.42.3

ФОРМАЛИЗОВАННЫЕ МОДЕЛИ ЛИНЕЙНОГО ВИДА ДЛЯ ДИФФЕРЕНЦИАЦИИ DOS АТАК НА ОСНОВЕ МЕТОДА ВЕСОВЫХ КОЭФФИЦИЕНТОВ

Г. А. Шангытбаева[1], Н. П. Карпинский[2], А. А. Жумагулова[3]

[1] Казахский национальный технический университет им.К. И. Сатпаева, Алматы, Казахстан;
[2] Бельско-Бяльская техническо-гуманитарная академия, Бельско-Бияла, Польша;
[3] Актюбинский региональный государственный университет им. К. Жубанова, Казахстан

Ключевые слова: формализованная математическая модель, клиент – серверная модель, DOS – атаки, DDOS – атаки, DRDoS – атаки.

Аннотация. В данной статье рассматриваются задачи DoS / DDoS / DRDoS атак по модели клиент – услуг связи. В результате анализа классификации DoS / DDoS / DRDoS–атак предложены формализованные математические модели. Они позволяют определить степень влияния показателей атак на компьютерную сеть. Данные структурированные формализованные математические модели позволяют учитывать структуру сети на основе большого процента меры влияния каждого вида атаки. Это дает возможность эффективно спроектировать защиту информационную систему с учетом информации об угрозах. Основываясь на классификации информационных угроз, характерных для атак типа DoS / DDoS / DRDoS предложены формализованные модели линейного вида для дифференциации атак на основе метода весовых коэффициентов. С помощью данных показателей и коэффициентов можно определить основные виды угроз в компьютерных системах. Это позволяет эффективно проектировать системы защиты информации с учетом информационных угроз.

Введение. Рост киберпреступности в последние годы позволяет несанкционированный доступ к ресурсам компьютерных сетей (КС). Среди самых распространенных многочисленных атак злоумышленников на КС является прерывание и искажения пакетного трафика. Самыми разрушительными атаками на сегодняшнее время является атаки, направленные на отказ в обслуживании законных услуг. В этом случае инициатор атак компрометирует узел – пользователя, эксплуатируя его ресурсы, для получения полного управления узлом. Инициатор атак направляет большое количество поддельного трафика к узлу – пользователя, потребляя при этом пропускную способность существенного объема, что приводит к невозможности обслуживать легитимный трафик [1].

К такому классу атак относятся DoS (Denial of Service) – во время которой происходит повышенный расход ресурсов процессора и уменьшения пропускной способности канала связи, что может привести к сильному замедлению работы всей КС, DDoS (Distributed Denial of Service) – распределенная атака, направлена на компьютер пользователя в КС с намерением сделать информационные ресурсы недоступными, DRDoS (Distributed Reflection Denial of Service) – распределенная отражена атака, направленная на поглощение пропускной способности сети. Поэтому разработка формализованной математической модели влияния различных видов DoS / DDoS / DRDoS – атак актуальной задачей [2].

Архитектуры клиент – серверных систем. Для того, чтобы увидеть ключевые задачи архитектуры устойчивой к нападению КС, сначала рассматривается упрощенная модель коммуникации клиент – сервер, которая изображена на рисунке 1.

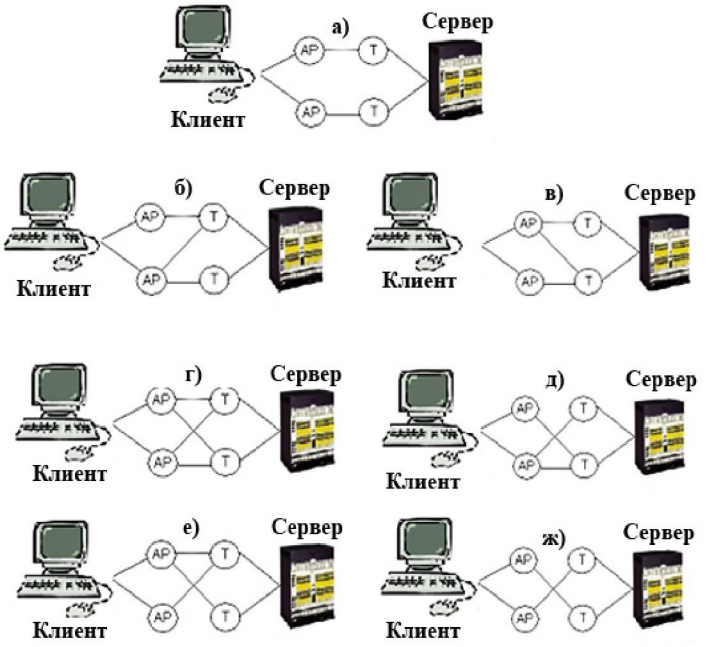

Рисунок 1 – Модель коммуникации клиент – сервер: AP – точка доступа, T – точка назначения

В данных моделях ограничимся двумя точками входа и двумя точками назначения. Линии, соединяющие точки входа и точки назначения, моделируют коммуникацию между ними в КС.

Под устойчивостью сети понимается способность сети обеспечить альтернативную коммуникацию при разрушении (или попытках разрушить) хотя бы одного пути между клиентом и сервером [3].

Формализованная математическая модель влияния различных видов DoS / DDoS / DRDoS – атак. В результате анализа классификации DoS / DDoS / DRDoS – атак нами предложено формализованную математическую модель (1), которая позволяет определить степень влияния показателей атак на КС:

$$
\begin{aligned}
P_{DoS} &= \beta_i(P_{Smurf}, P_{Fraggle}, P_{SYNFlood}, P_{DNS}),\\
P_{DDoS} &= \delta_i(P_{Trinoo}, P_{TFN/TFN2K}, P_{Stacheldraht}),\\
P_{DRDoS} &= \mu_i(P_{Smurf}, P_{Fraggle}, P_{DNS}, P_{SNMP}),
\end{aligned} \tag{1}
$$

где β_i, δ_i, μ_i – весовые коэффициенты влияния показателей DoS, DDoS, DRDoS атак, причем $\sum_{i=1}^{4}\beta_i = 1$, $\sum_{i=1}^{3}\delta_i = 1$, $\sum_{i=1}^{4}\mu_i = 1$.

Весовые коэффициенты определяют вклад основных видов атак DoS / DDoS / DRDoS в КС и позволяют учесть указанные атаки при разработке и эксплуатации систем защиты информации. С помощью данных показателей и коэффициентов можно определить основные виды угроз и их влияние на уровень безопасности КС, позволит эффективно проектировать системы защиты информации с учетом информационных угроз [4, 5].

Построим формализованные математические модели вероятности информационных угроз с характером DoS / DDoS / DRDoS – атак линейного вида на основе использования метода весовых коэффициентов:

$$
\begin{aligned}
P\_ИУ(P) &= \alpha_1 P_{Конф.} + \alpha_2 P_{Цел.} + \alpha_3 P_{Дост.},\\
P\_DoS(P) &= \beta_1 P_{Smurf} + \beta_2 P_{Fraggle} + \beta_3 P_{SYNFlood} + \beta_4 P_{DNS},\\
P\_DDoS(P) &= \delta_1 P_{Trinoo} + \delta_2 P_{TAN/TF2K} + \delta_3 P_{Stacheldraht},\\
P\_DRDoS(P) &= \mu_1 P_{Smurf} + \mu_2 P_{Fraggle} + \mu_3 P_{DNS} + \mu_4 P_{SNMP}.
\end{aligned} \tag{2}
$$

где *P_ИУ_(P)* – вероятность информационных угроз; *P_DoS(P)* – вероятность DoS атак; *P_DDoS(P)* – вероятность DDoS атак; *P_DRDoS(P)* – вероятность DRDoS атак; α_i, β_i, δ_i, μ_i – весовые коэффициенты, причем $\alpha_i \in [0;1]$, $\beta_i \in [0;1]$, $\delta_i \in [0;1]$, $\mu_i \in [0;1]$ соответственно.

Данные весовые коэффициенты можно определить экспериментальным методом для каждой конкретной сети. То есть спроектировать архитектуры сетей, представленных на рис. 1, и установить интенсивность различного вида атак на сеть. С помощью упрощенной модели коммуникации системы клиент – сервер и математической моделей (1) и (2) определяем матрицы активности сети, согласно которым формируем вывод об осуществлении вида атаки [6–8]:

$$
\alpha_{инф.угр.} = \begin{bmatrix}
\alpha_1^a & \alpha_2^a & \alpha_3^a\\
\alpha_1^b & \alpha_2^b & \alpha_3^b\\
\alpha_1^c & \alpha_2^c & \alpha_3^c\\
\alpha_1^d & \alpha_2^d & \alpha_3^d\\
\alpha_1^e & \alpha_2^e & \alpha_3^e\\
\alpha_1^f & \alpha_2^f & \alpha_3^f\\
\alpha_1^g & \alpha_2^g & \alpha_3^g
\end{bmatrix},\quad
\beta_{DoS} = \begin{bmatrix}
\beta_1^a & \beta_2^a & \beta_3^a & \beta_4^a\\
\beta_1^b & \beta_2^b & \beta_3^b & \beta_4^b\\
\beta_1^c & \beta_2^c & \beta_3^c & \beta_4^c\\
\beta_1^d & \beta_2^d & \beta_3^d & \beta_4^d\\
\beta_1^e & \beta_2^e & \beta_3^e & \beta_4^e\\
\beta_1^f & \beta_2^f & \beta_3^f & \beta_4^f\\
\beta_1^g & \beta_2^g & \beta_3^g & \beta_4^g
\end{bmatrix},
$$

$$\delta_{DDoS} = \begin{bmatrix} \delta_1^a & \delta_2^a & \delta_3^a \\ \delta_1^b & \delta_2^b & \delta_3^b \\ \delta_1^c & \delta_2^c & \delta_3^c \\ \delta_1^d & \delta_2^d & \delta_3^d \\ \delta_1^e & \delta_2^e & \delta_3^e \\ \delta_1^f & \delta_2^f & \delta_3^f \\ \delta_1^g & \delta_2^g & \delta_3^g \end{bmatrix}, \quad \mu_{DRDoS} = \begin{bmatrix} \mu_1^a & \mu_2^a & \mu_3^a & \mu_4^a \\ \mu_1^b & \mu_2^b & \mu_3^b & \mu_4^b \\ \mu_1^c & \mu_2^c & \mu_3^c & \mu_4^c \\ \mu_1^d & \mu_2^d & \mu_3^d & \mu_4^d \\ \mu_1^e & \mu_2^e & \mu_3^e & \mu_4^e \\ \mu_1^f & \mu_2^f & \mu_3^f & \mu_4^f \\ \mu_1^g & \mu_2^g & \mu_3^g & \mu_4^g \end{bmatrix}. \quad (3)$$

Итак, взяв общее количество атак за 100%, можно определить, сколько процессов будет принадлежать каждому виду атак. Тогда коэффициенты будут исчисляться согласно следующим соотношением:

$$\alpha_1^a = \frac{n^a_{Конф.}}{100\%}, \alpha_2^a = \frac{n^a_{Цл.}}{100\%}, \alpha_3^a = \frac{n^a_{Дост.}}{100\%},$$
$$\beta_1^a = \frac{n^a_{Smurf}}{100\%}, \beta_2^a = \frac{n^a_{Fraggle}}{100\%}, \beta_3^a = \frac{n^a_{SYNFlood}}{100\%}, \beta_4^a = \frac{n^a_{DNS}}{100\%}, \quad (4)$$
$$\delta_1^a = \frac{n^a_{Trinoo}}{100\%}, \delta_2^a = \frac{n^a_{TFN/TFN2K}}{100\%}, \delta_3^a = \frac{n^a_{Stacheldraht}}{100\%},$$
$$\mu_1^a = \frac{n^a_{Smurf}}{100\%}, \mu_2^a = \frac{n^a_{Fraggle}}{100\%}, \mu_3^a = \frac{n^a_{DNS}}{100\%}, \mu_4^a = \frac{n^a_{SNMP}}{100\%},$$

где $n^a_{Конф.}$, $n^a_{Цл.}$, $n^a_{Дост.}$ – количество показателей информационных угроз на сеть типа a); n^a_{Smurf}, $n^a_{Fraggle}$, $n^a_{SYNFlood}$, n^a_{DNS} – количество показателей атак вида DoS на сеть типа a); n^a_{Trinoo}, $n^a_{TFN/TFN2K}$, $n^a_{Stacheldraht}$ – количество показателей атак вида DDoS на сеть типа a); n^a_{Smurf}, $n^a_{Fraggle}$, n^a_{DNS}, n^a_{SNMP} – количество показателей атак вида DRDoS на сеть типа a).

Аналогичным образом находим количественные показатели различного вида атак для клиент – серверных моделей типа b), c), d), e), f) и g).

Проведенных исследований и с учетом аналитических выражений (4) и эмерджентности модели коммуникации клиент – сервер получено:

$$\alpha_1^a = \frac{3}{8}\cdot\frac{1}{k_e^a} = 0{,}375, \alpha_1^b = \frac{3}{8}\cdot\frac{1}{k_e^b} = 0{,}15, \alpha_1^c = \frac{3}{8}\cdot\frac{1}{k_e^c} = 0{,}15,$$
$$\alpha_1^d = \frac{3}{8}\cdot\frac{1}{k_e^d} = 0{,}125, \alpha_1^e = \frac{3}{8}\cdot\frac{1}{k_e^e} = 0{,}15, \alpha_1^f = \frac{3}{8}\cdot\frac{1}{k_e^f} = 0{,}15,$$
$$\alpha_1^g = \frac{3}{8}\cdot\frac{1}{k_e^g} = 0{,}75, \alpha_2^a = \frac{1}{8}\cdot\frac{1}{k_e^a} = 0{,}125, \alpha_2^b = \frac{1}{8}\cdot\frac{1}{k_e^b} = 0{,}05,$$
$$\alpha_2^c = \frac{1}{8}\cdot\frac{1}{k_e^c} = 0{,}05, \alpha_2^d = \frac{1}{8}\cdot\frac{1}{k_e^d} = 0{,}375, \alpha_2^e = \frac{1}{8}\cdot\frac{1}{k_e^e} = 0{,}05,$$
$$\alpha_2^f = \frac{1}{8}\cdot\frac{1}{k_e^f} = 0{,}05, \alpha_2^g = \frac{1}{8}\cdot\frac{1}{k_e^g} = 0{,}0625, \alpha_3^a = \frac{1}{2}\cdot\frac{1}{k_e^a} = 0{,}5,$$

$$\alpha_3^b = \frac{1}{2}\cdot\frac{1}{k_e^b} = 0{,}2,\ \alpha_3^c = \frac{1}{2}\cdot\frac{1}{k_e^c} = 0{,}2,\ \alpha_3^d = \frac{1}{2}\cdot\frac{1}{k_e^d} = 0{,}166,$$

$$\alpha_3^e = \frac{1}{2}\cdot\frac{1}{k_e^e} = 0{,}2,\ \alpha_3^f = \frac{1}{2}\cdot\frac{1}{k_e^f} = 0{,}2,\ \alpha_3^g = \frac{1}{2}\cdot\frac{1}{k_e^g} = 0{,}25.$$

Данные коэффициенты определяем экспериментальным методом, спроектировав архитектуры, позволяющие определить интенсивность атак на сеть.

Для вычисления коэффициентов эмерджентности k_e^a, k_e^b, k_e^c, k_e^d, k_e^e, k_e^f, k_e^g воспользуемся формулой (5):

$$K_e = \frac{n_з}{n_e}, \qquad (5)$$

где $n_з$ – число связей, n_e – число компонентов.

$$k_e^a = \frac{2}{2} = 1; k_e^b = \frac{5}{2} = 2{,}5; k_e^c = \frac{5}{2} = 2{,}5; k_e^d = \frac{6}{2} = 3;$$

$$k_e^e = \frac{5}{2} = 2{,}5; k_e^e = \frac{5}{2} = 2{,}5; k_e^g = \frac{4}{2} = 2.$$

Следует отметить, что наибольшим коэффициентом эмерджентности обладает модель коммуникации клиент – сервер типа d). Поэтому ее целесообразно использовать для обеспечения безопасной передачи информационных потоков в компьютерных сетях [9, 10].

Заключение. Основываясь на классификации информационных угроз, характерных для атак типа DoS / DDoS / DRDoS предложены формализованные модели линейного вида для дифференциации атак на основе метода весовых коэффициентов. С помощью данных показателей и коэффициентов можно определить основные виды угроз в компьютерных системах, позволяющие эффективно проектировать системы защиты информации с учетом информационных угроз.

Для определения вида атаки сформулирована математическая модель коммуникации клиента и сервера, содержащая вероятность компрометации узла количество всевозможных путей от точек доступа к точкам назначения. Проведенный модельный эксперимент показал, что при увеличении количества всевозможных путей от клиента к серверу активность сети низкая, что затрудняет определение реализации атаки.

ЛИТЕРАТУРА

[1] Галатенко В.А. Информационная безопасность. – М.: Финансы и статистика, – 1997. – 158 с.

[2] Steve G. Distributed reflection denial of service. [Электронний ресурс] // Portal : Gibson Research Corporation URL: http://grc.com/DoS/drDoS.htm, 15. 04. 2014.

[3] Karpiński M. Badania realizacji rozproszonych ataków w sieci komputerowej. // Wiedza w Technologii Telekomunikacyjnych i Optyka KTTO 2011 / Red. M. Voznak, J. Skapa, I. P. Kurytnik, B. Borowik. – Szczyrk, Polska: Wydawca VSB–Uniwersytet Techniczny w Ostrawie, Czechy, –2011. – P. 226–228. – ISBN 978–80–248–2399–7.

[4] Karpinski M.P. Modeling network traffic computer network in implementation attacks such as DOS / DDOS // Information Security, American Psychological Association. Ethical standards of psychologists. – Washington, DC: American Psychological Association. – 2011б. – N 1 (5). – P. 143-146.

[5] Aleksander M. Features of Denial of Service Attacks in Information Systems // Computer and mathematical methods in modeling. – 2012. – Vol. 2, N 2. – P. 129-133.

[6] Wu T., Zhang H., Ma J. Zhang, S. Intelligent DDoS attack defence model // Lecture Notes in Electrical Engineering. – 2014.

[7] Bhuyan M.H., Bhattacharyya D.K., Kalita J.K. An empirical evaluation of information metrics for low–rate and high–rate DDoS attack detection // Pattern Recognition Letters. – 2015. – 51. – P. 1-7.

[8] Bu T., Norden S., Woo T. Trading resiliency for security: Model and algorithms // In Proc. 12th IEEE International Conference on Network Protocols. – 2004. – P. 218-227.

[9] Wang J., Chien A.A. Using overlay networks to resist denial of service attacks // Submitted to ACM Conf. on Computer and Comm. Security, October, 2003.

[10] Michael T. Goodrich. Probabilistic Packet Marking for Large–Scale IP Traceback // IEEE / ACM Transactions on networking. – 2007. – Vol. 10, N 10.

REFERENCES

[1] Galatenko V.A. *Information security*. M.: Finance and Statistics, **1997**, pp. 150-158. (in Russ.).

[2] Steve G. *Distributed reflection denial of service*. Portal : Gibson Research Corporation URL: http://grc.com/DoS/drDoS.htm, 15. 04. **2014**. (in Eng.).

[3] Karpiński M. *Badania realizacji rozproszonych ataków w sieci komputerowej*. Wiedza w Technologii Telekomunikacyjnych i Optyka KTTO 2011 Szczyrk, Polska: Wydawca VSB–Uniwersytet Techniczny w Ostrawie, Czechy, **2011**, pp. 226-228. ISBN 978–80–248–2399–7. (in Eng.).

[4] Karpinski M.P. *Modeling network traffic computer network in implementation attacks such as DOS / DDOS*. Information Security, American Psychological Association. Ethical standards of psychologists. Washington, DC: American Psychological Association. №1 (5), **2011,** pp. 143-146. (in Eng.).

[5] Aleksander M. *Features of Denial of Service Attacks in Information Systems*. Computer and mathematical methods in modeling. Vol 2, № 2. **2012,** pp.129-133. (in Eng.).

[6] Wu T., Zhang H., Ma J. Zhang, S. *Intelligent DDoS attack defence model*. Lecture Notes in Electrical Engineering, **2014**. (in Eng.).

[7] Bhuyan M.H., Bhattacharyya D.K., Kalita J.K. *An empirical evaluation of information metrics for low–rate and high–rate DDoS attack detection*. Pattern Recognition Letters, 51, **2015**, pp. 1-7. (in Eng.).

[8] Bu T., Norden S. and Woo T. *Trading resiliency for security: Model and algorithms*. In Proc. 12th IEEE International Conference on Network Protocols, **2004**, pp. 218-227. (in Eng.).

[9] Wang J. and Chien A.A. *Using overlay networks to resist denial of service attacks*. Submitted to ACM Conf. on Computer and Comm. Security, October, **2003**. (in Eng.).

[10] Michael T. Goodrich. *Probabilistic Packet Marking for Large–Scale IP Traceback*. IEEE / ACM Transactions on networking, Vol. 10, N 10, January, **2007.** (in Eng.).

БӨЛІСТІ ЖЕЛІЛІК ШАБУЫЛДАРДЫ АНЫҚТАУ ЖӘНЕ ШЕКТЕУ ТИІМДІЛІКТЕРІН ЖОҒАРЫЛАТУ ӘДІСТЕРІ

Г. А. Шаңғытбаева[1], Н. П. Карпинский[2], А. А. Жұмағұлова[3]

[1] Қ. И. Сәтпаев атындағы Қазақ ұлттық техникалық университеті, Алматы, Қазақстан;
[2] Бельско-Бяльская технико-гуманитарлық академияся, Бельско-Бияла, Польша;
[3] Қ. Жұбанов атындағы Ақтөбе өңірлік мемлекеттік университеті, Қазақстан

Тірек сөздер: қалыптасқан математикалық модел, клиент – сервер моделі, DOS – шабуылдар, DDOS – шабуылдар, DRDoS – шабуылдар.

Аннотация. Мақалада клиент – қызметі байланысы бойынша DoS / DDoS / DRDoS шабуыл түрлерінің түрлі есептері қарастырылған. DoS / DDoS / DRDoS шабуылдарын бір жүйеге топтастыру есептері нәтижесінде математикалық үлгілерді қалыптастыру ұсынылады. Ол компьютерлік желілердегі қалыптасқан шабуылдардың көрсеткіштерінің әсер ету дәрежелерін анықтауға мүмкіндік береді. Мұндай құрылымды қалыптасқан математикалық моделдер әрбір шабуылға әсер ететін шаралардың өте үлкен көлемді болуына байланысты желінің құрылымын есепке алуға негіз бола алады. Соның нәтижесінде желілердегі болатын қауіп-қатерлерді есепке ала отырып, ақпараттық жүйелерді қорғау жұмыстарын тиімді түрде жобалауға мүмкіндік береді. Ақпараттарға төнетін қауіп-қатерлердің түрлеріне байланысты, DoS / DDoS / DRDoS шабуылдарына ғана тән салмақтық коэфициенттер әдісі негізіндегі шабуыл түрлеріне арналған сызықты түрдегі қалыптасқан үлгілері беріліп отыр. Берілген көрсеткіштер мен коэфициенттердің мәндерінің көмегімен компьютерлік жүйелерде кездесетін негізгі қауіп-қатерлердің түрлерін анықтауға болады. Олар ақпараттарға төнетін қауіп-қатерлерді ескере отырып ақпараттарды қорғау жүйелерін жобалауды тиімді жүзеге асыруға мүмкіндік береді.

Поступила 26.02.2015 г.