

ISSN 1991-3494

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

Х А Б А Р Ш Ы С Ы

ВЕСТНИК

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

THE BULLETIN

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

1944 ЖЫЛДАН ШЫҒА БАСТАҒАН
ИЗДАЕТСЯ С 1944 ГОДА
PUBLISHED SINCE 1944

2

АЛМАТЫ
АЛМАТЫ
ALMATY

2015

НАУРЫЗ
МАРТ
MARCH

Б а с р е д а к т о р

ҚР ҰҒА академигі

М. Ж. Жұрынов

Р е д а к ц и я а л қ а с ы :

биол. ғ. докторы, проф., ҚР ҰҒА академигі **Айтхожина Н.А.**; тарих ғ. докторы, проф., ҚР ҰҒА академигі **Байпақов К.М.**; биол. ғ. докторы, проф., ҚР ҰҒА академигі **Байтулин И.О.**; биол. ғ. докторы, проф., ҚР ҰҒА академигі **Берсімбаев Р.И.**; хим. ғ. докторы, проф., ҚР ҰҒА академигі **Газалиев А.М.**; а.-ш. ғ. докторы, проф., ҚР ҰҒА академигі **Дүйсенбеков З.Д.**; а.-ш. ғ. докторы, проф., ҚР ҰҒА академигі **Елешев Р.Е.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА академигі **Қалменов Т.Ш.**; фил. ғ. докторы, проф., ҚР ҰҒА академигі **Нысанбаев А.Н.**; экон. ғ. докторы, проф., ҰҒА академигі **Сатубалдин С.С.**; тарих ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Әбжанов Х.М.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Әбішев М.Е.**; техн. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Әбішева З.С.**; техн. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Абсадықов Б.Н.** (бас редактордың орынбасары); а.-ш. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Баймұқанов Д.А.**; тарих ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Байтанаев Б.А.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Давлетов А.Е.**; физ.-мат. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Қалимолдаев М.Н.**; геогр. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Медеу А.**; техн. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Мырхалықов Ж.У.**; биол. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Огарь Н.П.**; техн. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Таткеева Г.Г.**; а.-ш. ғ. докторы, проф., ҚР ҰҒА корр. мүшесі **Үмбетаев И.**

Р е д а к ц и я к е ñ е с і :

Ресей ҒА академигі **Велихов Е.П.** (Ресей); Әзірбайжан ҰҒА академигі **Гашимзаде Ф.** (Әзірбайжан); Украинаның ҰҒА академигі **Гончарук В.В.** (Украина); Армения Республикасының ҰҒА академигі **Джрбашян Р.Т.** (Армения); Ресей ҒА академигі **Лаверов Н.П.** (Ресей); Молдова Республикасының ҰҒА академигі **Москаленко С.** (Молдова); Молдова Республикасының ҰҒА академигі **Рудик В.** (Молдова); Армения Республикасының ҰҒА академигі **Сагян А.С.** (Армения); Молдова Республикасының ҰҒА академигі **Тодераш И.** (Молдова); Тәжікстан Республикасының ҰҒА академигі **Якубова М.М.** (Тәжікстан); Молдова Республикасының ҰҒА корр. мүшесі **Лупашку Ф.** (Молдова); техн. ғ. докторы, профессор **Абиев Р.Ш.** (Ресей); техн. ғ. докторы, профессор **Аврамов К.В.** (Украина); мед. ғ. докторы, профессор **Юрген Аппель** (Германия); мед. ғ. докторы, профессор **Иозеф Банас** (Польша); техн. ғ. докторы, профессор **Гарабаджиу** (Ресей); доктор PhD, профессор **Ивахненко О.П.** (Ұлыбритания); хим. ғ. докторы, профессор **Изабелла Новак** (Польша); хим. ғ. докторы, профессор **Полещук О.Х.** (Ресей); хим. ғ. докторы, профессор **Поняев А.И.** (Ресей); профессор **Мохд Хасан Селамат** (Малайзия); техн. ғ. докторы, профессор **Хрипунов Г.С.** (Украина)

Главный редактор

академик НАН РК

М. Ж. Журинов

Редакционная коллегия:

доктор биол. наук, проф., академик НАН РК **Н.А. Айтхожина**; доктор ист. наук, проф., академик НАН РК **К.М. Байпаков**; доктор биол. наук, проф., академик НАН РК **И.О. Байгулин**; доктор биол. наук, проф., академик НАН РК **Р.И. Берсимбаев**; доктор хим. наук, проф., академик НАН РК **А.М. Газалиев**; доктор с.-х. наук, проф., академик НАН РК **З.Д. Дюсенбеков**; доктор сельскохоз. наук, проф., академик НАН РК **Р.Е. Елешев**; доктор физ.-мат. наук, проф., академик НАН РК **Т.Ш. Кальменов**; доктор фил. наук, проф., академик НАН РК **А.Н. Нысанбаев**; доктор экон. наук, проф., академик НАН РК **С.С. Сатубалдин**; доктор ист. наук, проф., чл.-корр. НАН РК **Х.М. Абжанов**; доктор физ.-мат. наук, проф., чл.-корр. НАН РК **М.Е. Абишев**; доктор техн. наук, проф., чл.-корр. НАН РК **З.С. Абишева**; доктор техн. наук, проф., чл.-корр. НАН РК **Б.Н. Абсадыков** (заместитель главного редактора); доктор с.-х. наук, проф., чл.-корр. НАН РК **Д.А. Баймуканов**; доктор ист. наук, проф., чл.-корр. НАН РК **Б.А. Байтанаев**; доктор физ.-мат. наук, проф., чл.-корр. НАН РК **А.Е. Давлетов**; доктор физ.-мат. наук, проф., чл.-корр. НАН РК **М.Н. Калимолдаев**; доктор геогр. наук, проф., чл.-корр. НАН РК **А. Медеу**; доктор техн. наук, проф., чл.-корр. НАН РК **Ж.У. Мырхалыков**; доктор биол. наук, проф., чл.-корр. НАН РК **Н.П. Огарь**; доктор техн. наук, проф., чл.-корр. НАН РК **Г.Г. Таткеева**; доктор сельскохоз. наук, проф., чл.-корр. НАН РК **И. Умбетаев**

Редакционный совет:

академик РАН **Е.П. Велихов** (Россия); академик НАН Азербайджанской Республики **Ф. Гашимзаде** (Азербайджан); академик НАН Украины **В.В. Гончарук** (Украина); академик НАН Республики Армения **Р.Т. Джрбашян** (Армения); академик РАН **Н.П. Лаверов** (Россия); академик НАН Республики Молдова **С. Москаленко** (Молдова); академик НАН Республики Молдова **В. Рудик** (Молдова); академик НАН Республики Армения **А.С. Сагиян** (Армения); академик НАН Республики Молдова **И. Тодераш** (Молдова); академик НАН Республики Таджикистан **М.М. Якубова** (Таджикистан); член-корреспондент НАН Республики Молдова **Ф. Лупашку** (Молдова); д.т.н., профессор **Р.Ш. Абиев** (Россия); д.т.н., профессор **К.В. Аврамов** (Украина); д.м.н., профессор **Юрген Аппель** (Германия); д.м.н., профессор **Иозеф Банас** (Польша); д.т.н., профессор **А.В. Гарабаджиу** (Россия); доктор PhD, профессор **О.П. Ивахненко** (Великобритания); д.х.н., профессор **Изабелла Новак** (Польша); д.х.н., профессор **О.Х. Полещук** (Россия); д.х.н., профессор **А.И. Поняев** (Россия); профессор **Мохд Хасан Селамат** (Малайзия); д.т.н., профессор **Г.С. Хрипунов** (Украина)

«Вестник Национальной академии наук Республики Казахстан». ISSN 1991-3494

Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы)

Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан №5551-Ж, выданное 01.06.2006 г.

Периодичность: 6 раз в год

Тираж: 2000 экземпляров

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел. 272-13-19, 272-13-18.

www: nauka-nanrk.kz, bulletin-science.kz

© Национальная академия наук Республики Казахстан, 2015

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75

Editor in chief

M. Zh. Zhurinov,
academician of NAS RK

Editorial board:

N.A. Aitkhozhina, dr. biol. sc., prof., academician of NAS RK; **K.M. Baipakov**, dr. hist. sc., prof., academician of NAS RK; **I.O. Baitulin**, dr. biol. sc., prof., academician of NAS RK; **R.I. Bersimbayev**, dr. biol. sc., prof., academician of NAS RK; **A.M. Gazaliyev**, dr. chem. sc., prof., academician of NAS RK; **Z.D. Dyusenbekov**, dr. agr. sc., prof., academician of NAS RK; **R.Ye. Yeleshev**, dr. agr. sc., prof., academician of NAS RK; **T.Sh. Kalmenov**, dr. phys. math. sc., prof., academician of NAS RK; **A.N. Nysanbayev**, dr. phil. sc., prof., academician of NAS RK; **S.S. Satubaldin**, dr. econ. sc., prof., academician of NAS RK; **Kh.M. Abzhanov**, dr. hist. sc., prof., corr. member of NAS RK; **M.Ye. Abishev**, dr. phys. math. sc., prof., corr. member of NAS RK; **Z.S. Abisheva**, dr. eng. sc., prof., corr. member of NAS RK; **B.N. Absadykov**, dr. eng. sc., prof., corr. member of NAS RK (deputy editor); **D.A. Baimukanov**, dr. agr. sc., prof., corr. member of NAS RK; **B.A. Baytanayev**, dr. hist. sc., prof., corr. member of NAS RK; **A.Ye. Davletov**, dr. phys. math. sc., prof., corr. member of NAS RK; **M.N. Kalimoldayev**, dr. phys. math. sc., prof., corr. member of NAS RK; **A. Medeu**, dr. geogr. sc., prof., corr. member of NAS RK; **Zh.U. Myrkhalykov**, dr. eng. sc., prof., corr. member of NAS RK; **N.P. Ogar**, dr. biol. sc., prof., corr. member of NAS RK; **G.G. Tatkeeva**, dr. eng. sc., prof., corr. member of NAS RK; **I. Umbetayev**, dr. agr. sc., prof., corr. member of NAS RK

Editorial staff:

E.P. Velikhov, RAS academician (Russia); **F. Gashimzade**, NAS Azerbaijan academician (Azerbaijan); **V.V. Goncharuk**, NAS Ukraine academician (Ukraine); **R.T. Dzhrbashian**, NAS Armenia academician (Armenia); **N.P. Laverov**, RAS academician (Russia); **S.Moskalenko**, NAS Moldova academician (Moldova); **V. Rudic**, NAS Moldova academician (Moldova); **A.S. Sagiyan**, NAS Armenia academician (Armenia); **I. Toderas**, NAS Moldova academician (Moldova); **M. Yakubova**, NAS Tajikistan academician (Tajikistan); **F. Lupaşcu**, NAS Moldova corr. member (Moldova); **R.Sh. Abiyev**, dr.eng.sc., prof. (Russia); **K.V. Avramov**, dr.eng.sc., prof. (Ukraine); **Jürgen Appel**, dr.med.sc., prof. (Germany); **Joseph Banas**, dr.med.sc., prof. (Poland); **A.V. Garabadzhiu**, dr.eng.sc., prof. (Russia); **O.P. Ivakhnenko**, PhD, prof. (UK); **Isabella Nowak**, dr.chem.sc., prof. (Poland); **O.Kh. Poleshchuk**, chem.sc., prof. (Russia); **A.I. Ponyaev**, dr.chem.sc., prof. (Russia); **Mohd Hassan Selamat**, prof. (Malaysia); **G.S. Khripunov**, dr.eng.sc., prof. (Ukraine)

Bulletin of the National Academy of Sciences of the Republic of Kazakhstan.
ISSN 1991-3494

Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)

The certificate of registration of a periodic printed publication in the Committee of Information and Archives of the Ministry of Culture and Information of the Republic of Kazakhstan N 5551-Ж, issued 01.06.2006

Periodicity: 6 times a year

Circulation: 2000 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,
<http://nauka-nanrk.kz/>, <http://bulletin-science.kz>

© National Academy of Sciences of the Republic of Kazakhstan, 2015

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

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, Zhmagulova 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. Шангытбаева¹, Н. П. Карпинский², А. А. Жумагулова³

¹ Казахский национальный технический университет им. К. И. Сатпаева, Алматы, Казахстан;

² Бельско-Бяльская техническо-гуманитарная академия, Бельско-Бяла, 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.

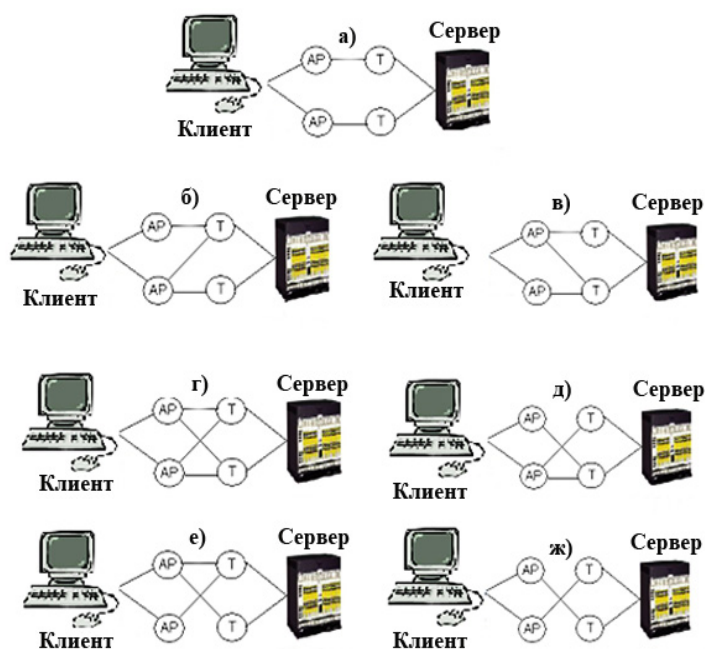


Рисунок 1 – Модель коммуникации клиент – сервер: AP – точка доступа, Т – точка назначения

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:

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

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

Аналогичным образом находим количественные показатели различного вида атак для клиент – серверных моделей типа б), с), d), e), f) и г).

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

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

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

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

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):

$$K_e = \frac{n_3}{n_e}, \quad (5)$$

где n_3 – число связей, n_e – число компонентов.

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

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

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. [Электронный 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. – 20116. – 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 АӘІСТЕРІ**

Г. А. Шаңғытбаева¹, Н. П. Карпинский², А. А. Жұмағұлова³

¹ Қ. И. Сәтпаев атындағы Қазақ ұлттық техникалық университеті, Алматы, Қазақстан;

² Бельско-Бяльская технико-гуманитарлық академиясы, Бельско-Бяля, 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 коэффициенттер әдісі негізіндегі шабуыл түрлеріне арналған сызықты түрдегі қалыптасқан үлгілері беріліп отыр. Берілген көрсеткіштер мен коэффициенттердің 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.

Publication Ethics and Publication Malpractice in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see <http://www.elsevier.com/publishingethics> and <http://www.elsevier.com/journal-authors/ethics>.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see <http://www.elsevier.com/postingpolicy>), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service <http://www.elsevier.com/editors/plagdetect>.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www.nauka-nanrk.kz

bulletin-science.kz

Редакторы *М. С. Ахметова, Д. С. Аленов, Т. А. Апендиев*
Верстка на компьютере *Д. Н. Калкабековой*

Подписано в печать 14.04.2015.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
18,9 п.л. Тираж 2000. Заказ 2.