ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2025»

PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2025»

2025
Астана

УДК 001(06)
ББК 72я631
F96

«ǴYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың XX Халықаралық ғылыми конференциясы = XX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2025» = The XX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2025». – Астана: – 3813 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-08-5373-7

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.В сборник вошли доклады студентов, магистрантов, докторантов имолодыхученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2025

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММ УНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.2

Интеллектуальные информационные системы

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған аі дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «IOT Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

СЕКЦИЯ 3
ЕСТЕСТВЕННЫЕ НАУКИ

	коэффициенттері өзгеруі мүмкін.		
DWT (дискретті вейвлет түрлендіру) әдісі	Суреттегі жиілік компоненттерін вейвлет түрлендіру арқылы талдайды. Әртүрлі рұқсат деңгейлеріндегі ендірілген деректерді зерттеуге мүмкіндік береді.	Вейвлет түрлендірілген суреттер үшін тиімді.	Күрделі есептеулерді талап етеді.

1-кесте. Стегоанализ әдістерінің кестесі

Осылайша, фотореалистік кескіндерде статистикалық әдістерді қолданудың алдын-ала міндеті туындайды, бұл кескіннің барлық пикселдерінен таңдау кезеңі, көрпе салуды анықтау үшін мүмкін болатын көптеген пикселдер.

Қорытынды

Стегоанализ – цифрлық кескіндердегі жасырын ақпаратты табу мен зерттеуге арналған маңызды сала. Оның ішінде статистикалық стегоанализ ерекше орны бар, себебі ол контейнер-суреттің статистикалық параметрлерін табиғи суреттермен салыстырып жасырын ақпараттың бар немесе жоқ екенін анықтайды. Бұл әдістер пиксельдік мәндердің таралуы, бит деңгейіндегі өзгерістер, дискретті түрлендіру коэффициенттері және түстердің таралу ерекшеліктерін талдау негізінде жұмыс істейді.

Заманауи стеганографиялық әдістер жасырын деректерді тиімді жасыруға мүмкіндік береді, бірақ статистикалық стегоанализ құралдары олардың көпшілігін таба алады. Дегенмен, стегоанализдің тиімділігі енгізілген деректердің көлеміне, контейнердің құрылымына және қолданылған стеганографиялық әдіске байланысты өзгеріп отырады. Сондықтан, қазіргі кезде стеганографиялық және стегоаналитикалық әдістерді зерттеу ақпараттық қауіпсіздік саласындағы өзекті мәселелердің бірі болып келеді.

Қолданылған әдебиеттер тізімі

1. Universal statistical steganalytic method.- 2017. [Электрондық ресурс]. URL: https://sciendo.com/article/10.1515/jee-2017-0016

2. Сегментация изображений как предварительный этап статистического стеганоанализа.- 2015. [Электрондық ресурс]. URL: https://cyberleninka.ru/article/n/segmentatsiya-izobrazheniy-kak-predvaritelnyy-etap-statisticheskogo-steganoanaliza

УДК 004.72.

DDOS-ШАБУЫЛДАРДЫҢ ЖАҢА БУЫНЫ

Оралбеков Ерсұлтан Аятұлы
eraoralbekovkz@gmail.com
Л. Н. Гумилев атындағы Еуразия ұлттық университетінің 3 курс студенті,
Астана, Қазақстан
Ғылыми жетекші – Казиева Назым Магидулловна

Аннотация. Мақалада DDoS (Distributed Denial of Service) шабуылдарының қазіргі жағдайы, олардың дамуы және заманауи қорғаныс әдістері қарастырылады. DDoS шабуылдарының негізгі түрлері, ықтимал нысандары және олардың жұмыс істеу принциптері

талқыланады. Сонымен қатар, жасанды интеллектің (AI) шабуылдарды күшейтудегі және оларға қарсы тұрудағы рөліне баса назар аударылады. Зерттеуде желілік деңгейде қорғану, бұлттық қорғау жүйелері және AI негізіндегі қорғаныс секілді стратегиялар талданады. Мақала киберқауіпсіздік саласындағы жаңа қауіптерге қарсы тиімді қорғаныс шараларын жетілдіруге бағытталған.

Кілт сөздер: DDoS, кибершабуыл, жасанды интеллект, киберқауіпсіздік, қорғаныс әдістері, желілік қауіпсіздік, трафик сүзгілеу, бұлттық қорғау, AI талдау, ботнеттер, Ransom DDoS, аномалияларды анықтау.

Қызмет көрсетуден бас тарту (DoS) шабуылдары – бұл шабуылдаушылардың белгілі бір жүйенің немесе желінің ресурстарын шамадан тыс жүктеп, оны заңды пайдаланушылар үшін қолжетімсіз етуге бағытталған әрекеттері. Ал таратылған қызмет көрсетуден бас тарту (DDoS) шабуылдары бірнеше бұзылған жүйелердің ресурстарын үйлестірілген түрде пайдалану арқылы мақсатты жүйенің жұмысын бұғаттайды. DoS және DDoS шабуылдары желі инфрақұрылымын шамадан тыс жүктеу арқылы компаниялар мен ұйымдарға айтарлықтай зиян келтіруі мүмкін. Мұндай шабуылдарды киберқылмыскерлер, хактивистер немесе қаржылық пайда табу мақсаттарды көздейтін тұлғалар жүзеге асыруы мүмкін[1].

DoS және DDoS шабуылдары бастапқыда қауіпсіздікке емес, функционалдылыққа негізделген интернет архитектурасының осалдығын пайдаланады. Жүйенің ішкі қауіпсіздігі қаншалықты мықты болса да, оның интернет желісіне тәуелділігі оны киберқауіптерге осал етеді. Интернеттің өсуі және DoS/DDoS шабуылдарының қаупі интернет пайда болғаннан бері артып келеді, бұл желіге қосыла алатын құрылғылар санының артуына әкелді [2]. Технологияның дамуы және оның қолжетімділігі адамдардың бір немесе бірнеше желілік құрылғылар арқылы интернетке қосылуын жеңілдетті. Зиянды желілік трафик тек дербес компьютерлерден ғана емес, сонымен қатар интернет заттар (IoT) құрылғыларынан да таралуы мүмкін.

DDoS шабуылдары көбінесе бот-желілерді (botnet) пайдаланады, яғни зиянды бағдарламалармен жұқтырылған құрылғылар тобын. Бұл бот-желілер басқарушы орталық (контроллер) арқылы нақты шабуылшының бұйрығымен жұмыс істейді. Мұндай шабуылдардың құрылымы шабуылдаушы, боттар (зақымданған құрылғылар), басқарушы сервер және құрбаннан (нысана жүйе) тұрады.

DDoS-шабуылдарды және олардан қорғану әдістерін зерттеу үшін әртүрлі көздер мен технологиялар қолданылды. Зерттеу үшін пайдаланылған негізгі материалдар мен әдістер:

Ғылыми мақалалар мен зерттеулер – беделді киберқауіпсіздік институттары мен университеттерінің жарияланымдары;

Киберқауіпсіздік есептері – Google, Cloudflare, Qrator, Microsoft және басқа да ірі IT-компаниялардың жыл сайынғы қауіпсіздік есептері;

Шынайы оқиғалар – соңғы жылдары тіркелген ауқымды DDoS-шабуылдар, олардың себептері мен салдары;

Киберқауіпсіздік мамандарының пікірлері – индустрия сарапшыларының сұхбаттары мен баяндамалары;

Тәжірибелік зерттеулер-симуляциялық DDoS-шабуылдарды талдау және олардан қорғану механизмдерін тексеру.

Мақалада DDoS-шабуылдардың түрлері, олардың әсер ету механизмдері, сондай-ақ жасанды интеллекттің (AI) рөлі негізгі зерттеу нысандары болып табылады. Олар:

1. DDoS-шабуылдардың негізгі түрлері
2. DDoS-шабуылдардың ықтимал нысандары
3. Жасанды интеллект пен машиналық оқытуда (AI & ML) қолданылатын нысандар
4. DDoS-шабуылдардан қорғану стратегиялары

Зерттеу барысында келесі қорғаныс әдістері қарастырылды:

- Желілік деңгейде қорғану: Желілік трафикті сүзгілеу, географиялық IP-блоктау, желіаралық экран (Firewall) қолдану.

- Бұлттық қорғау жүйелері: Cloudflare, Akamai, Imperva секілді сервистерді пайдалану.

- Жасанды интеллект негізіндегі қорғаныс: AI-талдағыштар көмегімен шабуылдарды алдын ала болжау және зиянды трафикті автоматты түрде бұғаттау.

Инфрақұрылымдық қабат шабуылдары (3,4-қабаттар):

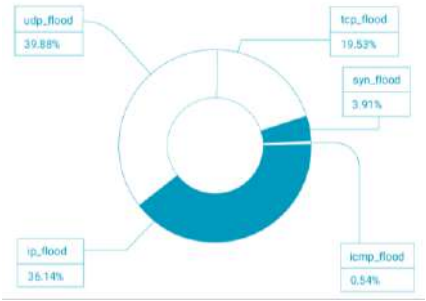
Шабуылдаушы желінің сыйымдылығын басып кететін немесе брандмауэр, IPS, жүктеме теңгергіші сияқты жүйелік ресурстарды байлап тастайтын үлкен көлемдегі трафикті жасауды көздейді. Бұл шабуылдарды анықтау оңай және шабуыл трафигін сүзу немесе сіңіру үшін кіріс трафигінен жылдамырақ ауқымды кеңейту арқылы азайтуға болады. Ең көп таралған шабуылдар:

SYN Flood Шабуылы үш жақты қол алысуды (SYN, SYN-ACK, ACK) аяқтау үшін пакеттер қолданылады. SYN топан шабуылында зиянды клиент ACK-сіз көптеген SYN пакеттерін жібереді, ал сервер осы пакетті күтіп тұрғанда қосылым ашық қалып, заңды қосылымдарға ресурс қалмайды.

ICMP (Ping) Flood шабуылы: ICMP (Internet Control Message Protocol) хаттамасы желі құрылғыларының бір-бірімен байланысын тексеру үшін қолданылады. ICMP топан шабуылында шабуылдаушы нысанға көп мөлшерде ICMP сұрау пакеттерін (ping) жібереді, бұл нысанның ресурстарын (әсіресе, желілік жолақты) сарқып, заңды трафиктің өтуіне кедергі келтіреді. Кейбір жағдайларда, шабуылдаушылар "smurf attack" деп аталатын әдісті қолданып, жалған көз IP-мекенжайымен ICMP сұрауларын тарату желілеріне жібереді, бұл нысанға күшейтілген шабуыл трафигін тудырады [3].

Қосымша қабат шабуылдары (6,7-қабаттар):

HTTP Flood Шабуылы: Шабуылдаушы HTTP сұрауларын нағыз пайдаланушы сияқты жібереді немесе қосымшамен адамның өзара әрекеттесуін имитациялайды, бұл сұраныс жылдамдығын шектеу сияқты жалпы жеңілдету әдістерін қолдану қиындығын арттыруы мүмкін. DDoS шабуылдарының жаңа сериясы секундына 398 миллион сұранысқа (rps) жетіп, бірнеше Интернет инфрақұрылым компанияларына әсер еткен ағынды мультиплекстеуге негізделген HTTP/2 "Жылдам қайтару" атты жаңа әдіске сүйенді. Салыстыру үшін, өткен жылы тіркелген ең үлкен DDoS шабуылы секундына 46 миллион сұранысқа жеткен. Ауқымды түсіну үшін, осы екі минуттық шабуыл Wikipedia 2023 жылдың қыркүйек айында хабарлаған мақалаларды қараудың жалпы санынан да көп сұраныстар жасады [4]. "Таза" векторлар бойынша таралуы аналитикалық деректер негізінде 1-суретте көрсетілген. 2024 жылы пакеттерді беру жылдамдығы бойынша шабуылдардың интенсивтілігі және максималды битрейті 1-кестеде көрсетілген.[5]



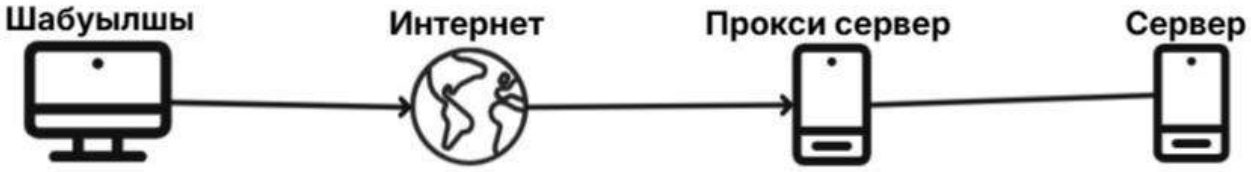
1-сурет. 2024 жылы "таза" векторлар бойынша бөлу [5].

1-кесте. DDoS-шабуылдарының қарқындылығы

Шабуыл түрі	Бит жылдамдығы (Гбит/с)	Жылдамдық (Mpps)
TCP flood	1140	179
UDP flood	882	152
IP fragmented flood	329	151
ICMP flood	113	153
SYN flood	91	64

Кіріс пакеттерін сүзу - Anti-DDoS-тың кеңінен қолданылатын әдістерінің бірі. Мысалы, тек ағымдағы TCP/IP қосылымы аясында жіберілген пакеттерге рұқсат беру. Кейбір флудтарды (мысалы, HTTP) клиентті аутентификациялау арқылы тоқтатуға болады, мысалы, Captcha бағдарламалық жасақтамасын пайдалану арқылы

Кері прокси-сервер (reverse proxy)



1-сурет. Кері прокси сұлбасы

Кері прокси-сервер (reverse proxy) – Anti-DDoS қорғанысында кеңінен қолданылатын тиімді әдістердің бірі. Ол кіру сұраныстарын өңдеп, шынайы серверге тек заңды трафикті жеткізу арқылы жүйенің тұрақтылығын қамтамасыз етеді.

Мысалы, кері прокси-сервер тек ағымдағы TCP/IP қосылымы аясында жіберілген пакеттерге рұқсат беріп, күдікті сұраныстарды сүзгіден өткізе алады. Сонымен қатар, белгілі бір флуд түрлерін (мысалы, HTTP flood) тоқтату үшін клиентті аутентификациялау әдістері қолданылады. Бұған Captcha бағдарламалық жасақтамасы немесе Rate Limiting (сұраныс жылдамдығын шектеу) сияқты механизмдер кіреді.

4-сурет. ICMP-флуд сұлбасы

Үшінші деңгейлі көлемді шабуыл кезінде шабуылдаушы, өз компьютерін немесе ботнетті пайдаланып, ICMP хаттамасынан ECHO сұрауларының көп санын жібереді. Шабуылға ұшыраған машина шексіз эхо-сұрауларға (жолақтың өткізу қабілеттілігі мен сервердің тиімділігін тексеру үшін әдетте қолданылатын шағын пакеттер) жауап берумен айналысады және белгілі бір сәтте оның барлық ресурстары сарқылады және іс жүзінде ол бұдан әрі шынайы пайдаланушыларға қызмет көрсете алмайды.

5-сурет. SYN-флуд сұлбасы

SYN flood және ACK flood - төртінші деңгейлі шабуылдар, яғни тасымалдау деңгейіндегі шабуылдар. Олар шабуылға ұшыраған серверге пакеттерді жіберу арқылы орындалады.

SYN (синхрондау) пакеті TCP/IP моделі аясында деректер алмасуды іске қосады. Алушы SYN-ACK (растау) жауабын береді, оған жіберуші ACK жауабын қайтарады.

Шабуылдаушы әдетте кездейсоқ жалған көз бояушы пакеттерді пайдаланады және кері байланыс алмайды, ал құрбан SYN жауабын қайтару үшін өз ресурстарын пайдаланады.

Қосымша деңгейіндегі шабуылдар OSI моделінің жоғарғы (алтыншы және жетінші) деңгейлеріндегі бағдарламалық жасақтаманың осалдықтарын пайдаланады. Бұл бағдарламалық жасақтама қателіктер тудыруы немесе құрбанды зиянды бағдарламалық жасақтама жұқтыруы мүмкін.

6-сурет. HTTP-флуд шабуылының сұлбасы

Бұл көлемді шабуыл жетінші деңгейде болады және ботнет арқылы орындалады. Осының барысында сервер HTTP командаларымен – GET және POST – толтырылып, оның ресурстарын тиімді түрде сарқады. Бұл типтегі шабуылдар бұрмаланған пакеттерді немесе күшейту әдістерін қолданбайды, олар интернет-трафиктің аз көлемін жасайды, сондықтан оларды тоқтату үшін жақсырақ түсіну қажет.

"Slowloris" атауы баяу азиялық сүтқоректінің атынан шыққан, ол тек HTTP тақырыптарын жібереді. Баяу және төмен шабуыл сияқты, ол сервер ресурстарын тауысып, басқа пайдаланушыларға қызмет көрсетуді қиындатады немесе мүлдем мүмкін етпейді.

Осы мақалада зерттеу барысында DDoS-шабуылдардың негізгі түрлері көрсетілді. Олардың ішінде желі трафигін шамадан тыс жүктеу арқылы сервер ресурстарын сарқытатын объёмдік (Volume-based) шабуылдар (UDP Flood, ICMP Flood, DNS Amplification), желілік хаттамалардың осалдықтарын пайдалану арқылы серверлердің жұмысын бұзатын протоколдық (Protocol-based) шабуылдар (SYN Flood, ACK Flood, Smurf атакасы) және веб-сайттар мен API-ларды шамадан тыс сұраныстармен жүктеп, оларды жұмыс істемейтін күйге келтіретін қолданбалы деңгейдегі (Application Layer attacks) шабуылдар (HTTP Flood, Slowloris, API DDoS) бар. Әрбір шабуыл түрінің өзіндік ерекшеліктері мен зардаптары бар, сондықтан олармен күресу үшін әртүрлі стратегиялар қолданылады.

Зерттеу DDoS-шабуылдардың ықтимал нысандарын анықтады. Оларға корпоративтік IT-инфрақұрылымдар, бұлттық сервистер, қаржы институттары, интернет-провайдерлер, үкіметтік және мемлекеттік серверлер жатады. Аталған нысандарға шабуыл жасаудың мақсаты – қызметті тоқтату, қаржылық шығындарға ұшырату, саяси тұрақсыздық тудыру және т.б. Нысандардың әртүрлілігіне байланысты қорғану шаралары да әр түрлі болуы мүмкін.

DDoS-шабуылдардан қорғану стратегияларын қарастыра отырып, желілік деңгейде қорғану (желілік трафикті сүзгілеу, географиялық IP-блоктау, желіаралық экран (Firewall) қолдану), бұлттық қорғау жүйелерін (Cloudflare, Akamai, Imperva секілді сервистерді пайдалану) және жасанды интеллект негізіндегі қорғанысты (AI-талдағыштар көмегімен шабуылдарды алдын ала болжау және зиянды трафикті автоматты түрде бұғаттау) анықтадық. Қорғану әдістерін тиімді қолдану үшін әрқайсысының артықшылықтары мен кемшіліктерін, сондай-ақ шабуылдың түрі мен нысанын ескеру қажет.

Алдағы уақытта заманауи күрделі шабуылдарды (IoT құрылғылары арқылы ұйымдастырылатын ботнеттер, Ransom DDoS (RDDoS) және бұлттық сервистерге бағытталған шабуылдар) және жасанды интеллект пен машиналық оқытудың (AI & ML) DDoS-шабуылдарда және қорғану жүйелерінде қолданылуын тереңірек зерттеу жұмыстары жүргізіледі. Бұл салалардағы жаңалықтар мен технологиялардың дамуына байланысты, қорғану стратегиялары да үнемі жетілдірілуді қажет етеді.

Менің ойымша, DDoS шабуылдарына қарсы қорғаныс тек техникалық шешімдермен шектелмеуі керек. Ол ұйымның қауіпсіздік мәдениетін қалыптастыруды, қызметкерлердің хабардарлығын арттыруды және жаңа қауіптерге бейімделу қабілетін қамтуы қажет. Сонымен қатар, AI/ML технологияларын пайдалану арқылы шабуылдарды алдын ала анықтау мен болжау – ең тиімді әдістердің бірі. Ұйымдар мен компаниялар тұрақты қауіпсіздікті қамтамасыз ету үшін көп деңгейлі қорғаныс жүйесін енгізіп, трафикті интеллектуалды сүзгілеп, желіні үздіксіз мониторингтен өткізуі керек. Болашақта DDoS шабуылдарына қарсы қорғаныс жүйелерін автоматтандыру мен жетілдіру үшін жасанды интеллект технологияларына ерекше көңіл бөлу қажет деп есептеймін.

Қолданылған әдебиеттер тізімі

1. Kamila Bekshentayeva, Detection of Denial of Service Attacks Using Echo State Networks, Simon Fraser University Summer 2021

2. Eirik Bårli, DDoS and DoS Mitigation Using a Variational Autoencode, UNIVERSITY OF OSLO Spring 2019

3. Toony Mustafa for AWS MENA Community https://dev.to/awsmenacommunity/aws-best-practices-for-ddos-summary-50do Oct 18, 2021

4. Emil Kiner, Tim April Google mitigated the largest DDoS attack to date, peaking above 398 million rps https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps/ October 11, 2023

5. **DDoS-атаки, боты и BGP-инциденты в 2024 году: статистика и тренды** https://blog.qrator.net/ru/ddos-boty-i-bgp-incidenty-v-2024-godu-statistika-i_210/

6. Титов Ф. М. Исследование методов защиты от атаки ddos. 2021

УДК 004.056

БҰЛТТЫ ТЕХНОЛОГИЯЛАРДЫ ПАЙДАЛАНУ КЕЗІНДЕГІ ТӘУЕКЕЛДЕР МЕН ҚАУІПСІЗДІК ШАРАЛАРЫН ЗЕРТТЕУ

Рамазанова Ж, Нұрлан А, Жайсанбаева А
ramazanovazamila8@gmail.com, nurlanaisulu19@gmail.com, j.arujan04@gmail.com

Л.Н. Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің Ақпараттық қауіпсіздік кафедрасының 3-курс студенттері, Астана, Қазақстан
Ғылыми жетекші – Казиева Н.М.

Аңдатпа. Қазіргі таңда бұлтты технологиялар – интернет желісі арқылы есептеу ресурстары, деректер және бағдарламалық құралдарға ыңғайлы қолжетімділікті қамтамасыз ететін заманауи шешімдердің бірі ретінде кеңінен таралды. Олар ақпаратты сақтауды, өңдеуді және таратуды жеңілдетіп, білім беру мекемелері мен жеке тұлғалар үшін айтарлықтай экономикалық және операциялық тиімділік әкеледі. Алайда, бұл технологияларды қолдану барысында деректердің қауіпсіздігі, рұқсатсыз қолжетімділік және кибершабуыл секілді қауіптер де өзекті мәселеге айналады. Осы зерттеуде біз бұлтты сервистердің әртүрлі түрлерін және олардың қолдану салаларын жан-жақты талдаймыз, сонымен қатар Microsoft Azure платформасында енгізілген шифрлау, көпфакторлы аутентификация және мониторинг әдістері негізінде қауіпсіздікті қамтамасыз ету механизмдерін қарастырамыз. Нәтижесінде, сенімді және тұрақты ақпараттық инфрақұрылымды қалыптастыруға бағытталған кешенді қауіпсіздік стратегиялары ұсынылады.

Кілт сөздер: Бұлтты технологиялар, ақпараттық қауіпсіздік, деректерді қорғау, IaaS, PaaS, SaaS, Microsoft Azure, киберқауіпсіздік, қауіпсіздік механизмдері.

Кіріспе. Цифрлық технологиялардың қарқынды дамуы ақпаратты өңдеу, сақтау және таратудың дәстүрлі тәсілдерінен түбегейлі айырмашылықтарға әкелді. Бұл өзгерістердің негізінде жатқан негізгі тенденциялардың бірі – бұлтты сервистердің пайда болуы, олар ұйымдар мен жеке тұлғалар үшін үнемді, икемді және қолжетімді шешімдер ұсынады. Кеңейтілетін мүмкіндіктері мен қолжетімділігі арқасында, бұл технологиялар қазіргі IT саласының жетекші трендтерінің бірі болып саналады. Дегенмен, ақпарат алмасу үрдістерін интернет арқылы жүзеге асыру барысында деректердің құпиялылығы мен бүтіндігіне қауіп төндіретін бірқатар қауіптер орын алады. Осы мақалада біз осындай қауіптердің негіздерін ашып көрсетіп, олардың алдын алу мақсатында Microsoft Azure платформасындағы заманауи қауіпсіздік шаралары – шифрлау, көпфакторлы аутентификация, мониторинг және аудит құралдарын егжей-тегжейлі талқылаймыз [3].

Бұлтты сервис

[1] мақалада көрсетілгендей бұлтты сервис дегеніміз есептеу ресурстарына, бағдарламалық қамтамасыз етуге және ақпаратқа, оларды өңдейтін деректер орталықтарында орналастырылған жүйеге интернет арқылы алыстан қол жеткізуге мүмкіндік беретін