ӘОЖ 004.056

ВЕБ-САЙТТЫ ҚОРҒАУ

Мағауия Әсемгүл
magauiyaasemgul@gmail.com
«Бағдарламалық қамтамасыздандыру» білім бағдарламасының 3 курс студенті
Жоғары инженерлік технологиялық колледжі, Орал қ, Қазақстан Республикасы
Ғылыми жетекшісі – **Қанибаева Ө.Т.**

Аннотация: Мақалада желілік қауіпсіздікті пайдалану және зиянды желімен күресу әдістері туралы айтылады**.**

Кілт сөздер: интернет, брандмауэр,компьютерлік трафик, пакеттік сүзгілер, қол жеткізуді басқару тізімі

Бүгінгі таңда веб-қосымшаларда өңделетін ақпараттың жоғары құны бұзылу қаупімен бірге компаниялардың ақпараттық қауіпсіздігін бұзады. Бұл жағдайда веб-қосымшаларды қорғау үшін не істеу керек деген сұрақ туындайды. Веб-қосымшаның брандмауэрлері сипатталған мәселелердің шешімі болып табылады. Сондай - ақ веб-қосымшаларға (Web Application Firewall (WAF)) арнайы бағытталған қолданбалы деңгейдегі трафикті сүзу құралдары болып табылады. Web Application Firewall қолданбасы дәстүрлі түрде веб-ресурстарды қорғаудың ең тиімді тәсілі болып саналады. Әлемдік нарықтағы негізгі жетекші өнімдерді талдай отырып, әдетте WAF-қа тән қорғаныс механизмдерінің тізімін жасауға болады :

1) хаттаманы тексеру;
2) қолтаңбаны талдау;
3) Машиналық оқыту;

Машиналық оқыту - бұл веб-қосымшаның кіру идентификаторларын арнайы модельге енгізу, содан кейін оған келіп түскен сұраныстарды салыстыру процесі. Теорияда машиналық оқытуға негізделген қорғаныс механизмі өзінің шектеулеріне ие және әрдайым қолданылмаса да, қолтаңбалық талдауды қолдану қажеттілігін жоққа шығарады.

Модельді әзірлеу екі кезеңнен тұрады

Алдын ала өңдеу. Бұл кезең белгілерді алып тастаудан және оларды таңдаудан тұрады.

Белгілерді алу үшін біз екі әдісті салыстырамыз:кейбір сипаттамалық белгілер жиынтығын және n - grams көмегімен автоматты түрде. Бірінші жағдайда келесі белгілер бөлінеді:

1) сұраныстың, жолдың, дәлелдердің және әртүрлі тақырыптардың ұзындығы
2) әдіс идентификаторы (GET/POST);
3) аргументтердегі аргументтердің, әріптердің, сандардың және "арнайы" таңбалардың саны;

Сайт немесе веб – сайт бір немесе бірнеше логикалық байланысты веб-беттер, сондай-ақ сервер мазмұнының орналасқан жері.Сайттарды ақпараттық қауіпсіздіктің ықтимал қауіптерінен қорғау оның иесі үшін маңызды міндет болып табылады, мысалы сайттың қолжетімсіздігі салдарынан әлеуетті клиенттерден пайда алмау, іздеу нәтижелеріндегі сайттың позициясының төмендеуі, ұйымның беделінің төмендеуі және т. б. сияқты салдарлар болуы мүмкін.

Веб-сайттарда келесі қауіп түрлері бар :

• веб-сайттың мазмұнын өзгерту - яғни шабуылдаушының сайтта кез келген ақпаратты орналастыруы;

• шабуылдаушының деректерді, соның ішінде парольдер, клиенттердің мәліметтер базасы туралы ақпаратты жоюы;

• зиянды әрекеттерді тудыруы мүмкін зиянды бағдарламаларды енгізу (мысалы, пайдаланушының жеке деректерін ұрлау, алаяқтық сайтқа бағыттау немесе веб-сайтқа кірушілерді вирустық бағдарламалармен жұқтыру)

• DDOS шабуылы – заңды пайдаланушылардың сайтқа кіруін қиындататын немесе тоқтататын қауіп.

Веб-сайтты қорғау құралдарына мыналар жатады [4]:

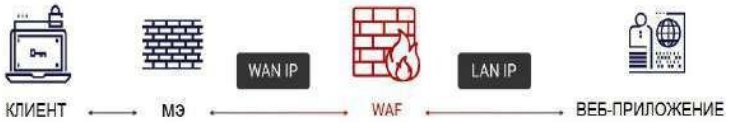
• веб-қосымшалардың брандмауэрі (Web application firewall, WAF)

• вирустарға арналған веб-сайтты талдау құралдары;

• веб-қосымшаларға жүктеме теңестіргіштері;

• веб-қосымшалардың қауіпсіздік сканерлері.

Веб-қосымшалардың брандмауэрінің жұмыс принципі оның негізгі қорғаныс компонентін – машиналық оқытуды қолдануға негізделген, оның көмегімен рұқсат етілген қол жеткізу идентификаторларының "АҚ" тізімі жасалады (қазіргі уақытта веб-сайт қолданбаларда кіру идентификаторының үш түрі қолданылады: HTTP параметрлері, ресурс идентификаторы,сеанс идентификаторы, cookie.



Сурет 1. Веб-қосымшалардың брандмауэрін желіге орналастыру кері прокси режимінде.

Вирустарға арналған веб-сайтты талдау құралдары сайт файлдарында немесе оның кодында зиянды бағдарламалық жасақтаманы (бағдарламалық жасақтаманы) анықтауға мүмкіндік береді. Веб-сайтты зиянды бағдарламаларға тексеру әдістері мен құралдарының ішінде мыналарды бөліп көрсетуге болады: онлайн қызметтер (веб-беттің кодын статикалық және динамикалық талдауды жүзеге асырады), антивирустық бағдарламалар (Жергілікті веб-сервердегі файлдарды, сондай-ақ сайт әкімшілерінің компьютерлерін сканерлеу). Веб-қосымшаларға жүктемені теңестіру жүктемені серверлер, маршрутизаторлар, брандмауэрлер сияқты бірнеше желілік құрылғылар арасында бөлуге мүмкіндік береді. Бұл операция қосымша бағдарламалық жасақтама түрінде немесе жеке серверде жүзеге асырылуы мүмкін. 2-суретте теңдестіруші жүктемені серверлер арасында бөлетін схема көрсетілген. Жүктемені теңестіру сервердің шамадан тыс жүктелуін және нәтижесінде клиенттердің сайтқа кіруіндегі қиындықтарды болдырмайды

Сурет 2. Жүктемені теңестіру арқылы клиенттердің сервер ресурстарына қол жеткізу схемасы.

DDoS шабуылдарынан қорғау үшін екі тәсіл қолданылады – сайт иесі ұйымның инфрақұрылымында бағдарламалық жасақтама кешенін құру немесе арнайы үшінші тарап қызметін таңдау. Бұл жұмыс үшінші тараптың арнайы қызметтерін пайдалану тәсілін қарастырады [12]. 3-суретте үшінші тарап қызметінің DDoS шабуылдарынан қорғау схемасы көрсетілген. Пайдаланушы сайтқа кіруге тырысқанда, одан сұрау қызметті ұсынатын компанияның бұлтына жіберіледі. Бұл бұлтта трафикті тексеру және сүзу жүреді. Егер трафик шабуылдаушы деп танылса, онда ол бұғатталады. Қалғаны пайдаланушыға қажетті сайтты сақтайтын веб-серверге жіберіледі [3].

Сурет 3. Үшінші тарап қызметі арқылы DDoS шабуылдарынан қорғау схемасы.

Веб-қосымшаларды қорғау сканерлері веб-сайтты қорғау құралы ретінде веб-қосымшалардағы осалдықтарды іздеуге арналған [13].

Байес классификаторы, тірек векторлық әдісі және шешім ағаштары сияқты Алгоритмдер жиынтығы салыстырылады. Таңдау "IEEE Conference on Data Mining" (2006) [4] және Oracle өз өнімдерінде не ұсынатынына негізделген. Кесте бағандары-ең жоғары тиімділікті көрсететін жіктеу алгоритмдері. Жолдарда белгілерді таңдаудың алго ритақтары, ал ұяшықтарда дұрыс жіктелген элементтердің пайызы берілген.

Кесте 1 – Ең жоғары тиімділікті көрсететін жіктеу алгоритмдері.

	C4.5	CART	RandomTree
CFS + BestFirst 8 признаков	90.4839 %	90.4839 %	88.4418 %
CFS + Genetic 10 признаков	**91.7187 %**	**91.4042 %**	90.1957 %
CFS + RankSearch 6 признаков	90.312 %	90.3938 %	89.991 %
CFS + LinearForward 8 признаков	90.4839 %	90.4839 %	88.4418 %
ConsistencySub setEval + GreedlyStepwise 16 признаков	93.2924 %	92.8846 %	92.4818 %
ConsistencySubsetEval + LinearForward 16 признаков	93.2924 %	92.8846 %	92.4818 %
FULL (20 признаков)	93.4578 %	92.5424 %	91.5025 %

Зерттеу нәтижелері бойынша бірінші әдіс ең жоғары тиімділікті көрсетті. Бұл жағдайда белгілерді таңдау үшін генетикалық алгоритмнің корреляциямен үйлесуі, C4.5 классификациясы үшін ең қолайлы. Бұл конфигурациямен кеңістіктің өлшемін 2 есе азайтуға болады, ал тану сапасы 2% - дан аз төмендеді. Айта кету керек, белгілерді автоматты түрде алу жағдайында өлшемнің 87 белгіден 40-қа дейін төмендеуі жіктеу сапасын нашарлатып қана қоймайды, сонымен қатар оны арттырады.Web application firewall (WAF) - веб-қосымшаларды әртүрлі шабуылдардан, уақытша бағдарламалық жасақтамадан және осалдықтардан қорғау үшін қолданылатын, қолданба деңгейінде жұмыс істейтін және SQL инъекциясы, кросс - сайт сценарийі (XSS), кросс сияқты көптеген шабуылдардан қорғауды қамтамасыз ететін бағдарламалық жасақтама немесе аппараттық құрал-веб-қосымшалардың осалдығын пайдалануы мүмкін сайтты жалған сұрау (CSRF) және басқа шабуылдар.Рассмның негізгі міндеті Қазіргі уақытта WAF-ті айналып өту үлкен қауіп төндіреді, өйткені ол шабуылдаушыларға веб - қосымшалардың осалдықтарын пайдалануға және оны қорғаудың

осы әдісіне қарамастан құпия ақпаратқа қол жеткізуге мүмкіндік береді. Қарастырылып отырған осалдықтар ұйымдарға айтарлықтай қаржылық және беделді зиян келтіруі мүмкін.

Мәселенің ауырлығын көрсететін кейбір фактілерді келтірейік: - кеңінен қолдану: Gartner сауалнамасына сәйкес, бүкіл әлем бойынша веб-қосымшаларға иелік ететін немесе пайдаланатын ұйымдардың 80%-дан астамы WAF-ты веб-қосымшалардың қауіпсіздігін қамтамасыз ету бөлігі ретінде қолданады. Бұл көптеген ұйымдардың WAF жұмысына байланысты қауіпсіздікті бұзу қаупі бар екенін білдіреді; үнемі дамып келе жатқан айналып өту әдістері: зиянкестер WAF айналып өтудің жаңа әдістерін үнемі дамытады. Мысалы, соңғы жылдары WAF-ты айналып өту үшін JSON және XML негізіндегі пайдалы жүктемелерді пайдаланудың өсуі байқалды. Демек, ұйымдар өздерінің веб-қосымшаларын тиімді қорғау үшін ең жаңа технологиялар мен тенденциялардан хабардар болуы керек; - сәтті айналып өтудің нәтижесінде туындаған күрделі мәселелер: WAF-ті сәтті айналып өту шабуылдаушыларға веб-қосымшалардағы осалдықтарды пайдалануға, құпия ақпаратты ұрлауға және веб - серверде ерікті командаларды орындауға мүмкіндік береді.

Бұл ұйымдарға айтарлықтай қаржылық және беделге нұқсан келтіруі, сондай-ақ клиенттердің сенімін жоғалтуы мүмкін; - кешенді тәсіл: ұйымдар осалдықтарды үнемі бағалау, енуді тестілеу және оқиғаларға жауап беруді жоспарлау сияқты басқа да қауіпті емес шараларды қабылдауы керек. Осылайша, WAF-ті айналып өту бүгінгі күні маңызды мәселе болып табылады, өйткені ол шабуылдаушыға мүмкіндік береді

Осы тәуекелдерге және тиісті осалдықтарға ұшыраған өнімдердің тізімі. Қазіргі уақытта ашық бастапқы коды бар Web application firewall көп. Әдістемеге сүйене отырып, іріктеу жүргізілді, нәтижесінде бүгінгі күнге дейін ең танымал және озық 10 ұсыныс ұсынылды

1- ModSecurity;
2-NAXSI
3- libModSecurity;
4- Comodo WAF;
5- Imperva WAF;
6- F5 BIG-IP Application Security Manager;
7-Barracuda WAF;
8- Cisco Web Security Appliance;
9- Fortinet FortiWeb;
10- Shadow Daemon.

Қолданба деңгейіндегі қорғаныс экрандары (Web Application Firewalls, WAF) веб - қосымшаларға шабуылдарды анықтау және болдырмау үшін қолданылады. Веб-қосымшалардың қауіпсіздігін талдаудың өзекті міндеттерінің бірі-"man in the Browserk (MitB)" моделі аясында веб-қосымшалардың клиенттік жағында қорғаныс экрандарын сәйкестендіру бағдарламалық жасақтамасын әзірлеу. Бұл жұмыс mitb моделі шеңберінде қолданбалы экрандарды сәйкестендіру мүмкіндіктерін зерттеді және осы функционалдылықты жүзеге асыратын BeEF фреймворкіне арналған бағдарламалық модуль іске асырылды. Қорғаныс экрандарын сәйкестендіру әдетте келесі веб-нысандардың қолтаңбалық талдауы негізінде жүзеге асырылады: сеанс идентификаторлары, HTTP тақырыптары, cookie файлдары, жауап кодтары және т.б. қорғаныс экрандарын сәйкестендірудің белгілі құралдары WAFW00F және sqlmap. Serverk-тің HTTP тақырыбының қолтаңбасы негізінде sqlmap-та "Wallarmk "экранын анықтайтын модульге мысал келтірейік:

```
retval = False
for vector in WAF_ATTACK_VECTORS:
    _, headers, _ = get_page(get=vector)
    retval = re.search(r"nginx-wallarm",
                       headers.get(HTTP_HEADER.SERVER, ""),
                       re.I) is not None
    if retval:
```

7 break

Сонымен қатар, бұл құралдарды қолдану шектеулі және веб - қосымшаның клиенттік бөлігін талдау тұрғысынан негізгі болып табылатын MitB моделінде қолдануға болмайды. Қорғаныс экрандарын сәйкестендіру мүмкіндігін қамтамасыз ету үшін mitb моделі белгілі қолтаңба базаларын қолдана отырып, BeEF (Browser Explotation Framework) шеңберіне арналған бағдарламалық модульді енгізді. Әзірленген модуль келесідей жұмыс істейді: ол http сұранысын жібереді, содан кейін веб - қосымшадан алынған жауапты талдайды. ЕО-бұл экранды сәйкестендіру бөлігінде ешқандай нәтиже бермеді, содан кейін жіберу - ется әртүрлі шабуыл векторлары бар HTTP сұрауларының сериясы, ол болған кезде қорғаныс экранының реакциясына әкеледі. Экран қолтаңбасы бар арнайы тақырып қоса алады немесе сеанс идентификаторын орната алады. Егер қауіпсіздік экраны HTTP сұрауларымен анықталмаса, онда веб - қосымшаның жауап кодтары талданады. Қолтаңбаны талдау үшін қорғаныс экрандарының қолтаңбаларының жиынтығы қажет. Оны жасау үшін wafw00f және sqlmap құралдарының қолтаңба базалары пайдаланылды, кейбір қолтаңбаларды авторлар қосты.

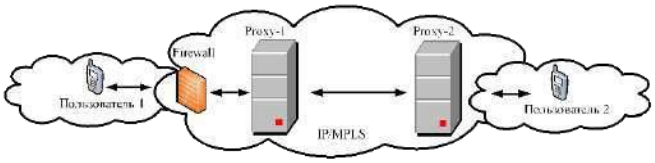
Брандмауэр – бұл АЖ-ға кіретін және АЖ - дан шығатын ақпаратты бақылауды жүзеге асыратын жергілікті (бір компонентті) немесе функционалды таратылатын құрал (кешен) және ақпаратты сүзгілеу арқылы АЖ-ны қорғауды қамтамасыз етеді, яғни оны критерийлер жиынтығы бойынша анықтау және оны тарату туралы шешім қабылдау (бастап) АС. Бүгінгі таңда брандмауэр кез - келген корпоративті желінің қауіпсіздігін қамтамасыз ету жүйесінің ажырамас элементі болып табылады, ол қорғаныс жүйесін құру кезінде қалыптасқан тәжірибе ғана емес, сонымен қатар ақпараттық қауіпсіздік саласындағы нормативтік құжаттардың міндетті талабы болып табылады . Брандмауэрді қолданудағы маңызды міндеттердің бірі-оның саясатының дұрыс конфигурациясы. Брандмауэр саясатының конфигурациясы дегеніміз-желілік трафиктің өту мүмкіндігін анықтайтын сүзу ережелерінің жиынтығы. Жүйенің кірісіне желілік анализатор арқылы жиналған PCAP форматындағы желілік трафик қоқысы немесе брандмауэрдің қосылу нүктесінен өтетін трафиктің үздіксіз ағыны беріледі. Алынған барлық трафик талдау кезеңінен өтеді, оның нәтижелері мәліметтер базасына орналастырылады, онда олар, мысалы, кластерлік талдау әдістері арқылы өңделеді. Кластерлік талдау нәтижелері негізінде формальды ережелер, яғни брандмауэрдің белгілі бір моделіне байланысты емес ережелер жасалады. Құрылған нысандық ережелер трафикті беру бағыты, ис - дәлдік және тағайындалған мекенжайлар мен порттар туралы ақпараттан, сондай-ақ трафикті өткізіп жіберу немесе бұғаттау туралы ақпараттан тұрады. Әрі қарай, формальды ережелер белгілі бір брандмауэр үшін сүзу ережелеріне аударылады. Сүзу ережелерін құрудың ұқсас механизмі "Wireshark" желілік анализаторында бар. Сүзу ережелерін брандмауэрдің әртүрлі модельдері ережелерінің форматтарын қолдана отырып, белгілі бір арнайы пакет үшін жасауға болады. Екінші тәсілдің мысалы ретінде ҮЕҰ - РТК-да әзірленген SPT-2 аралық экранына арналған ережелерді құру моделін келтіруге болады. Ұсынылған әдіс қол жетімділікті ажыратудың бейресми саясаты негізінде сүзу ережелерін қалыптастырудан тұрады. Мұндай саясат бейресми түрде сипатталады, яғни қол жетімділікті бөлу ережелерін айқын көрсететін кестелер түрінде. Әдістің мәні белгілі бір брандмауэр моделіне сәйкес жалпы, бейресми ережелерден олардың егжей-тегжейлі сипаттамасына көшу болып табылады. Ережелер субъект-объект-әрекет моделі түрінде ұсынылады. Субъект-әрекетті (адам немесе процесс) жасайтын адам. Нысан-бұл әрекет орындалатын нәрсе (файл, қалта, ағын). Үшінші тәсіл-автоматтандыру құралдарын қолдану, әдетте графикалық интерфейспен, брандмауэрдің белгілі бір моделі үшін сүзу ережелерін құру-мысалы, "Firewall Builder" бағдарламалық жасақтамасы. Желі элементтері графикалық нысандар түрінде ұсынылады. Мұндай нысандар аппараттық құрылғыларды да ұсынады, олардың үстінен басқару жүзеге асырылады, сонымен қатар барлық ережелер құрылатын әртүрлі элементтер: желілік интерфейстер, протоколдар, порттар және т.б. сүзу ережелерін қалыптастыру қажетті объектілерді қажетті ережелер ұяшықтарына апару арқылы жүзеге асырылады. Осылайша, саясатты құру негізінде сүзу ережелері қалыптасады, мұнда мұндай ережелерді көрсету таңдалған брандмауэр моделіне

арналған ережелер форматына сәйкес келеді. Қарастырылған тәсілдердің артықшылықтары мен кемшіліктері бар. Оларды пайдаланудың негіздемесі желідегі түйіндердің санына және құжаттаманың толықтығына байланысты. Жақсы құжатталған жүйелер үшін "Firewall Builder" - де қолданылатын әдіс қолайлы. Қол жеткізу саясатының құжаттамасы бар жүйелер үшін, бірақ оның тек үстірт сипаттамасы болып табылады, YEҰ - да жасалған әдіс ең қолайлы болып табылады. Трафикті пассивті тыңдауға негізделген әдісті ең перспективалы деп бөлуге болады, өйткені ол сүзу ережелерін құру процесін толығымен автоматтандырады, бұл оны желіге кіруді шектеу ережелерін құруға қатысты біртұтас етеді.

1. Отандық шешімдердің көмегімен сайттың қауіпсіздігін қамтамасыз ету

Қазіргі уақытта сайттарды қорғау үшін шетелдік өндірушілерден әртүрлі құралдар мен қызметтер қолданылады. Сонымен, веб-қосымшалардың брандмауэрі ретінде американдық Imperva компаниясының маңызды веб-қосымшалардың қауіпсіздігін қамтамасыз етуге арналған шешімі танымал-Imperva SecureSphere Web Application Firewall. Оны ауыстыру үшін киберқауіпсіздік қызметтерін ұсынатын және корпоративтік деректерді қорғауға кепілдік беретін аталған мақсаттағы бағдарламалық жасақтаманың көптеген басқа нұсқаларын табуға болады. Веб-қосымшалардың отандық брандмауэрлерінің бірі-Solid Wall WAF. Бұл шешім бағдарламалық жасақтама, виртуалды құрылғы, бағдарламалық-аппараттық кешен түрінде немесе бұлтты қызмет ретінде жүзеге асырылуы мүмкін. Solid Wall WAF-тің Imperva SecureSphere Web Application Firewall-тен артықшылығы-бұл электронды есептеу машиналары мен мәліметтер базасына арналған ресейлік бағдарламалардың бірыңғай тізілімінде. Сондай-ақ, веб-қосымшалардың отандық брандмауэрі-Positive Technologies компаниясының pt Application Firewall шешімі. Оның американдық Imperva SecureSphere Web Application Firewall-дан айырмашылығы келесідей:

- ресейлік кешен электронды есептеу машиналары мен мәліметтер базасына арналған ресейлік бағдарламалардың бірыңғай тізіліміне енгізілген.
- отандық өнімде ретроспективті талдау бар (кіріктірілген динамикалық сканерді қолдана отырып, шабуылды тексеруді жүзеге асыратын трафик журналдарын талдау.



Сурет 4. Ақпарат алмасу.

Веб-сайтты қорғауға арналған импорттық антивирустық санатта киберқауіпсіздік бағдарламалық жасақтамасын жасаушылар арасында әлемдік көшбасшы болып саналатын жапондық Trend Micro компаниясының Trend Micro Web Security деп атауға болады. Алайда, біздің елімізде жоғары деңгейдегі отандық антивирустық бағдарлама бар, онда ең алдымен Kaspersky компаниясы әзірлеген түрлі қаражатты бөлуге болады.

• Шетелдік DDoS шабуылынан қорғау қызметтерінің арасында CloudFlare DDoS protection танымал, ол американдық CloudFlare компаниясында жасалған. Оны ауыстыру үшін Ростелек компаниясы құрған "трафикті бақылау және DDoS – шабуылдардан қорғау қызметі"-DDoS-тан қорғау қызметінің отандық өкілін ұсынуға болады. Бұл қызмет маңызды ақпараттық инфрақұрылым объектілерін, жеке деректерді, Ақпараттық жүйелерді, маңызды объектілердегі технологиялық процесті басқарудың автоматтандырылған жүйелерін және қаржылық операцияларды қорғауға қатысты ресейлік нормативтік құқықтық актілердің талаптарын орындауға мүмкіндік береді. Сонымен қатар, ресейлік компанияның қызметі CloudFlare DDoS protection-тен келесі артықшылықтармен ерекшеленеді:

• Ростелек компаниясы ұсынатын жабдықты ДҚО-ға физикалық көшіруді көздейтін деректер орталығының (ДҚО) DDoS қорғау қызметін пайдалану мүмкіндігі;

• кілттерді ашпай Hyper Text Transfer Protocol Secure (HTTPS) сүзгісінің болуы.

Сондай-ақ, сайттарды DDoS-шабуылдардан қорғау қызметін DDoS-Guard компаниясы әзірлеген "сайтты қорғау және жеделдету" қызметі ұсынады. Бұл қызметтің CloudFlare өнімінен артықшылығы:

1- DDoS компаниясы ұсынатын жабдықтың физикалық қозғалысын көздейтін DDOS DDoS қорғау қызметін пайдалану мүмкіндігі- Guard DOC;

2- кілттерді ашпай https сүзгісінің болуы.

Қолданылған әдебиеттер тізімі:

1. Ковалев А.А. Военная безопасность России и ее информационная политика в эпоху цивилизационных конфликтов: Монография // А.А. Ковалев, В.А. Шамахов. – М.: Риор, 2018, 32 с.

2. Конотопов М.В. Информационная безопасность. Лабораторный практикум // М.В. Конотопов. – М.: КноРус, 2013, 136 с.

3. Кузнецова А.В. Искусственный интеллект и информационная безопасность общества // А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. – М.: Русайнс, 2017, 64 с.

4. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации // А.А. Малюк. – М.: ГЛТ, 2004, 280 с.

5. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: Учебное пособие для вузов // А.А. Малюк. – М.: Горячая линия
- Телеком, 2004, 280 с.

6. Мельников Д.А. Информационная безопасность открытых систем: учебник // Д.А. Мельников. – М.: Флинта, 2013, 448 с.

7. Одинцов А.А. Экономическая и информационная безоп асность предпринимательства // А.А. Одинцов. – М.: Academia, 2004, 384 с.

8. Партыка Т.Л. Информационная безопасность: Учебное пособие // Т.Л. Партыка, И.И. Попов. – М.: Форум, 2018, 88 с.

9. Партыка Т.Л. Информационная безопасность: Учебное пособие // Т.Л. Партыка, И.И. Попов. – М.: Форум, 2012, 432 с.

10. Петров С.В. Информационная безопасность: Учебное пособие // С.В. Петров, И.П. Слинькова, В.В. Гафнер. – М.: АРТА, 2012, 296 с.

11. Семененко В.А. Информационная безопасность // В.А. Семененко. – М.: МГИУ,
2011, 277 с.

12. Семененко В.А. Информационная безопасность: Учебное пособие // В.А. Семененко. – М.: МГИУ, 2010, 277 с.

13. Чернопятов А. Наука, образование и практика: профессионально-общественная аккредитация, тьюторство, информационные технологии, информационная безопасность // А.Чернопятов. – М.: Русайнс, 2013, 144 с.

14. Чипига А.Ф. Информационная безопасность автоматизированных систем // А.Ф. Чипига. – М.: Гелиос АРВ, 2010, 336 с.

15. Шаньгин В.Ф. Информационная безопасность и защита информации // В.Ф. Шаньгин. – М.: ДМК, 2014, 702 с.

16. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие // В.Ф. Шаньгин. – М.: Форум, 2018, 256 с.

17. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие // В.Ф. Шаньгин. – М.: ИД ФОРУМ, НИЦ Инфра-М, 2013, 416 с.