ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ
әл-Фараби атындағы Қазақ ұлттық университетінің

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН
Казахский национальный университет
имени аль-Фараби

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
al-Farabi Kazakh National University

SERIES
PHYSICO-MATHEMATICAL

6 (340)

NOVEMBER – DECEMBER 2021

PUBLISHED SINCE JANUARY 1963

PUBLISHED 6 TIMES A YEAR

ALMATY, NAS RK

NAS RK is pleased to announce that News of NAS RK. Series physico-mathematical journal has been accepted for indexing in the Emerging Sources Citation Index, a new edition of Web of Science. Content in this index is under consideration by Clarivate Analytics to be accepted in the Science Citation Index Expanded, the Social Sciences Citation Index, and the Arts & Humanities Citation Index. The quality and depth of content Web of Science offers to researchers, authors, publishers, and institutions sets it apart from other research databases. The inclusion of News of NAS RK. Series of chemistry and technologies in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential content of chemical sciences to our community.

Қазақстан Республикасы Ұлттық ғылым академиясы «ҚР ҰҒА Хабарлары. Физикалық-математикалық сериясы» ғылыми журналының Web of Science-тің жаңаланған нұсқасы Emerging Sources Citation Index-те индекстелуге қабылданғанын хабарлайды. Бұл индекстелу барысында Clarivate Analytics компаниясы журналды одан әрі the Science Citation Index Expanded, the Social Sciences Citation Index және the Arts & Humanities Citation Index-ке қабылдау мәселесін қарастыруда. Webof Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын усынады. ҚР ҰҒА Хабарлары. Химия және технология сериясы Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді химиялық ғылымдар бойынша контентке адалдығымызды білдіреді.

НАН РК сообщает, что научный журнал «Известия НАН РК. Серия физико-математическая» был принят для индексирования в Emerging Sources Citation Index, обновленной версии Web of Science. Содержание в этом индексировании находится в стадии рассмотрения компанией Clarivate Analytics для дальнейшего принятия журнала в the Science Citation Index Expanded, the Social Sciences Citation Index и the Arts & Humanities Citation Index. Web of Science предлагает качество и глубину контента для исследователей, авторов, издателей и учреждений. Включение Известия НАН РК в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному контенту по химическим наукам для нашего сообщества.

«ҚР ҰҒА Хабарлары.
Физика-математикалық сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *математика, информатика, механика, физика, ғарыштық зерттеулер, астрономия, ионосфера.*
Мерзімділігі: жылына 6 рет.
Тиражы: 300 дана.
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Мұратбаев көш., 75.

«Известия НАН РК.
Серия физика-математическая».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *математика, информатика, механика, физика, космические исследования, астрономия, ионосфера.*
Периодичность: 6 раз в год.
Тираж: 300 экземпляров.
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

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

News of the National Academy of Sciences of the Republic of Kazakhstan. Physical-mathematical series.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *mathematics, computer science, mechanics, physics, space research, astronomy, ionosphere.*
Periodicity: 6 times a year.
Circulation: 300 copies.
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Address of printing house: ST «Aruna», 75, Muratbayev str, Almaty.

NEWS
OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 6, Number 340 (2021), 48–58 https://doi.org/10.32014/2021.2518-1726.101

УДК 004.49
ҒТАМР 28.23.25

Усатова О.А.[1,2], Жұмабекова А.Т.[1,*], Мэтсон Э.[3], Карюкин В.И.[1], Ілесова Б.Е.[1]

[1]Әл-Фараби атындағы Қазақ Ұлттық Университеті, Алматы, Казахстан;
[2]Ақпараттық және есептеуіш технологиялар институты, Алматы, Казахстан;
[3]Пердью Университеті, Вест Лафайет, АҚШ.
E-mail: zhumabekova2702@gmail.com

АҚПАРАТТЫҚ РЕСУРСТАРҒА ТӨНЕТІН ҚАУІП ТҮРЛЕРІ ЖӘНЕ ОЛАРДЫ МАШИНАЛЫҚ ОҚЫТУДЫ ӘДІСТЕРІН ҚОЛДАНУ АРҚЫЛЫ АНЫҚТАУ

Аннотация. Мемлекеттің дамуымен қатар ақпараттық-коммуникациялық технологиялар мен ақпараттық ресурстардың қарқынды дамуын ескере отырып, ақпараттық қауіпсіздікті қамтамасыз етуге қатысты мәселелер күн өткен сайын маңызды бола түсуде. Ақпараттық қауіпсіздік – мұқият зерделеуді қажет ететін ұлттық қауіпсіздік жүйесінің негізгі элементтерінің бірі. Ұсынылған мақалада ақпараттық қауіпсіздік қатерлері бағытталған ақпараттық қауіпсіздік аспектісі, төнген қауіптің әсер ету дәрежесі, пайда болу сипаты мен төнген қауіптер көзінің орналасуы белгілері бойынша жіктеліп, статистика сипатталады. Сонымен қатар, ақпараттық қауіпсіздік құралдарына зерттеу жүргізілді. Соның ішінде, ақпаратты криптографиялық қорғау құралдары, автоматтандырылған жүйелерге пайдаланушылардың ақпараттық ресурстарға қол жеткізуін шектеу құралдары, желіаралық экран құралдары, антивирустық қорғаныс құралдары және спамға қарсы құралдарға талдау болды. Стемингті орындау үшін Python NLTK кітапханасынан PorterStemmer пайдаланылды. Эксперименттік бөлімде машиналық оқыту әдістерін қолдану арқылы спамның таралуын болдырмау мәселесі қарастырылды. Машиналық оқыту деп аналитикалық модель құруды автоматтандыратын деректердің талдау әдісін айтамыз. Оның негізгі идеясы тек компьютерлік алгоритмді қолдану ғана емес, сонымен қатар жиналған тәжірибе көмегімен өз бетінше түрлі есептерді шешуді үйрену. Осы тәжірибеде жай Байес классификаторы, векторлық машинаны қолдау, логистикалық регрессия, k-әдісі жақын көршілер, шешім ағашы, кездейсоқ орман және XGBoost алгоритмдері қолданылды. Бұл машиналық оқыту алгоритмдері қауіптерді анықтау мен жіктеудің заманауи тәсілі болып табылады. Осы модельдердің артықшылықтары мен кемшіліктері анықталған. Ұсынылған тәжірибеде спам және спам емес мәтіндері бар деректер жиынтығы пайдаланылды. Мәтіндерді жіктеу бірнеше кезеңдерді қамтыды және класстарды басқару мен класстарды теңестіру іске асты. Эксперимент барысында теңдестірілген және теңгерімсіз мәліметтерді жіктеу нәтижелері ұсынылды. Әртүрлі машиналық оқыту алгоритмдерімен тәжірибе жасау арқылы жақсы классификация нәтижелері алынды. Ақпараттық қауіпсіздікті қамтамасыз етуде машиналық оқыту әдістерін қолданудың көмегі зор.

Түйінді сөздер: машиналық оқыту, ақпараттық қауіпсіздік, нейрондық желі, үлкен деректер, ақпараттық ресурстар, қауіп, шабуыл.

Кіріспе. Ақпараттық технологиялар қарқынды дамып келе жатқан әлемдік қоғамдастықтың қалыптасуына әсер ететін құбылысқа айналды. Осы тұрғыдан алғанда, біздің еліміз ақпараттық дәуірге енген дамушы мемлекеттердің бірі болып саналады. Ақпараттық технологиялар адам өмірінің ажырамас бір бөлігіне айналғандықтан да ақпараттық ресурстардың қауіпсіздігін қамтамасыз етуді дамытуды талап етеді. Бүкіл әлем бойынша Интернеттің қарқынды дамуымен қатар киберқылмыскерлерге, шабуылдаушыларға сан түрлі қауіп-қатерлер тудыруға, шабуылдар жасауға үлкен мүмкіндік туды. Соңғы жылдардағы басылымдарда ақпараттық қауіпсіздігін бұзудың жағымсыз салдарымен байланысты көптеген маңызды оқиғалар мен есептер жарияланып жатыр. Интернет-қосымшалар түрлі шабуылдарға осал болуы мүмкін, сондықтанда бұл жүйенің құпиялылығының, тұтастығының және қол

жетімділігінің бұзылуына әкеледі. Құпиялылық, тұтастық, қол жетімділік – ақпараттық қауіпсіздіктің негізі болып табылады. Құпиялылықта деректерді қорғаудың дәрежесін анықтайды, яғни ақпаратқа рұқсат етілген субъектілеріне ғана қолжетімді болуын қадағалайды. Тұтастық – ақпараттың мазмұны мен дұрыстығының рұқсат етілмеген өзгертулерінен немесе жойылып кетуінен қорғалуын білдіреді. Рұқсаты жоқ пайдаланушылардың тұтастықты бұзуына жол бермеу үшін түрлі қауіпсіздік құралдары мен алгоритмдерді пайдалану қажет. Ақпараттық қызметке қол жеткізу мүмкіндігін беретін, ақпарат қауіпсіздігінің маңызды бөлігінің бірі – қолжетімділік [1].

Қазақстан Президентінің халқына кезекті ұсынылған Жолдауында Республиканың 2030 жылға дейінгі даму стратегиясында ұлттық қауіпсіздік элементтерінің бірі ақпараттық қауіпсіздік болып табылатыны жеткізілген [2]. Сондай-ақ, ұлттық қауіпсіздік мемлекетіміздің дамуының басым міндетіне айналды. Ақпараттық қауіпсіздікті қамтамасыз етудің тиімді шараларын іске асыру бүгінгі таңда күрделі процесс, себебі адамдар мен хакерлерге қарағанда құрылғылардың саны көбейіп, шабуылдың неғұрлым күрделі әдістерін қолданады. Ақпараттық қауіпсіздігінің алғашқы мемлекеттік Концепциясы 2006 жылы, ал екіншісі 2011 жылы қабылданған. Қазақстан Республикасының ұлттық қауіпсіздігі туралы 2020 жылғы 16 қарашадағы өзгерістер мен толықтырулар енгізілген заңында ұлттық ақпараттық қауіпсіздік жүйесі құрылатыны және күшейтілетіні айқындалған [2].

Материалдар мен әдістер. Ақпараттық қауіпсіздік қатерлері әр түрлі белгілері бойынша жіктеледі. Қасақана жасалынған қауіп бағытталған ақпараттық қауіпсіздік аспектісі бойынша жіктеледі: құпиялылық қаупі, тұтастыққа қауіп және қол жетімділік қауіп [1]. Төнген қауіптің әсер ету дәрежесіне байланысты пассивті және белсенді түрі бар. Егер жүйенің құрылымы мен мазмұнына өзгеріс енгізілмесе қауіптің пассивті түріне, ал жүйенің құрылымы мен мазмұны өзгеріске ұшыраса белсенді түріне жатады [3]. Пайда болу сипаты бойынша табиғи және жасанды қауіптер деп екіге бөлінеді. Табиғи (объективті) қауіп адамның еркінсіз объективті физикалық процестердің немесе табиғат құбылыстарының ақпараттық ортаға әсерінен туындаса, жасанды (субъективті) қауіп адамның ақпараттық сферасына әсерінен туындайды. Жасанды қауіптің өзі кездейсоқ және қасақана жасалынған қауіп болып жіктеледі [4].

Қазіргі таңда ақпараттық қауіпсіздіктің негізгі қауіптері және олардың пайыздық көрсеткіші 1-кестеде бейнеленген [5]:

1-кесте. Ақпараттық қауіпсіздіктің негізгі қауіптері

Қауіптер	Пайыздық көрсеткіштер
Ақпараттық жүйеге сыртқы ену	~5%
Кездейсоқ программалық қамтамасыз етудің бұзылуы	~6%
Кездейсоқ жабдықтың істен шығуы	~15%
Зиянды программалық қамтамасыз ету	~51%

Төнген қауіптер көзінің орналасуы бойынша сыртқы және ішкі қауіп болып екі үлкен топқа бөлінеді. Ұйымдардың ішкі субъектісі болып табылатын орындаушы тарапынан ақпараттың қауіпсіздігіне төнген қауіп ішкі қауіп деп аталып, оларға ақпараттың таралуы және жоғалуы, рұқсатсыз кіру, т.с.с. жатады. Ал ұйым ресурстарынан тыс субъекті болып табылатын бастамашылардан төнетін қауіп сыртқы қауіп болады. Сыртқы қауіптер: фишинг, киберқылмыскерлер шабуылдары, DDos шабуылдары, спам, зиянды программалар (вирустар, трояндар және т.б.), шпиондық программалар (spyware, adware), botnets (зомби желілері) және т.б. [6].

Ақпараттық қауіпсіздікті қамтамасыз ету мақсатында басқару жүйесін құру кезінде ақпаратты қорғауға мүмкіндік беретін ақпараттық қауіпсіздік құралдарын қолдану қажет. Олардың функцияларының үйлесімділігін, қолдану тиімділігін ескере отырып, ақпаратты қорғау құралдарын таңдау қажет. Шамадан тыс қайта сақтандыру үлкен шығындарға әкелуі мүмкін. Төмендегі 1 суретте сыртқы және ішкі қауіптерге қарсы тұру кезінде ақпаратты қорғау құралдары бейнеленген [6].

1.1 сурет

1.2 сурет

1 сурет. Ақпаратты сыртқы қауіптерден (1.1 сурет) және ішкі қауіптерден қорғау құралдары (1.2 сурет).

Қауіптерді машиналық оқыту әдістерімен анықтау**.** Қауіптерді анықтау үшін сан түрлі әдістер, құралдар пайдаланылады. Солардың ішіндегі ең маңызды, тиімді әдістерінің бірі – машиналық оқыту әдісі. Бұл әдісті ақпараттық жүйелер объектілерін дәлірек анықтау үшін қолданылады. Машиналық оқыту әдісі қазіргі уақытта күрделі алгоритмдер көмегімен көптеген нақты уақыттағы тапсырмалар үшін танымал. Машиналық оқыту дегеніміз – аналитикалық модель құруды автоматтандыратын деректерді талдау әдісі. Осы машина үлкен деректер көмегімен статистикалық мәліметтер негізінде күрделі алгоритмдерді пайдалана отырып болжам жасайтын есептік статистикамен тығыз байланысты. Машиналық оқыту мәліметтердің көлеміне, сапасы мен сипатына негізделіп нәтиже шығару үшін қай алгоритм тиімді екенін анықтау мақсатында деректерді пайдаланады [7].

[7] мақалада автор аномалияларды анықтау әдістерін статистикалық тәсілдер, таным және машиналық оқыту деп жіктеген. Машиналық оқыту әдістері талданатын заңдылықтарды жіктейтін ашық немесе жасырын модельге негізделген. Оны нейрондық желілер, анық емес логика, генетикалық алгоритмдер және Байес желілері деп бөледі. Жалпы түсіндірмесі 2-кестеде талданған [8].

2-кесте. Машиналық оқыту әдістері

Әдістер атауы	Анықтамасы	Артықшылықтары мен кемшіліктері
Нейрондық желілер	Көрінбейтін өрнектерді тану мүмкіндігін береді және дәл сәйкес келмейтін үлгілер алдыңғы кіріс үлгілерінің алдын ала анықталған құрылымдарынан ерекшеленеді.	Шектеулі және толық емес деректерді жалпылау және болашақ көрінбейтін үлгілерді тану мүмкіндігі бар.
Анық емес логика	Анық емес жиын теориясынан алынған, оған сәйкес шамамен алынған пайымдау және классикалық предикат логикасынан дәл алынбаған.	Дәлелдеу анық емес. Әсіресе порт сканерлеуге қарсы тиімді.
Генетикалық алгоритмдер	Эволюциялық алгоритм техникасын қолданатын биологиялық шабытпен іздеу эвристикасы.	Генетикалық алгоритмдер жіктеу ережелерін шығаруға және анықтау процесінің оңтайлы параметрлерін таңдауға қабілетті.
Байес желілері	Айнымалылар арасындағы ықтималдық қатынасты кодтайтын модель. Бұл әдіс статистикалық схемалармен бірге кіруді анықтау үшін жиі қолданылады.	Айнымалылар мен оқиғаларды болжау арасындағы және бұрынғы білімді де, деректерді де қосу мүмкіндігі бар.

Деректерден аномалияларды, қауіптерді анықтау үшін машиналық оқыту әдістерін қолдануды [9] мақалада сипатталған. Әдеби шолуында модельдер төрт тұрғыдан талданады: ауытқуларды анықтау әдістерін қолдану, машиналық оқыту әдістері, машиналық оқыту модельдерінің өнімділік көрсеткіштері және ауытқуларды анықтаудың жіктелуі. 4 кезеңнен тұратын, сондай-ақ зерттеуді жоспарлау, оны жүргізу кезеңдерін мен есептілікті қамтитын Китченхэм және Чартерс әдісіне жүйелі түрде шолуды жүргізген. Оның әр кезеңі бірнеше қадамнан тұрады. Алдымен зерттеу сұрақтарын анықтап, іздеу стратегиясын жасайды. Келесі қадамда алу және қосу ережелерін қамтитын зерттеулерді іріктеу процедураларын анықтап, жиналған зерттеу жұмыстарын фильтрациялау үшін қолданылатын

сапаны бағалау ережелерін табады. Ең алғашқы анықталған зерттеу сұрақтарына жауап беру үшін экстракция стратегиясын нақтылап, алынған деректердің синтезін қамтиды.

Корпоративті желілер үшін қолтаңбаны талдау әдістері мен машиналық оқыту әдістерінің комбинациясын қолдануы [10] мақалада ұсынылады. Random Forest алгоритмімен корпоративтік желілердегі трафикті талдау және шабуылдарды анықтау, ал шабуылдардың класстарын нақтылау үшін AdaBoost қолданылуы ұсынылған. Олар қарапайым қол қою әдістері мүмкін емес сипатталған класстарындағы шабуылдардың жаңа түрлерін анықтау үшін пайдаланады. Бірақ, белгілі шабуылдар үшін оларды дәл анықтау мақсатында қолтаңбаға негізделген әдістер тиімді болуы мүмкін.

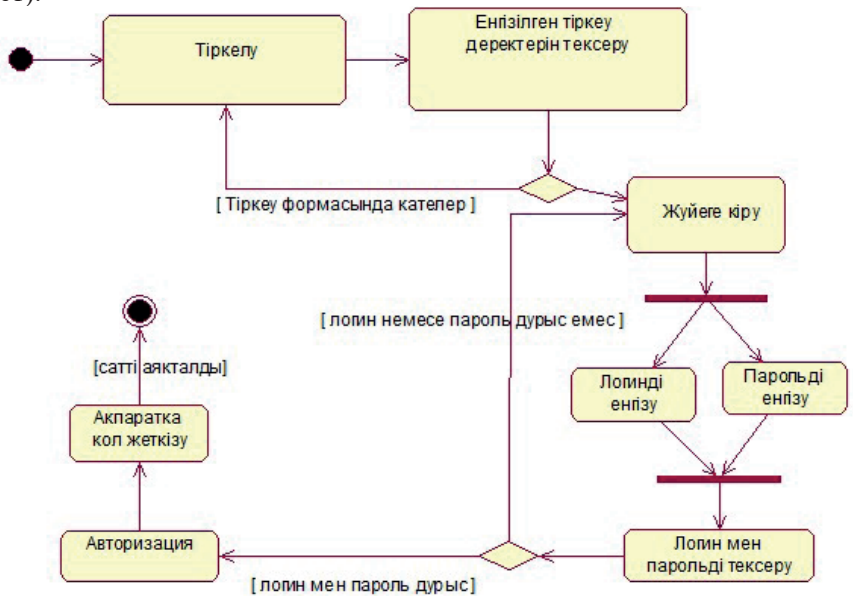
RNN-IDS моделін қолдану арқылы шабуылдарды анықтау [11] мақалада талданады. Шабуылдардарды жіктеудің екі мәселесі, екілік жіктеу және шабуылдардың 4 классына жіктеу қарастырылады. RNN-IDS моделі шабуылдарды анықтаумен қатар екілік және көп классты жіктеуде жоғары қабілетке ие. Үлкен көлемді деректерді жіктеу үшін қайталанатын нейрондық желілерді қолданады. Нәтижесінде, екілік жіктеу үшін қателердің 0,1% -дан аз дәлдігіне, ал шабуыл түрі бойынша жіктеу үшін 0,5% -ға қол жеткізілді.

Желілік ауытқуларды анықтау мәселесіне арналған екі түрлі автокодератордың жұмысының тиімділігін [12] мақалада ұсынылды. Нәтижесінде бұл әдіс NSL-KDD жинағында шабуылдарды анықтау дәлдігін 88,28% бен 88,65%-ға дейін арттыруға мүмкіндік беретінін анықтады.

Ақпараттыққауіпсіздікқұралдары. Ақпараттыққауіпсіздікқұралдарынаақпараттыкриптографиялық қорғау құралдары; автоматтандырылған жүйелерге пайдаланушылардың ақпараттық ресурстарға қол жеткізуін шектеу құралдары; желіаралық экран құралдары; антивирустық қорғаныс құралдары; спамға қарсы құралдар және т.б. жатады.

Криптографиялық әдісте ақпаратты шифрлау, кодтау немесе басқаша түрлендіру жүргізу арқылы ақпарат тікелей өзі қорғалады, сондықтанда ақпаратты криптограмма кілтінсіз оған қол жеткізу мүмкін емес [13]. Криптографияның бірнеше түрлері бар. Олар: ашық кілтті криптожүйелер, симметриялық криптожүйелер, кілтті басқару және электрондық жазба жүйесі.

Қолданушылардың автоматтандырылған жүйедегі ақпараттық ресурстарды пайдалану үшін қорғау құралдарының рұқсатсыз кіруден қорғайды. Бұл құрал үш сатыдан тұрады, олар: сәйкестендіру, аутентификация және авторизация [14]. Қолданушы өзінің тіркелу логинін (идентификатор) енгізу арқылы сәйкестендіру сатысынан өтеді. Осы идентификатор иесі қолданушы екенін тексеру мақсатында аутентификация сатысы орындалады. Ол үшін аутентификация параметрлерін енгізіледі. Оның параметрлеріне желі адрестері, парольдер, симметриялы құпия кілттер, электронды сандық кілт, биометриялық мәліметтер (саусақ іздері, дауыстық ақпарат) және т.б. жатады. Көп жағдайда сәйкестендіру мен аутентификациялау процедурасы бір мезетте орындалады. Жоғарыдағы екі процесс сәтті аяқталған жағдайда автоматтандырылған жүйелерде пайдаланушыларды тіркеу кезеңі жүзеге асырылады. Белгілі бір адамға немесе адамдар тобына белгілі бір әрекеттерді орындау құқығын беру, яғни авторизация сәтті орындалды. Төмендегі UML диаграммасында процесстің жүзеге асырылу реті көрсетілген (2 сурет).



2 сурет. Ақпараттық ресурстарға қол жеткізуін шектеу құралдары UML диаграммасында.

Келесі құрал желіаралық экран құралдары (брандмауэр), олардың көмегімен желі порттарына шектеу кою арқылы желіге рұқсатсыз қол жеткізуден қорғалады. Бұл желіге немесе компьютерге кіру және шығу деректері үшін сүзгі рөлін атқаратын аппараттық құрал. Оларды бірнеше критерийлер бойынша жіктелінеді [15]: OSI моделі деңгейінде жұмыс істеу арқылы, қосылу схемасына сәйкес, орындауы бойынша, қолданылатын технология бойынша.

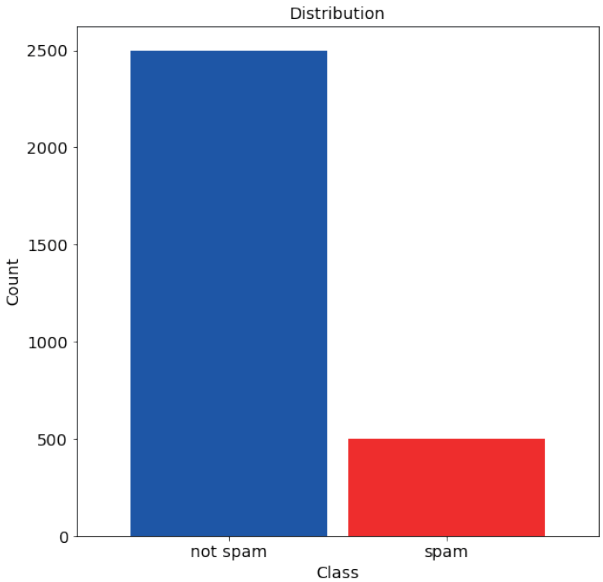
Көп қолданылатын антивирустық қорғаныс құралдары компьютерді антивирустық программа көмегімен түрлі вирустардан қорғау, антивирустық мәліметтер базасын үнемі жаңарту шараларын жүргізіледі [16]. Вирус анықталған жағдайда вирустанған файлды тазарту, енген вирусты жою, басқа файлдармен байланысын үзу және карантин енгізу сияқты процесстерді жүзеге асырады.

Спам электрондық поштаны, интернет ресурстарын пайдаланушылар үшін маңызды мәселеге айналды. Қолданыстағы спаммен күресу әдістерін ұйымдастыру әдісіне қарай үлестірілген және жергілікті деп бөлуге болды, ал жабық әдістер жеке категория ретінде қарастырылады. Үлестірілген әдістер бір-бірімен мәліметтер алмасатын көптеген тәуелсіз пошталық жүйелерден спам туралы ақпарат жинауға қатысуды қамтиды. Осы әдістің бір кемішілі таратылған спам – сүзу әдістері шеңберінде бір пошта жүйесінде сүзгіні дәл реттеу мүмкін емес. Жергілікті әдіс үлестірілген әдістен айырмашылығы бастапқыда белгілі бір пошта жүйесіне жақсы бейімделу мүмкіндігіне ие. Осы әдісті жұмыс принципіне бойынша Байес сүзгісі, формальды протокол ережелеріне негізделген әдістер, процедуралық әдістер, жіберушінің аутентификациясы деп жіктеледі [17].

Ақпаратты қорғаудың негізгі міндеті киберқылмыскерлердің жолын шатастыру, құпия ақпаратқа қол жеткізбеу.

Зерттеу нәтижесі. Машиналық оқыту алгоритмдерінің көмегімен спамның анықталуы. Спамның таралуын болдырмау үшін машиналық оқыту алгоритмдерін қолдану төмендегі тәжірибеде көрсетілген. Спам және спам емес мәтіндері бар деректер жиынтығы пайдаланылды. Деректер келесідей таратылады (3 сурет).

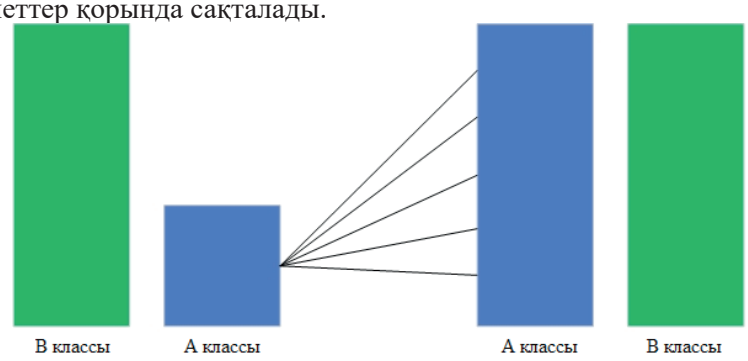
Мәтіндерді жіктеу үшін мәтіндерді алдын ала өңдеуге және жіктеуге келесі негізгі шаралар қабылданды: мәтіндерді тазарту, тоқтату сөздерін жою, жүйелеу және лемматизация, тепе-теңдік класстары, векторизация, классификация.



3 сурет. Екі классты деректер жиынтығы

Бірінші кезеңде спам мәтіндерді алдын ала өңдеу және тазалау қажет. Ол үшін алдымен барлық сөздер кіші әріпке ауыстырылады. Осыдан кейін көп жағдайда мағынасы аз болғандықтан тыныс белгілері, сандар, арнайы таңбалар мен сілтемелер алынып тасталады. Сонымен қатар, өте жиі кездесетін сөздерді алып тастау қажет («және», «кіру», «қосу», «бұл», «үшін», «уақыт»). Содан кейін мағынасы ұқсас сөздердің санын азайту үшін түбір алуды немесе лемматизацияны орындау қажет. Бұл тәсілдердің айырмашылығы – соңғысы инфинитивті сөз формасын алады, ал біріншісі түбір алу үшін аффикстер мен сөз жалғауларын жояды. Бұл мақалада Python NLTK кітапханасындағы «PorterStemmer» пайдаланылады.

Бұл жинақта деректер теңдестірілмеген түрде берілген, яғни бір класстың пайда болу саны екіншісінің пайда болуынан едәуір асып түседі. Жақсы классификаторды дайындау кезінде теңгерімсіз класстар маңызды мәселе болып табылады. Класстар өте теңгерімсіз болғандықтан, жіктеуіш барлық даналарды ең көп ұсынылған класспен белгілеу арқылы жеткілікті дәл нәтиже береді. Алайда, басқа классты қате жіктеу бағалаудың негізгі көрсеткіштерін білдіретін accuracy, precision, recall және F1 шаралары тұрғысынан нашар нәтижеге әкеледі. Бұл мәселені шешу үшін класстар теңестіріледі. Мұны істеу үшін, кіші класс қалаған өлшемге жету үшін оның даналарын бірнеше рет көшіру арқылы көпшілік классқа сәйкес келетін мөлшерде өседі (4 сурет). Бұл шешімнің артықшылығы – барлық құнды ақпарат мәліметтер қорында сақталады.



4 сурет. Теңестіру класстары

Векторизация кезеңінде мәтіндер сандық түрге айналады. Бұл үшін TF-IDF сияқты тиімді жиілік өлшемі жиі қолданылады. TF-IDF келесі формула бойынша есептеледі:

$$TF\_IDF = TF \times IDF, \quad (1)$$

мұнда TF – құжаттағы сөздің пайда болу жиілігінің осы құжаттағы сөздердің жалпы санына қатынасы.

$$TF_{d,w} = \frac{count(w,d)}{count(N,d)}, \quad (2)$$

мұнда $count(w,d)$ – d құжатындағы w сөзінің жиілігі және $count(N,d)$ - d құжатындағы N сөздерінің саны.

IDF, керісінше, әр сөздің D корпусында пайда болу жиілігіне негізделген салмағын білдіреді:

$$IDF_{w,d} = \log \frac{count(D)}{count(w,d)}, \quad (3)$$

мұндағы $count(D)$ - құжаттар саны.

Мәтіндерді жіктеу үшін келесі ең тиімді машиналық оқыту алгоритмдері қолданылды: Наиф Байес классификаторы, логистикалық регрессия, векторлық машинаны қолдау, k әдісі – жақын көршілер, шешім ағашы, кездейсоқ орман және XGBoost.

Жіктеу моделінің сапасын бағалау үшін келесі көрсеткіштер қолданылды:

$$accuracy = \frac{TP + TN}{TP + FP + TN + FN}, \quad (4)$$

$$precision = \frac{TP}{TP + FP}, \quad (5)$$

$$recall = \frac{TP}{TP + FN}, \quad (6)$$

$$F1\_score = 2\frac{precision \times recall}{precision + recall}, \quad (7)$$

мұнда TP (шын позитив) сынақ данасы спам ретінде дұрыс жіктелгенін көрсетеді; TN (шын теріс) сынақ данасы спам емес деп дұрыс жіктелгенін көрсетеді; FP (жалған позитивті) қате спам ретінде жіктелген сынақ данасын көрсетеді; FN (жалған теріс) қате түрде спам емес деп жіктелген сынақ нұсқасын көрсетеді. Теңдестірілген және теңгерілмеген үлгілерді жіктеудің эксперименттік нәтижелері 3-кестеде келтірілген.

3-кесте. Теңгерімсіз деректер жиынтығының жіктелуі

теңгерімсіз үлгі								
Жіктеуіш	Жай Байес классификаторы	Векторлық машинаны қолдау	Логистика-лық регрессия	k-әдісі жақын көршілер	Шешім ағашы	Кездей-соқ орман	XGBoost	Орташа мәндер
Accuracy	0.87	0.98	0.95	0.96	0.96	0.96	0.98	0.95
Precision	1.00	0.99	1.00	0.90	0.89	0.98	0.98	0.96
Recall	0.26	0.90	0.71	0.87	0.87	0.76	0.90	0.75
F1-score	0.42	0.94	0.83	0.89	0.88	0.86	0.94	0.82
теңдестірілген үлгі								
Жіктеуіш	Жай Байес классификаторы	Векторлық машинаны қолдау	Логистика-лық регрессия	k-әдісі жақын көршілер	Шешім ағашы	Кездей-соқ орман	XGBoost	Орташа мәндер
Accuracy	0.99	1.00	0.99	0.95	0.98	0.99	0.99	0.98
Precision	0.97	1.00	0.99	0.90	0.96	0.99	0.98	0.97
Recall	1.00	1.00	0.99	0.99	0.99	0.99	0.99	0.99
F1-score	0.99	1.00	0.99	0.95	0.98	0.99	0.99	0.98

Талқылануы. Әр түрлі жіктеу модельдерінің нәтижелері теңдестірілмеген мәліметтер бойынша дайындалған модельдердің теңдестірілген деректер бойынша оқытылғаннан төмен көрсеткіштерінің бар екенін көрсетеді. Әр түрлі машиналық оқыту алгоритмдерінің ішінде қолдау векторлық машиналық қолдау, логистикалық регрессия, кездейсоқ орман және XGBoost жақсы нәтиже көрсетті. Жай Байес классификаторы жақсы жұмыс жасағанымен де, оның барлық функциялары өзара тәуелсіз деген болжаммен байланысты алгоритм белгілі бір шектеулерден зардап шегетінін атап өткен жөн. Қарапайымдылығына қарамастан, k-әдісі жақын көршілер жақсы жіктеу нәтижелеріне қол жеткізеді. Кездейсоқ орман алгоритмі бірнеше тәуелсіз шешім ағаштарын қолданатындықтан, оның өнімділігі бір шешім ағашына қарағанда жақсы екені айқын.

Қорытынды. Ақпараттық қауіпсіздікті қамтамасыз ету, қауіптерден қорғау құралдары мен әдістері бүкіл әлем бойынша үлкен мәселе. Өкінішке орай, бүгінгі таңда күніне каншама мың зиянды программалар анықталады және олар киберқылмыскерлерге ақпараттық ресурстарға шабуылдауға, қауіп-қатер келтіруге үлкен мүмкін береді. Осы мақалада ақпараттық ресурстарды қорғаудың ақпаратты криптографиялық қорғау құралдары, автоматтандырылған жүйелерге пайдаланушылардың ақпараттық ресурстарға қол жеткізуін шектеу құралдары, желіаралық экран құралдары, антивирустық қорғаныс құралдары және спамға қарсы құралдар қарастырылды. Сондай-ақ, машиналық оқыту әдістеріне негізделген қорғаудың жаңа түрлері, генетикалық алгоритмдер, түсініксіз логика, нейрондық желілер және Байес желілеріне үлкен көңіл бөлінді. Бұл зерттеудің нәтижелері ақпараттық ресурстарға төнген қауіптерді анықтау әдістері мен қауіпсіздік құралдарын әзірлеу қажеттілігін көрсетеді. Келесі зерттеулерде бұл мәселені жалғастырылып, ақпараттық ресурстарға төнген қауіптерді анықтау мақсатында машиналық оқыту әдісіне жаңа алгоритм, жаңа тәсілдер құрастыру жоспарлануда. Машиналық оқытудың жаңа әдістерін қолдану қауіпсіздіктің дамуына өз үлесін қосатынына сеніміміз мол.

Жумабекова А.Т.[1*], Усатова О.А.[1,2], Мэтсон Э.[3], Карюкин В.И.[1], Илесова Б.Е.[1]

[1]Казахский Национальный Университет имени аль-Фараби, Алматы, Казахстан;
[2]Институт информационных и вычислительных технологий, Алматы, Казахстан;
[3]Университет Пердью, Вест Лафайет, США.
E-mail: zhumabekova2702@gmail.com

ВИДЫ УГРОЗ ИНФОРМАЦИОННЫМ РЕСУРСАМ И МЕТОДЫ ИХ ОПРЕДЕЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ

Аннотация. Наряду с развитием страны, с учетом стремительного развития информационных и коммуникационных технологий и информационных ресурсов все большее значение приобретают вопросы, связанные с информационной безопасностью. Информационная безопасность – один из ключевых элементов системы национальной безопасности, требующий тщательного изучения. В представленной статье приведена статистика, классифицирующая угрозы информационной

безопасности по аспекту целевой информационной безопасности, степени воздействия угрозы, характеру возникновения и местоположению источника угрозы. Кроме того, было проведено исследование средств защиты информации. К ним относятся средства криптографической защиты информации, средства ограничения доступа пользователей к информационным ресурсам в автоматизированных системах, средства межсетевого экрана, средства антивирусной защиты и средства защиты от спама. Для выполнения стемминга использовался PorterStemmer из библиотеки Python NLTK. В экспериментальной части была рассмотрена задача предотвращения распространения спама с использованием методов машинного обучения. Машинное обучение – это метод анализа данных, который автоматизирует создание аналитической модели. Его основная идея – не только использовать заданный алгоритм, но и научиться самостоятельно решать различные задачи с помощью опыта. В этом эксперименте использовались Наивный байесовский классификатор, машина опорных векторов, логистическая регрессия, метод ближайших соседей, дерево решений, случайный лес и алгоритмы XGBoost. Эти алгоритмы машинного обучения представляют собой современный способ выявления и классификации угроз. Выявлены достоинства и недостатки этих моделей. В предлагаемом эксперименте использовался набор данных со спамом и неспамовыми текстами. Классификация текстов проходила в несколько этапов, при этом происходило управление классами и выравнивание классов. В ходе экмперимента были представлены результаты классификации сбалансированных и несбалансированных данных. Хорошие результаты классификации были получены в результате экспериментов с различными алгоритмами машинного обучения. Использование методов машинного обучения является большим подспорьем в обеспечении информационной безопасности.

Ключевые слова: машинное обучение, информационная безопасность, нейронная сеть, большие данные, информационные ресурсы, угроза, атака.

Zhumabekova A.[1*], Ussatova O.[1,2], Matson E.[3], Karyukin V.[1], Ilessova B.[1]

[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan;
[2]Institute of Information and Computing Technologies, Almaty, Kazakhstan;
[3]Purdue University, West Lafayette, USA.
E-mail: *zhumabekova2702@gmail.com*

THE TYPES OF THREATS TO THE INFORMATION RESOURCES AND THE METHODS OF THEIR DETECTION WITH THE USE OF MACHINE LEARNING METHODS

Abstract. Along with the development of the country, taking into account the rapid growth of information and communication technologies and information resources, issues related to information security are becoming increasingly important. Information security is one of the key elements of a national security system that requires careful study. The presented article provides statistics that classify information security threats according to the aspect of target information security and the degree of threat impact, the nature of the occurrence, and the location of the threat source. In addition, a study was conducted on information security tools. It includes cryptographic protection of information, restricting user access to information resources in automated systems, firewall, anti-virus protection, and anti-spam tools. PorterStemmer from Python NLTK library was used for stemming. Furthermore, machine learning techniques have been developed to prevent the spread of spam, which is one of the risk detection methods and is a branch of artificial intelligence. Machine learning is a data analysis technique that automates the creation of an analytical model. Its main idea is to use a computer algorithm and learn how to solve various problems independently with the help of experience. This experiment used a Naïve Bayesian classifier, support vector machine, logistic regression, k-nearest neighbors, decision tree, random forest, and XGBoost algorithms. These machine learning algorithms represent a modern way to identify and classify threats. The advantages and disadvantages of these models are revealed. The proposed experiment used a dataset with spam and non-spam texts. The classification of texts took place in several stages, while the classes were managed and the classes were aligned. During the experi-ment, the results of the classification of balanced and unbalanced data were presented. Good classification results were obtained as a result of experiments with various machine learning algorithms. The use of machine learning methods is of great help in ensuring information security.

Key words: machine learning, information security, neural network, big data, information resources, threat, attack.

Information about the authors:

Ussatova Olga – Ph.D., chief scientific secretary, Senior Researcher, Institute of Information and Computer Technology; Ph.D., Acting associate professor, Al-Farabi Kazakh National University, AlmatyKazakhstan, uoa_olga@mail.ru https://orcid.org/0000-0002-5276-6118;

Zhumabekova Aidana – Master, Ph.D. student, Al-Farabi Kazakh National University, Almaty, Kazakhstan, zhumabekova2702@gmail.com, https://orcid.org/0000-0003-4242-7988;

EricMatson – PhD., Professor, Purdue University, West Lafayette, USA, ematson@purdue.edu, https://orcid.org/0000-0001-9200-4903;

Karyukin Vladislav – Master, Senior Lecturer, Al-Farabi Kazakh National University, Almaty, Kazakhstan,vladislav.karyukin@gmail.com, https://orcid.org/0000-0002-8768-0349;

IlessovaBakhytgul – Master, Ph.D.student, Al-Farabi Kazakh National University, Almaty, Kazakhstan,bakhytgul92@gmail.com, https://orcid.org/0000-0001-8357-519X.

ӘДЕБИЕТТЕР

[1] Невструев А.А. (2021) Ақпараттық қауіпсіздік: қорғау ұғымы мен деңгейлері. VI Халықаралық ғылыми -практикалық конференция мақалаларының студенттердің ғылыми зерттеу жинағы. Пенза, ICNS Ғылым және білім, 35-37 б.

[2] Қазақстан Республикасының заңы, ҚР ұлттық қауіпсіздігі туралы (2020.16.11. берілген өзгерістер мен толықтырулармен), [Электрондық ресурс]. - URL: https://online.zakon.kz/Document/?doc_id=31106860#pos=32;-44.

[3] Жеке мәліметтердің ақпараттық жүйелерінің ақпараттық қауіпсіздігіне қатерлер моделі. (2018). «№10 балалар көркемсурет мектебі» коммуналдық бюджеттік қосымша білім беру мекемесі, 10 бет. https: //dshi10.kmr.muzkult.ru/media/2018/08/06/1228197305/Model_ugroz.pdf.

[4] Ермаков Е.В., Козырева Е.В., Панасюра С.В., Горбачѐв А.П. (2016) Сымсыз сенсорлық желілердегі ақпараттық қауіпсіздікке қатердің жіктелуі. Ақпараттық кеңістіктің қауіпсіздігі Студенттердің, аспиранттар мен жас ғалымдардың XV Бүкілресейлік ғылыми-практикалық конференциясы материалдарының жинағы. Қорған: Қорған мемлекеттік университетінің баспасы, ISBN 978-5-40-01266-2., 122-124 бет. URI: *http://hdl.handle.net/123456789/4438.*

[5] *http://www.risidata.com/Database.*

[6] Байтимирова Н.П., Марченко С.В., Паршин К.А. (2016) Сымсыз сенсорлық желілердегі ақпараттық қауіпсіздікке қатердің жіктелуі. Ақпараттық кеңістіктің қауіпсіздігі Студенттердің, аспиранттар мен жас ғалымдардың XV Бүкілресейлік ғылыми-практикалық конференциясы материалдарының жинағы. Қорған: Қорған мемлекеттік университетінің баспасы, ISBN 978-5-40-01266-2., 95-98 бет.

[7] Анна Л. Бучак, Эрхан Гувен. А. (2016) Киберқауіпсіздіктің кіруін анықтау үшін деректерді өндіру мен машиналық оқыту әдістеріне шолу, IEEE коммуникациялық сауалнамалар мен оқулықтар, т. 18, № 2, DOI: 10.1109/COMST.2015.2494502.

[8] Ромулус Костаче, Алиреза Арабамери, Хосейн Моайеди, Куок Бао Фам, М.Сантош, Хоанг Нгуен, Маниш Панди мен Бинх Тай Фам. (2021) Нейрондық желі, қарапайым Байес, XGBoost және жіктеу мен регрессия ағашымен үйлесімді логиканы қолдана отырып, су тасқынының ықтимал индексін бағалау, Халықаралық Геокарто, DOI: 10.1080/10106049.2021.1948109.

[9] Али Боу Нассиф, Манар Әбу Талиб, Қасым Насир, Фатима Мохамад Дакалбаб. (2021) Аномалияны анықтауға арналған машиналық оқыту: жүйелі шолу. IEEE Access мультидисциплинарлы жылдам шолу ашық қатынау журналы, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9439459.

[10] Бахарева Н.Ф., Тарасов В.Н., Шухман А.Е., Полежаев П.Н., Ушаков Ю.А., Матвеев А.А. (2018) Машиналық оқыту әдістерінің көмегімен корпоративтік желілерге шабуылдарды анықтау. Танымдық ақпараттық технология басқару жүйелерінде. 14 Том, № 3, ISSN 2411-1473, DOI: 10.25559/SITITO.14.201803.626-632.

[11] Инь С., Чжу Ю., Фэй Дж., Хе Х. (2017) Қайталанатын нейрондық желілерді қолдану арқылы интрузияны анықтауға арналған терең оқыту әдісі // IEEE қатынауы. 2017. том. 5. б. 21954-21961. DOI: 10.1109/AC-CESS.2017.2762418.

[12] Айгун Р.К., Явуз А.Г., (2017) Автокодкодерге негізделген стохастикалық жетілдірілген модельдермен желілік аномалияны анықтау. 2017 IEEE 4 -ші киберқауіпсіздік және бұлтты есептеу бойынша халықаралық конференция (CSCloud). Нью-Йорк, 2017. С. 193-198 бет. DOI: 10.1109/CSCloud.2017.39.

[13] Абдуахадов Алибек Акмал угли. (2021) Компьютерлік желдерде ақпаратты қорғау. Универсам: Инженерлік ғылымдар: Электрон. ғылыми. журн. №5 (86), URL: https://7universum.com/ru/tech/archive/item/11789.

[14] Ақпаратты қорғау. Аспаптар мен машинажасауда ғылымды қажет ететін технологиялар және университетте инновациялық қызметтің дамуы Бүкілресейлік ғылыми-техникалық конференция материалдары. 3 том. Мәскеу, Ресей. *https://docplayer.com/64005222-Naukoemkie-tehnologii-v-priboro-i-mashinostroenii-i-razvitie-innovacionnoy-deyatelnosti-v-vuze.html.*

[15] Пей-Мин Хо, Юки Йококура (2021). Өрістердің тиімді теориясынан брандмауэр. Universe, 7(7), 241. *https://doi.org/10.3390/universe7070241.*

[16] Горшков А.В., Лохвицкий В.А., Хомоненко А.Д., Рыбакова Е.А., Горшков В.Н. (2016) Сәулелік диаграммаларды қолдана отырып антивирустық құралдардың көп критерийлі таңдауы. Көліктегі зияткерлік технологиялар. № 2. 23-29 бет. *https://cyberleninka.ru/article/n/multi-criteria-choice-of-antivirus-tools-with-using-the-ray-diagrams*

[17] Шейхи С., Хейрабади М.Т., Баззаз А. (2020) Мазмұнға негізделген мүмкіндіктер мен орташа нейрондық желіні қолдана отырып, SMS-спамды табудың тиімді моделі. Халықаралық инженерлік журнал, Том 33, №2, 221-228 бет. Doi: *10.5829/IJE.2020.33.02B.06.*

REFERENCES

[1] Nevstruev (2021). Information security: concept and levels of protection. Student scientific research collection of articles of the VI International scientific and practical conference. Penza, ICNS “Science and Education”. P.35-37.

[2] On the national security of the Republic of Kazakhstan. With changes and additions as of November 16, 2020, [Electronic resource]. - URL: https://online.zakon.kz/Document/?doc_id=31106860#pos=32;-44.

[3] Model of threats to information security of information systems of personal data. Municipal budgetary institution of additional education “Children’s Art School Nomber 10”. Page 10. https://dshi10.kmr.muzkult.ru/media/2018/08/06/1228197305/Model_ugroz.pdf.

[4] Ermakov E.V., Kozyreva E.V., Panasyura S.V., Gorbachev A.P., (2016) Classification of information security threats in wireless sensor networks. Security of the information space Collection of materials of the XV All-Russian scientific-practical conference of students, graduate students and young scientists. Kurgan, ISBN 978-5-40-01266-2., P.122-124. URI: *http://hdl.handle.net/123456789/4438.*

[5] *http://www.risidata.com/Database*.

[6] Baitimirova N.P., Marchenko S.V., Parshin K.A. (2016) Classification of information security threats in wireless sensor networks. Security of the information space Collection of materials of the XV All-Russian scientific-practical conference of students, graduate students and young scientists. Kurgan, ISBN 978-5-40-01266-2., P. 95-98. URI: *http://hdl.handle.net/123456789/4438.*

[7] Anna L. Buczak, Erhan Guven. (second quarter 2016) A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection, IEEE Communications surveys & Tutorials, vol. 18, no. 2,. DOI: 10.1109/COMST.2015.2494502.

[8] Romulus Costache, Alireza Arabameri, Hossein Moayedi, Quoc Bao Pham, M. Santosh, Hoang Nguyen, Manish Pandey & Binh Thai Pham. (2021) Flash-flood potential index estimation using fuzzy logic combined with deep learning neural network, naïve Bayes, XGBoost and classification and regression tree, Geocarto International. DOI: 10.1080/10106049.2021.1948109.

[9] Ali Bou Nassif, Manar Abu Talib, Qassim Nasir, Fatima Mohamad Dakalbab. (2021) Machine Learning for Anomaly Detection: A Systematic Review. IEEE Access Multidisciplinary Rapid Review Open Access Journal, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9439459.

[10] Bakhareva N.F., Tarasov V.N., Shukhman A.E., Polezhaev P.N., Ushakov Yu.A., Matveev A.A. (2018) Identifying attacks on corporate networks using machine learning methods. Cognitive information technology in control systems. Volume 14, № 3, ISSN 2411-1473, DOI: 10.25559/SITITO.14.201803.626-632.

[11] Yin C., Zhu Y., Fei J., He X. (2017) A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks // IEEE Access. Vol. 5. Pp. 21954-21961. DOI: 10.1109/AC-CESS.2017.2762418.

[12] Aygun R.C., Yavuz A.G. (2017) Network Anomaly Detection with Stochastically Improved Autoencoder Based Models // 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud). New York, NY. Pp. 193- 198. DOI: 10.1109/CSCloud.2017.39.

[13] Abduakhadov Alibek Akmal ugli. (2021) Information protection in computer networks. Universam:

technical sciences: electronic scientific journal №5 (86), URL: https://7universum.com/ru/tech/archive/item/11789.

[14] Protection of information. (2016) Technological Naukoemkie prıвoro_i maşinostroenii razvitie innovaцionnoj dejatelьnosti vuze Materialы Vserossijskoj naucno-texniceskoj conferences. Tom 3, Moscow, Russia. https://docplayer.com/64005222-Naukoemkie-tehnologii-v-priboro-i-mashinostroenii-i-razvitie-innovacionnoy-deyatelnosti-v-vuze.html.

[15] Pei-Ming Ho, and Yuki Yokokura (2021). Firewall from Effective Field Theory. *Universe* 2021, *7*(7), 241. *https://doi.org/10.3390/universe7070241.*

[16] Gorshkov A.V., Lokhvitskii V.A, Khomonenko A.D., Rybakova E.A., Gorshkov V.N. (2016) Multi-Criteria Choice of Antivirus Tools with Using the Ray Diagrams. Intellectual Technologies on Transport. No 2, P.23-29. https://cyberleninka.ru/article/n/multi-criteria-choice-of-antivirus-tools-with-using-the-ray-diagrams.

[17] Sheikhi S., Kheirabadi M.T., Bazzaz A. (February 2020) An Effective Model for SMS Spam Detection Using Content-based Features and Averaged Neural Network. International Journal of Engineering journal, Vol. 33, No. 2, P.221-228. Doi: *10.5829/IJE.2020.33.02B.06.*

МАХМҰНЫ

ФИЗИКА

ИНФОРМАТИКА

МАТЕМАТИКА

СОДЕРЖАНИЕ

ФИЗИКА

ИНФОРМАТИКА

МАТЕМАТИКА

CONTENTS

PHYSICS

COMPUTER SCIENCE

MATHEMATICS

Publication Ethics and Publication Malpracticein
the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines 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 otherlanguage, 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 сайтах:

www:nauka-nanrk.kz

http://physics-mathematics.kz/index.php/en/archive

ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Редакторы: *М.С. Ахметова, А. Ботанқызы, Д.С. Аленов, Р.Ж. Мрзабаева*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 10.12.2021.
Формат 60x881/8. Бумага офсетная. Печать –ризограф.
9,5 п.л. Тираж 300. Заказ 6.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19