КОМПЬЮТЕРНЫЕ НАУКИ, ПРИБОСТРОЕНИЕ И АВТОМАТИЗАЦИЯ
КОМПЬЮТЕРЛІК ҒЫЛЫМДАР, АСПАП ЖАСАУ ЖӘНЕ АВТОМАТТАНДЫРУ
COMPUTER SCIENCE, INSTRUMENTATION AND AUTOMATION

ӘОЖ 004.056.53
ҒТАХА 28.23.15
https://doi.org/10.53364/24138614_2025_38_3_13

С.А. Адилжанова[1], **Б. Қ. Ыбрайымбай**[1*], **Л. Ш.Черикбаева**[1]

[1]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан

[*]*E-mail: baxa.nusipov01@mail.ru*

ЭНЕРГЕТИКАЛЫҚ НЫСАНДАР ҮШІН МАШИНАЛЫҚ ОҚЫТУ ӘДІСТЕРІН ҚОЛДАНУ АРҚЫЛЫ DDOS ШАБУЫЛДАРЫНАН ҚОРҒАУ ЖҮЙЕСІН ӘЗІРЛЕУ

Аңдатпа. *Энергетикалық нысандарды цифрландыру олардың жұмыс істеуінің ажырамас бөлігіне айнала отырып, киберқауіптердің, соның ішінде қызмет көрсетуден бас тартуға бағытталған шабуылдардың (DDoS) артуына алып келуде. Мұндай шабуылдар SCADA жүйелері, IoT құрылғылары және интеллектуалды энергетикалық желілердің тұрақты жұмысын бұзып, сыни инфрақұрылымға елеулі қатер төндіреді. Мақалада энергетикалық сектордағы DDoS шабуылдарын анықтау мен болдырмаудың заманауи әдістері қарастырылады. Бұл мақсатта машиналық оқыту әдістері (Random Forest, Decision Tree, Gradient Boosting, SVM) және терең оқыту модельдері (CNN, LSTM), сондай-ақ олардың гибридті нұсқалары (LSTM-CNN) талданады. Модельдердің тиімділігі CICDDoS2019 және KDD-CUP деректер жиынтықтары, сондай-ақ SCADA жүйесінің модельденген тестілік ортасында бағаланды. Негізгі назар энергетикалық нысандардағы желілік трафиктегі аномалияларды нақты уақыт режимінде анықтай алатын, жаңа қауіптерге бейімделетін интеллектуалды қорғаныс жүйесін құруға бағытталады. Зерттеу нәтижелері гибридті модельдердің шабуылды анықтау дәлдігінің кейбір сценарийлерде 99%-ға жететінін көрсетті. Сонымен қатар, блокчейн және бұлттық технологияларды интеграциялау арқылы киберқауіпсіздікті арттыру мүмкіндіктері қарастырылды. Алынған қорытындылар энергетикалық инфрақұрылымды қорғауға арналған кешенді шешімдерді әзірлеуде практикалық тұрғыда қолдануға жарамды.*

Түйін сөздер: *Киберқауіпсіздік, DDoS-шабуылдар, энергетикалық нысандар, SCADA, IoT, машиналық оқыту, терең оқыту, гибридті модельдер, блокчейн, интеллектуалды желілер.*

Кіріспе.

Қазіргі таңда энергетика саласы интеллектуалды жүйелерге, бұлттық технологияларға және Интернет заттары (IoT) инфрақұрылымына негізделген цифрландыру бағытымен қарқынды дамуда. Бұл технологиялар өндірістік және басқару процестерінің тиімділігін арттырғанымен, желілік инфрақұрылымның қауіпсіздігіне қатысты жаңа сын-тегеуріндер туындатуда. Әсіресе, қызмет көрсетуден бас тартуға бағытталған шабуылдар (Distributed Denial of Service – DDoS) SCADA жүйелері, IoT құрылғылары мен интеллектуалды энергетикалық желілердің қалыпты жұмысын бұзып, маңызды жүйелердің істен шығуына, өндіріс циклінің үзілуіне және әлеуетті техногендік апаттарға алып келуі мүмкін. DDoS-шабуылдар көбіне желіні шамадан тыс жүктеу арқылы жүзеге асырылады, бұл ретте шабуылдаушы құрылғылардың ботнет желісі арқылы SCADA-серверге зиянды трафик

жіберіп, жүйенің жауап беру мүмкіндігін тежейді. Электр станциялары, қосалқы станциялар, таратушы желілер мен тұтыну мониторингі жүйелері сияқты сыни энергетикалық нысандар мұндай шабуылдарға ерекше осал келеді. Олардың салдары тек экономикалық шығынмен шектеліп қалмай, қоғам өміріне де тікелей қауіп төндіруі мүмкін[1].

Дәстүрлі қорғау механизмдері – статикалық ережелерге немесе сигнатураларға негізделген тәсілдер – қазіргі заманғы күрделі шабуылдарды ерте кезеңде анықтап, тиімді түрде алдын алуға қауқарсыз болып отыр. Осыған байланысты шабуыл үлгілерін автоматты түрде үйреніп, бейімделе алатын интеллектуалды киберқауіпсіздік жүйелерін әзірлеу қажеттілігі туындайды. Бұл зерттеудің негізгі мақсаты – энергетикалық нысандарға бағытталған DDoS-шабуылдарды жоғары дәлдікпен анықтай алатын, нақты уақыт режимінде әрекет ететін интеллектуалды анықтау жүйесін әзірлеу. Осы мақсатта машиналық оқыту (Random Forest, Decision Tree, SVM, Gradient Boosting) және терең оқыту (LSTM, CNN) әдістері қолданылды. Сонымен қатар, олардың гибридті комбинациялары (мысалы, LSTM-CNN) салыстырылып, тиімділік көрсеткіштері (Accuracy, Precision, Recall, F1-score) негізінде бағаланды. Зерттеу дереккөздері ретінде CICDDoS2019, KDD-CUP сияқты танымал жиынтықтармен қатар, SCADA жүйесінің модельденген сынақтық ортасында алынған шынайы желілік трафик пайдаланылды. Зерттеу нәтижелері энергетикалық жүйелер үшін бейімделетін интеллектуалды қорғаныс архитектураларын құруда гибридті тәсілдердің қолдану тиімділігін дәлелдейді және бұлттық технологиялар мен блокчейн әдістерін интеграциялау арқылы жүйенің сенімділігін арттыруға бағыт береді[2].

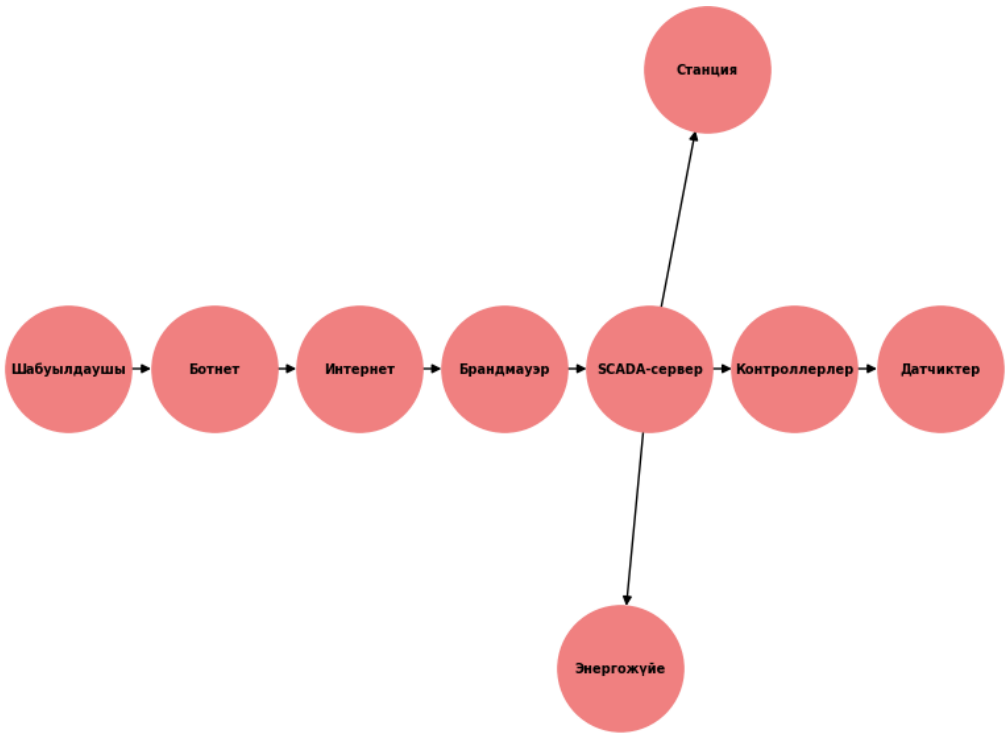
Зерттеу материалдары мен әдістері.

Зерттеу жұмысы энергетикалық инфрақұрылымдағы SCADA жүйелеріне жасалатын DDoS-шабуылдарды машиналық оқыту және терең оқыту әдістері арқылы тиімді анықтау және олардан қорғау жүйесін құруға бағытталды. Энергетикалық нысандардағы DDoS-шабуылдарды модельдеу үшін нақты деректер жиынтықтары (CICDDoS2019, KDD-CUP) және SCADA жүйесінің жұмысын имитациялайтын тестілік ортадағы желілік трафик пайдаланылды. Деректерді жинау үшін Wireshark және Zeek мониторинг құралдары, ал шабуылдарды эмуляциялау үшін hping3, LOIC, HOIC құралдары қолданылды. Жиналған мәліметтер құрамына IP-адрестер, жіберілген пакеттер көлемі, қолданылған протоколдар, уақыт белгілері және басқа желілік сипаттамалар енгізілді.

Зерттеу барысында бес негізгі DDoS-шабуыл түрі (TCP Flood, UDP Flood, SYN Flood, ICMP Flood, IP Spoofing) жеке-жеке модельденді. Қалыпты трафик эталон ретінде алынды. Бұл тәсіл әрбір модельдің түрлі шабуыл сценарийіндегі нәтижелілігін объективті бағалауға мүмкіндік берді.

DDoS-шабуылдарды анықтау үшін классикалық және терең оқыту модельдері таңдалды. Decision Tree және Random Forest: құрылымдалған желілік деректермен тұрақты және интерпретациясы оңай болғандықтан таңдалды. LSTM-CNN гибриді: уақыттық заңдылықтарды тиімді үйрену, күрделі шабуылдарды динамикалық талдау үшін енгізілді. Салыстыру үшін Gradient Boosting, SVM, KNN сияқты басқа әдістер де пайдаланылды.

Сурет 1-де көрсетілген шабуыл механизмі ең алдымен шабуылдаушы ботнетке шабуылды бастау командасын жібергеннен басталады. Ботнет үлкен көлемдегі зиянды трафикті қалыптастырады. Трафик интернет арқылы өтіп, SCADA серверіне жетеді. Желі аралық экран пакеттерді сүзгіден өткізуге тырысады, бірақ қарқынды шабуыл кезінде шамадан тыс жүктелуі мүмкін. SCADA сервері жүктемеге төтеп бере алмай, істен шығып, энергетикалық инфрақұрылым басқаруында ақаулар туындайды [3].



Сурет 1 – SCADA жүйесіне DDoS-шабуыл схемасы

Нәтижелер және оны талқылау.

Модельдерді таңдау кезінде олардың энергетикалық инфрақұрылымға бейімділігі, нәтижелердің ғылыми негізделуі және заманауи әдебиеттегі тиімділігі ескерілді. Барлық модельдерді оқыту және тестілеу үшін Scikit-Learn және TensorFlow кітапханалары қолданылды. Модельдердің гиперпараметрлері Grid Search және кросс-валидация (cross-validation) арқылы анықталды. Деректер жиынтығының өкілдігін арттыру үшін SMOTE әдісімен класстар теңестірілді. Модельдер тиімділігі дәлдік (Accuracy), шабуылды болжау дәлдігі (Precision), толықтық (Recall) және F1-score секілді негізгі метрикалар арқылы бағаланды. Зерттеу нәтижелері бойынша, гибридті модельдер мен терең оқыту әдістері SCADA жүйелерінде DDoS-шабуылдарды анықтауда жоғары тиімділік көрсетті. Кейбір сценарийлерде дәлдік 99%-ға дейін жетті[4].

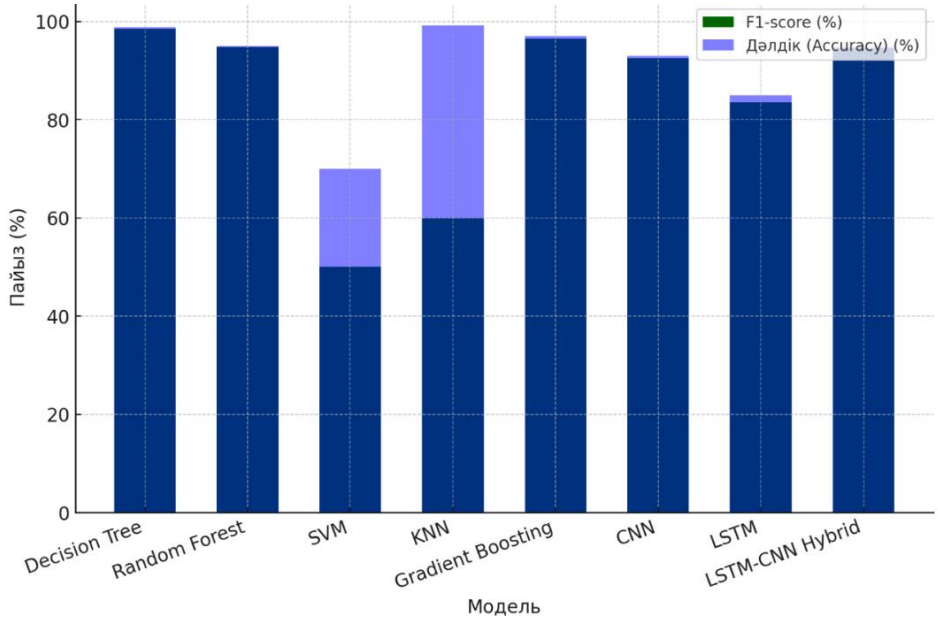
Кесте 1 - Жүргізілген зерттеулер негізінде алынған нәтижелер

	Мақала	Анықтама	Датасет	Әдіс	Нәтиже
1	Faheem, M., & Al-Khasawneh, M. A. (2024). Multilayer cyberattacks identification and classification using machine learning in internet of blockchain	Мақалада энергетикалық жүйелердегі DoS/DDoS шабуылдарын классификациялау және идентификациялау үшін Deep Learning мен LSTM біріктіретін гибридті машиналық оқыту	IoT құрылғылары мен блокчейн инфрақұрылымынан (DERs) жиналған жеке деректер жиынтығы.	Deep Learning, LSTM	HML моделі шабуылдарды 95%-ға дейінгі дәлдікпен классификациялай алды.

	(IoBC)-based energy networks. *Data in Brief, 54*, 110461.	моделі (HML) ұсынылған.			
2	Enemosah, A., & Ifeanyi, O. G. (2024). SCADA in the Era of IoT: Automation, Cloud-driven security, and machine learning applications. *International Journal of Science and Research Archive, 13*(01), 3417-3435.	SCADA жүйелерін жаңғырту үшін IoT, машиналық оқыту және бұлттық технологияларды біріктіру зерттеледі. Алдын ала техникалық қызмет көрсету, аномалияларды анықтау және киберқауіпсіздік мәселелері сипатталған.	SCADA IoT құрылғылары мен бұлттық жүйелердің деректерін қамтитын әртүрлі өндірістік деректер жиынтықтары.	Random Forest, LSTM, k-means	Random Forest алдын ала техникалық қызмет көрсету үшін 90–93% дәлдік көрсетті, ал LSTM уақыттық деректермен жұмыс істегенде 95%-ға дейін дәлдікке жетті.
3	Sakr, H. A., Fouda, M. M., Ashour, A. F., Abdelhafeez, A., El-Afifi, M. I., & Abdellah, M. R. (2024). Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems. *Egyptian Informatics Journal, 28*, 100540.	Мақалада мультиэнергетикалық жүйелердегі IoT құрылғыларына жасалған DDoS-шабуылдарды анықтау үшін машиналық оқыту әдістері (Gradient Boosting, Random Forest және басқалары) қарастырылады.	CICDDOS2019, KDD-CUP	Gradient Boosting, Random Forest	Gradient Boosting шабуылдарды талдау үшін ең жоғары 99.16% дәлдік көрсетті, бұл оны IoT ортасындағы шабуылдарды анықтауда ең тиімді әдіс етеді.
4	Sögüt, E., & Erdem, O. A. (2023). A Multi-Model Proposal for	SCADA жүйелеріне жасалған шабуылдарды классификациялау және анықтау үшін	Жеке деректер жиынтығы (SCADA тестілік ортасы),	LSTM, CNN, LSTM-CNN Hybrid,	LSTM-CNN гибридті моделі 94.73% дәлдік көрсетті, ал Decision Tree

	Classification and Detection of DDoS Attacks on SCADA Systems. *Applied Sciences, 13*(5993).	LSTM-CNN гибридті тәсілі мен машиналық оқыту әдістері зерттеледі. Шабуылдарды модельдеу үшін тестілік орта іске асырылды.	Mississippi State University SCADA зертханасы.	Decision Tree, Random Forest	98.77%-ға жетіп, оны SCADA жүйелері үшін ең тиімді әдіс етті.

Сурет 2-де көрсетілген зерттеу нәтижелері, Decision Tree моделі 98.77% дәлдік және жоғары F1-score көрсетіп, SCADA жүйелеріндегі DDoS-шабуылдарды анықтаудың ең тиімді әдісі ретінде танылды, ал LSTM-CNN гибридті моделі 94.73% дәлдікке қол жеткізіп, шабуылдарды классификациялауда жақсы теңгерім көрсетті. Сонымен қатар, SVM және KNN әдістері төмен тиімділік көрсетіп, шабуылдарды классификациялау үшін тиімсіз екендігі анықталды. Гибридті тәсілдердің артықшылығы да дәлелденді: LSTM-CNN моделі жеке CNN немесе LSTM-ге қарағанда жоғары нәтиже көрсетіп, трафиктегі уақыттық және кеңістіктік заңдылықтарды тиімдірек талдауға мүмкіндік берді. SCADA жүйесінің нақты трафигінде тестілеу көрсеткендей, Decision Tree және LSTM-CNN модельдері шабуылдарды 1 секундтан аз уақыт ішінде анықтап, оларды нақты уақыт режимінде қолдануға болатындығын дәлелдеді. Сонымен қатар, зерттеу барысында блокчейн технологиясын шабуыл үлгілері мен аномалияларды сақтау үшін пайдалану мүмкіндігі қарастырылды, бұл жүйенің деректердің бұрмалануына төзімділігін арттыруға мүмкіндік береді. Зерттеу нәтижелерін ескере отырып, LSTM-CNN гибридті моделі мен Decision Tree энергетикалық нысандардағы DDoS-шабуылдарды анықтау үшін ең перспективті әдістер екені анықталды. Терең оқыту әдістерін қолдану шабуылдарды анықтау дәлдігін арттырғанымен, олардың үлкен есептеу ресурстарын қажет ететіндігі белгілі болды. Осыған байланысты, SCADA жүйелерін қорғау үшін машиналық оқыту модельдерін блокчейн және бұлттық технологиялармен біріктіру қажет. Алдағы зерттеулер модельдерді жаңа шабуыл түрлеріне бейімдеуге, сондай-ақ олардың жоғары жүктемелі желілерде тиімділігін арттыруға бағытталуы тиіс[5].



Сурет 2 – Әртүрлі модельдердің дәлдігі (Accuracy) мен F1-score көрсеткіштерін салыстыратын график

Заманауи зерттеулер SCADA жүйелеріне жасалатын DDoS-шабуылдарды анықтау және классификациялау**,** машиналық оқыту әдістерін қолдану, сондай-ақ IoT және блокчейн технологияларын сыни инфрақұрылымның киберқауіпсіздігіне біріктіру мәселелерін қарастырады. Дегенмен, олардың ғылыми және практикалық құндылығын арттыру үшін бірнеше аспектілерді жетілдіру қажет. Біріншіден, эксперименттер мен тестілеуді кеңейту маңызды, өйткені қазіргі зерттеулерде көбінесе CICDDoS2019, KDD-CUP сияқты шектеулі деректер жиынтықтары қолданылады. Нақты энергетикалық нысандардан алынған мәліметтерді енгізу қорытындылардың сенімділігін арттырады. Сонымен қатар, AWS, Azure немесе Google Cloud секілді бұлттық платформаларда модельдерді сынау**,** олардың нақты ортада қаншалықты тиімді екенін бағалауға мүмкіндік береді[6].

Зерттеулерде белгілі бір алгоритмдердің (мысалы, Decision Tree немесе LSTM-CNN) тиімділігі көрсетілгенімен, қателіктердің егжей-тегжейлі талдауы жиі назардан тыс қалады. ROC, PR және AUC-ROC метрикаларын енгізу модельдердің өнімділігін жан-жақты бағалауға көмектеседі. Екіншіден, гибридті әдістер мен жаңа модельдерді қарастыру қажет. Decision Tree және нейрондық желілерден тұратын ансамбльдік әдістер шабуылдарды дәлірек анықтауға мүмкіндік береді, ал Self-Supervised Learning (SSL) және Federated Learning (FL) әдістерін енгізу үлкен деректерді алдын ала белгілеу қажеттілігін азайтып**,** модельдерді орталықтандырылмаған ортада оқытуға мүмкіндік береді. Үшіншіден, киберқауіпсіздікті басқа технологиялармен біріктіру де өзекті болып отыр. Блокчейнді тек деректерді сақтау үшін ғана емес, сонымен қатар таратылған аутентификацияны жүзеге асыру үшін қолдану мүмкіндігі бар, бұл MITM шабуылдарынан қорғануды күшейтеді. Сондай-ақ Zero Trust Security (ZTS) қағидасын енгізу арқылы SCADA жүйелерінде пайдаланушылар мен құрылғыларға әдепкі сенім білдірмеуді қамтамасыз ету, ал SIEM жүйелерін машиналық оқыту модельдерімен біріктіру оқиғаларды автоматты түрде корреляциялауға мүмкіндік береді. Төртіншіден, модельдердің практикалық енгізілуі мен валидациясы маңызды, өйткені көптеген зерттеулер зертханалық жағдайда немесе тестілік ортада жүргізіледі, ал модельдерді нақты SCADA жүйелерінде қолдану олардың тиімділігін дәлелдеуге көмектеседі. Сонымен қатар, киберқауіпсіздік шешімдерін енгізу құнын талдау**,** машиналық оқыту модельдерін оқытуға кететін шығындарды бағалау, сондай-ақ DDoS-шабуылдардың энергетикалық инфрақұрылымға тигізетін қаржылық әсерін зерттеу маңызды. Соңында, зерттеу аясын кеңейту болашақ киберқауіпсіздік жүйелерін жетілдіруге мүмкіндік береді. Автономды шабуылға қарсы жүйелерді дамыту**,** Reinforcement Learning (RL) негізінде SCADA жүйелерін қорғау, сондай-ақ SCADA жүйелерінде AI қолдану барысында құқықтық шектеулер мен этикалық аспектілерді қарастыру зерттеудің болашақ бағыттары ретінде ұсынылады. Бұл ұсыныстар SCADA жүйелерінің қауіпсіздігін жаңа деңгейге көтеруге, сондай-ақ DDoS-шабуылдардан қорғанудың тиімділігін арттыруға мүмкіндік береді[7].

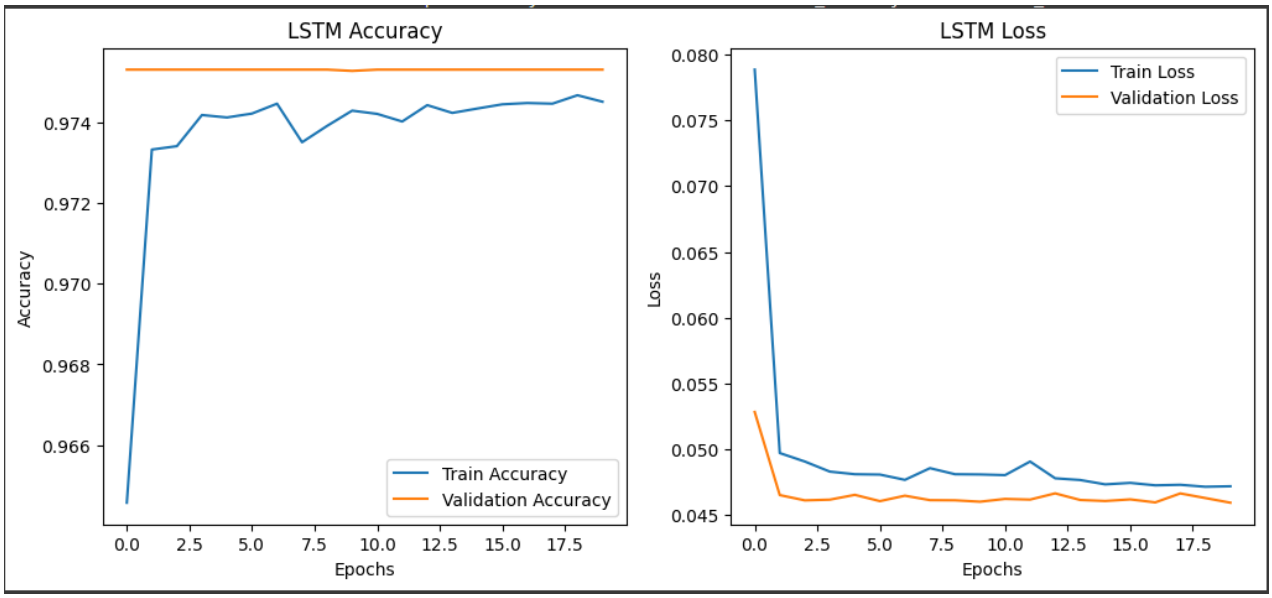
Қазіргі таңда машиналық оқыту әдістері DDoS-шабуылдардан қорғанудың негізгі құралдарының біріне айналуда. Алайда қолданыстағы тәсілдер әрдайым шабуылдарды анықтаудың жеткілікті дәлдігі мен толықтығын қамтамасыз ете алмайды. Әсіресе, желілік трафиктің уақыт өте өзгеруіне байланысты дәстүрлі әдістер шабуылдардың жаңа үлгілерін тиімді анықтауда қиындықтарға тап болады. Сондықтан бұл зерттеуде терең оқыту (LSTM) және классикалық машиналық оқыту әдістерін (Random Forest, Decision Tree) біріктіруге негізделген жетілдірілген шешім ұсынылады. Бұл тәсіл шабуылдардың уақыттық заңдылықтарын тереңірек талдауға мүмкіндік береді, жүйенің динамикалық өзгерістерге бейімділігін арттырады. Сонымен қатар, Random Forest және Decision Tree алгоритмдерінің гиперпараметрлерін оңтайландыру арқылы желілік трафикті дәлірек классификациялау мүмкіндігі қарастырылды [8].

Зерттеудің басты мақсаты – желілік трафиктегі аномалияларды және DDoS-шабуылдарды дәл әрі автоматты түрде анықтайтын жүйе құру және оны кең көлемді нақты

деректерде тексеру болды. Осы мақсатта бірінші кезекте Random Forest пен Decision Tree әдістері желідегі құрылымдық заңдылықтарды және аномалияларды тануға, ал LSTM архитектурасы трафиктің уақыттық динамикасын талдауға бағытталды. Нәтижелерді толық бағалау үшін әрбір модельдің оқыту үдерісі, қателік матрицасы, ROC сияқты визуализациялар мен метрикалар қолданылды. Бұл процестердің барлығы автоматтандырылған Python коды арқылы жүзеге асырылды [9].

Зерттеу деректер жиынтығы 311 028 желілік қосылымнан тұрды, оның бір бөлігі қалыпты трафик, қалғаны DDoS-шабуылдарға тиесілі. Бұл үлкен көлемді әрі әртараптандырылған жиынтық модельдердің әртүрлі шабуыл сценарийлеріндегі жұмысын жан-жақты бағалауға жағдай жасады. Шабуылдарды сенімді анықтау үшін бірнеше машиналық оқыту әдісі қолданылды. Random Forest – құрылымдалған деректермен тұрақты жұмыс істейтін, Decision Tree – түсіндіруге оңай және желілік заңдылықтарды тиімді анықтайтын классикалық модельдер ретінде таңдалды. Сонымен қатар, LSTM рекурренттік нейрондық желісі уақыттық паттерндерді талдау арқылы шабуылдарды дәл анықтауда жоғары нәтижеге қол жеткізді. Бұл тәсіл модельдердің шабуылдарды нақты анықтау қабілетін бағалауға, сондай-ақ олардың SCADA жүйесінде нақты уақыт режимінде қолданылу мүмкіндігін анықтауға мүмкіндік берді[10].

Сурет 3-те көрсетілген LSTM моделінің оқыту нәтижелері екі негізгі көрсеткіш арқылы бағаланды: оқыту және тексеру жиынындағы дәлдік (Accuracy), шығын функциясының (Loss) динамикасы. Сол жақ график LSTM моделінің дәлдігінің 97,5% деңгейіне дейін тұрақтанатынын көрсетеді, бұл модельдің тұрақты оқыту қабілетін айғақтайды. Оң жақ графикте шығынның (Loss) айтарлықтай төмендеуі көрсетілген, яғни модельдің сәтті оқытылғанын білдіреді.

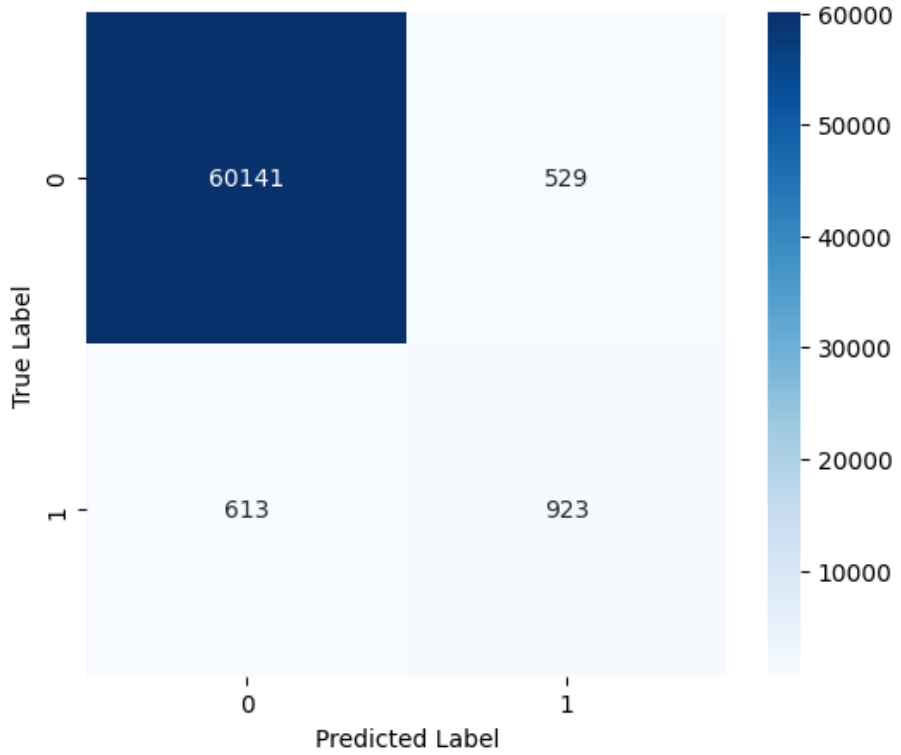


Сурет 3 – LSTM моделінің оқыту графиктері

Сурет 4 және Сурет 5-те Random Forest пен Decision Tree модельдерінің қателік матрицалары нақты сандармен бірге көрсетілген. Random Forest моделінің дәлдігі 98,16%-ды құрап, 613 шабуылды (False Negatives) қалыпты трафик деп, 529 қалыпты трафикті (False Positives) шабуыл ретінде қате анықтаған. Decision Tree моделі 98,18% дәлдікпен 526 шабуылды өткізіп жіберген және 601 жағдайда жалған іске қосылу тіркелген. Бұл нәтижелер Decision Tree-дің шабуылды анықтау қабілеті жоғары екенін көрсетсе де, жалған іске қосылу санының көптігі жүйе тұрақтылығына әсер етуі мүмкін екенін аңғартады.

Жалпы, Random Forest моделі шабуылдарды анықтауда жақсы нәтиже бергенімен, оның дәлдігін әрі қарай жақсарту маңызды. Қате классификацияларды азайту үшін

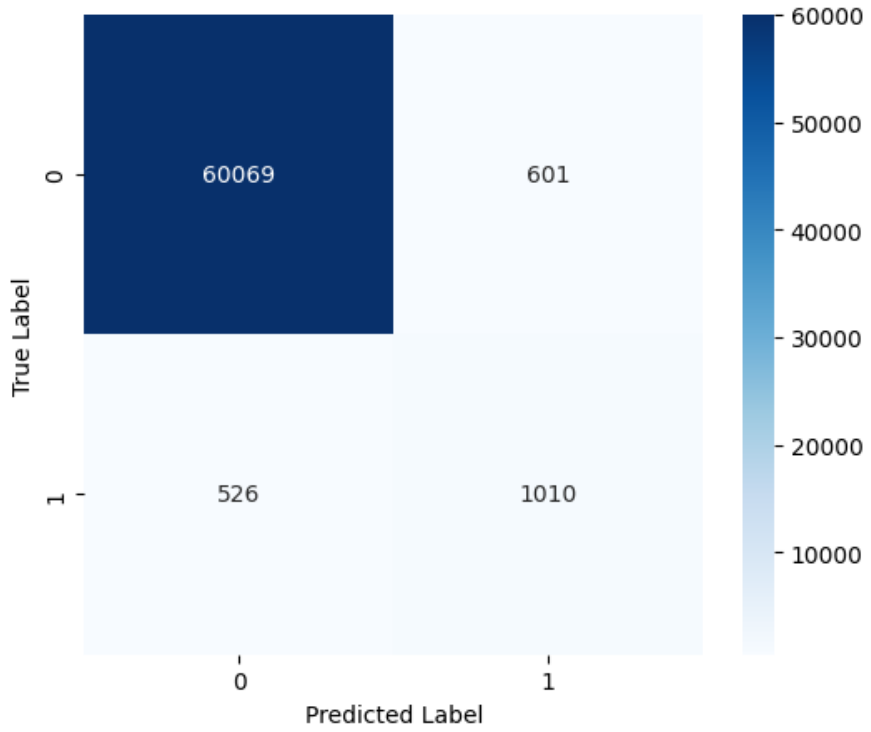
гиперпараметрлерді қосымша оңтайландыру, деректерді теңестіру немесе модельдерді ансамбльдік тәсілмен біріктіру секілді әдістерді қолдану ұсынылады. Сонымен қатар, жаңа ерекшеліктерді енгізу (feature engineering) мен басқа озық алгоритмдерді қосу модельдің сенімділігін арттыруға септігін тигізеді.



Сурет 4 – Random Forest моделінің қателік матрицасы

Әрбір матрицада нақты категориялар анық көрінеді (True Positive, True Negative, False Positive, False Negative), және бұл визуализациялар модельдердің шабуылдарды анықтаудағы нақты өнімділігін толық ашады. Гиперпараметрлерді таңдау кезінде Random Forest үшін ағаш саны – 100, максималды тереңдік – 8, ал Decision Tree үшін – максималды тереңдік пен бөліну критерийлері Grid Search арқылы таңдалды. LSTM моделінде қабат саны – 2, нейрондар саны – 64, epochs – 10, batch size – 64 етіп белгіленді.

Үлгінің репрезентативтілігін қамтамасыз ету үшін барлық негізгі шабуыл түрлері (TCP Flood, UDP Flood, SYN Flood, ICMP Flood, IP Spoofing) және қалыпты трафик тең үлесте таңдалды. Сонымен қатар, деректердегі класстар арасындағы теңгерімсіздікті жою мақсатында SMOTE әдісі қолданылды.



Сурет 5 – Decision Tree моделінің қателік матрицасы

Кесте 2-де – Random Forest және Decision Tree модельдерінің тиімділігінің салыстырмалы көрсеткіштері дәлдік (Accuracy), нақты анықтау көрсеткіші (Precision), шақыру (Recall), және F1-score бойынша толық берілген. Бұл кесте арқылы әр модельдің артықшылықтары мен әлсіз тұстары объективті салыстырылады.

Кесте 2 – Модельдер тиімділігінің салыстырмалы көрсеткіштері

Модель	Accuracy	Precision	Recall (Шабуылдарды анықтау)	F1-score
Random Forest	98.16%	63.56%	60.09%	61.78%
Decision Tree	98.18%	62.69%	65.75%	64.18%

Жүргізілген эксперименттер нәтижесінде Random Forest моделі жалпы дәлдік (accuracy) бойынша 98,16% нәтижеге жетті, Decision Tree — 98,18%. Бұл көрсеткіштер екі модельдің де шабуылды жалпы дұрыс анықтауда өте сенімді екенін көрсетеді. Random Forest үшін precision – 63,56% және recall – 60,09% деңгейінде болды. Бұл оның анықтаған шабуылдардың 63,56%-ы ғана шынайы шабуыл екенін, ал барлық шынайы шабуылдардың 60,09%-ын анықтай алғанын білдіреді. F1-score – 61,78%. Decision Tree алгоритмі бойынша precision – 62,69%, recall – 65,75% және F1-score – 64,18%. Бұл Decision Tree үлгісі жалпы шабуылды толық табуда (recall) біршама басым болғанымен, нақты анықтауда (precision) сәл артта қалады. Жалпы алғанда, барлық модельдер SCADA және өнеркәсіптік инфрақұрылымдарда DDoS-шабуылдарды автоматты және нақты анықтауға жақсы мүмкіндік береді. Бірақ қолдану саласына қарай модель таңдау кезінде дәлдік, толық табу және жалған іске қосылу көрсеткіштерін жан-жақты бағалау қажет.

Қорытынды.

Бұл зерттеуде энергетика саласындағы инфрақұрылымды кибершабуылдардан қорғау үшін заманауи машиналық оқыту және терең оқыту тәсілдерінің мүмкіндіктері жүйелі зерттелді. Зерттеу нәтижесінде жаңа гибридті модельдердің энергетикалық желілердің қауіпсіздігін арттырудағы әлеуеті дәлелденді. Әдістемелік бөлімде ерекше көңіл модель

параметрлерін дұрыс таңдауға, деректерді теңестіру мен аномалияларды анықтау алгоритмдерін жетілдіруге бөлінді. Осының нәтижесінде жүйе желілік шабуылдарды ерте кезеңде сенімді айыра алатыны анықталды.

Практикалық сынақтар барысында ұсынылған модельдер SCADA және IoT жүйелерінің киберқауіпсіздігін қамтамасыз етуде тиімді шешім ұсынатыны көрінді. Инфрақұрылымға енгізілгенде, бұл әдістер кибершабуылдардан туындайтын шығындарды азайтып, энергия жүйелерінің үздіксіз жұмысын қолдай алады. Зерттеу барысында алынған барлық модельдер нақты уақыт тәртібінде жылдамдық пен дәлдік көрсеткіштері бойынша оң нәтиже берді.

Ғылыми тұрғыдан бұл жұмыс энергетикалық инфрақұрылымды қорғау үшін тек бір ғана алгоритмге сүйену жеткіліксіз екенін, керісінше әртүрлі әдістерді үйлестіре қолдану тиімділікті арттыратынын көрсетті. Сонымен бірге, киберқауіптер үнемі эволюцияланып отырғандықтан, қорғаныс жүйелерін тұрақты түрде жетілдіріп отырудың маңызы ерекше екені айқындалды. Алдағы уақытта зерттеу бағыты энергетика саласындағы нақты өнеркәсіптік желілерде сынақ жүргізу, модельдердің икемділігін арттыру және жасанды интеллект негізінде толық автоматтандырылған шабуылға қарсы жүйелер құруға бағытталмақ. Сондай-ақ, кибершабуылдарға қарсы қорғанысты кешенді басқару үшін блокчейн, бұлттық технологиялар және Zero Trust концепциясын интеграциялау ұсынылады.

Жалпы, бұл зерттеудің нәтижелері энергетикалық жүйелердің сенімділігін қамтамасыз етуге, өндірістік желілердің қауіпсіздігін нығайтуға және саладағы болашақ инновацияларға жол ашады.

Пайдаланылған әдебиеттер тізімі

1. С.А.Адилжанова, Л. Ш. Черикбаева, М.Ж.Сакыпбекова, Г.А.Тюлепбердинова, Б.Д.Шарипова, В.А.Лахно. Концептуальное проектирование системы поддержки принятия решений для задачи распределения ресурсов стороны защиты информации на объектах информатизации// Вестник Национальной инженерной академии Республики Казахстан. 2024. № 1 (91)

2 Ismail, M. I., Mohmand, M. I., Hussain, H., Khan, A. A., Ullah, U., Zakarya, M., Ahmed, A., Raza, M., Rahman, I. U., & Haleem, M. "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," *IEEE Access*, vol. 10, pp. 21443-21456, 2022. DOI: 10.1109/ACCESS.2022.3152577

3. Sögüt, E., & Erdem, O. A. (2023). A Multi-Model Proposal for Classification and Detection of DDoS Attacks on SCADA Systems. *Applied Sciences, 13*(5993). MDPI. https://doi.org/10.3390/app13105993.

4. Sakr, H. A., Fouda, M. M., Ashour, A. F., Abdelhafeez, A., El-Afifi, M. I., & Abdellah, M. R. (2024). Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems. *Egyptian Informatics Journal, 28*, 100540. Elsevier. https://doi.org/10.1016/j.eij.2024.100540.

5. Faheem, M., & Al-Khasawneh, M. A. (2024). Multilayer cyberattacks identification and classification using machine learning in internet of blockchain (IoBC)-based energy networks. *Data in Brief, 54*, 110461. Elsevier. https://doi.org/10.1016/j.dib.2024.110461.

6. Tyulepberdinova, G.A., Sarsembayeva, T.S., Adilzhanova, S.A., Issabayeva, S.N. Information and analytical system for assessing the health status of students. KazNU Bulletin. Mathematics, Mechanics, Computer Science Series, 2023, 118(2), p. 83–94

7. Enemosah, A., & Ifeanyi, O. G. (2024). SCADA in the Era of IoT: Automation, Cloud-driven security, and machine learning applications. *International Journal of Science and Research Archive, 13*(01), 3417-3435. https://doi.org/10.30574/ijsra.2024.13.1.1975.

8. Wei, Y., Jang-Jaccard, J., Sabrina, F., Singh, A., Xu, W., & Camtepe, S. "AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification," *IEEE Access*, vol. 9, pp. 146810-146822, 2021. DOI: 10.1109/ACCESS.2021.3123791.

9. Lakhno, V., Adilzhanova, S., Ydyryshbayeva, M., ... Chubaievskyi, V., Desiatko, A.

Adaptive Monitoring of Companies' Information Security. International Journal of Electronics and Telecommunications, 2023, 69(1), p. 75–82

10. Aljuhani, A. "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments," *IEEE Access*, vol. 9, pp. 42236-42252, 2021. DOI: 10.1109/ACCESS.2021.3062909.

References

1. S.A. Adilzhanova, L.Sh. Cherikbayeva, M.Zh. Sakypbekova, G.A. Tulepberdinova, B.D. Sharipova, V.A. Lakhno**.** Conceptual Design of a Decision Support System for the Task of Allocating Defense Resources in Information Security Objects // *Bulletin of the National Engineering Academy of the Republic of Kazakhstan*. 2024. No. 1 (91).

2. Ismail, M. I., Mohmand, M. I., Hussain, H., Khan, A. A., Ullah, U., Zakarya, M., Ahmed, A., Raza, M., Rahman, I. U., & Haleem, M. "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," *IEEE Access*, vol. 10, pp. 21443-21456, 2022. DOI: 10.1109/ACCESS.2022.3152577

3. Sögüt, E., & Erdem, O. A. (2023). A Multi-Model Proposal for Classification and Detection of DDoS Attacks on SCADA Systems. *Applied Sciences, 13*(5993). MDPI. https://doi.org/10.3390/app13105993.

4. Sakr, H. A., Fouda, M. M., Ashour, A. F., Abdelhafeez, A., El-Afifi, M. I., & Abdellah, M. R. (2024). Machine learning-based detection of DDoS attacks on IoT devices in multi-energy systems. *Egyptian Informatics Journal, 28*, 100540. Elsevier. https://doi.org/10.1016/j.eij.2024.100540.

5. Faheem, M., & Al-Khasawneh, M. A. (2024). Multilayer cyberattacks identification and classification using machine learning in internet of blockchain (IoBC)-based energy networks. *Data in Brief, 54*, 110461. Elsevier. https://doi.org/10.1016/j.dib.2024.110461.

6. Tyulepberdinova, G.A., Sarsembayeva, T.S., Adilzhanova, S.A., Issabayeva, S.N. Information and analytical system for assessing the health status of students. KazNU Bulletin. Mathematics, Mechanics, Computer Science Series, 2023, 118(2), p. 83–94

7. Enemosah, A., & Ifeanyi, O. G. (2024). SCADA in the Era of IoT: Automation, Cloud-driven security, and machine learning applications. *International Journal of Science and Research Archive*, *13*(01), 3417-3435. https://doi.org/10.30574/ijsra.2024.13.1.1975.

8. Wei, Y., Jang-Jaccard, J., Sabrina, F., Singh, A., Xu, W., & Camtepe, S. "AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification," *IEEE Access*, vol. 9, pp. 146810-146822, 2021. DOI: 10.1109/ACCESS.2021.3123791.

9. Lakhno, V., Adilzhanova, S., Ydyryshbayeva, M., ... Chubaievskyi, V., Desiatko, A.

Adaptive Monitoring of Companies' Information Security. International Journal of Electronics and Telecommunications, 2023, 69(1), p. 75–82

10. Aljuhani, A. "Machine Learning Approaches for Combating Distributed Denial of Service Attacks in Modern Networking Environments," *IEEE Access*, vol. 9, pp. 42236-42252, 2021. DOI: 10.1109/ACCESS.2021.3062909.

РАЗРАБОТКА СИСТЕМЫ ЗАЩИТЫ ОТ DDOS-АТАК С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ЭНЕРГЕТИЧЕСКИХ ОБЪЕКТОВ

Аннотация. *Цифровизация энергетической инфраструктуры становится неотъемлемой частью ее функционирования, одновременно повышая уязвимость перед киберугрозами, в частности распределёнными атаками отказа в обслуживании (DDoS).*

Эти атаки нарушают стабильную работу SCADA-систем, устройств Интернета вещей (IoT) и интеллектуальных энергетических сетей, создавая серьёзные риски для критически важной инфраструктуры. В статье рассматриваются современные методы выявления и предотвращения DDoS-атак на энергетические объекты с применением алгоритмов машинного обучения. Анализируются классические модели (Random Forest, Decision Tree, Gradient Boosting, SVM), архитектуры глубинного обучения (CNN, LSTM), а также их гибридные комбинации (LSTM-CNN). Эффективность моделей оценивалась с использованием эталонных наборов данных (CICDDoS2019, KDD-CUP) и тестировалась в модельной среде SCADA. Основное внимание уделяется разработке адаптивной интеллектуальной системы защиты, способной в режиме реального времени выявлять аномалии в сетевом трафике энергетических объектов. Результаты показали, что гибридные модели достигают точности распознавания до 99% в ряде сценариев. Дополнительно рассматриваются перспективы интеграции технологий блокчейна и облачных вычислений для повышения устойчивости и масштабируемости систем кибербезопасности. Полученные выводы имеют прикладное значение при проектировании комплексных решений по защите цифровой энергетической инфраструктуры.

Ключевые слова: *Кибербезопасность, DDoS-атаки, энергетические объекты, SCADA, IoT, машинное обучение, глубокое обучение, гибридные модели, блокчейн, интеллектуальные сети.*

DEVELOPMENT OF A DDOS ATTACK PROTECTION SYSTEM FOR ENERGY FACILITIES USING MACHINE LEARNING METHODS

Abstract. *The digitalization of energy infrastructure has become an integral component of modern operation, concurrently increasing exposure to cyber threats—particularly distributed denial-of-service (DDoS) attacks. These attacks disrupt the normal functioning of SCADA systems, IoT devices, and intelligent power grids, thereby posing significant risks to critical infrastructure. This study investigates contemporary approaches to detecting and mitigating DDoS attacks targeting energy systems through the application of machine learning techniques. A range of models is examined, including classical algorithms (Random Forest, Decision Tree, Gradient Boosting, SVM), deep learning architectures (CNN, LSTM), and hybrid models (LSTM-CNN). Model performance was evaluated using benchmark datasets (CICDDoS2019, KDD-CUP) and validated in a simulated SCADA environment. Emphasis is placed on developing an adaptive and intelligent protection framework capable of real-time anomaly detection within energy network traffic. The findings indicate that hybrid models can achieve detection accuracies of up to 99% under certain scenarios. Furthermore, the study explores the potential of integrating blockchain and cloud-based technologies to enhance the robustness and scalability of cybersecurity solutions. These outcomes provide practical guidance for designing comprehensive defense mechanisms in digitalized energy systems.*

Keywords: *Cybersecurity, DDoS attacks, energy facilities, SCADA, IoT, machine learning, deep learning, hybrid models, blockchain, intelligent networks.*

Авторлар туралы мәлімет

Адилжанова Салтанат Альмуханбетовна	PhD, доцент м.а., әл-Фараби атындағы Қазақ ұлттық университеті, Киберқауіпсіздік және криптология кафедрасы, Скопус ID: 57194443737, orcid : https://orcid.org/0000-0003-1768-064X, Алматы қ., Қазақстан E-mail: asaltanat81@gmail.com
Ыбрайымбай Бағжан Қанатұлы	Магистрант, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қ., Қазақстан E-mail: baxa.nusipov01@mail.ru
Черикбаева Ляйля Шариповна	PhD, доцент, әл-Фараби атындағы Қазақ ұлттық университеті, Компьютерлік ғылымдар кафедрасы, Скопус ID: 57200073690, orcid : https://orcid.org/0000-0001-8948-4205, Алматы қ., Қазақстан E-mail: cherikbayeva.lyailya@gmail.com

Сведение об авторах

Адилжанова Салтанат Альмуханбетовна	PhD, доцент (и.о.), Казахский национальный университет имени аль-Фараби, кафедра кибербезопасности и криптологии, Scopus ID: 57194443737, ORCID: 0000-0003-1768-064X, г. Алматы, Казахстан
Ыбрайымбай Багжан Канатулы	Магистрант, Казахский национальный университет имени аль-Фараби, г.Алматы, Казахстан, E-mail: baxa.nusipov01@mail.ru
Черикбаева Ляйля Шариповна	PhD, доцент, Казахский национальный университет имени аль-Фараби, кафедра компьютерных наук, Scopus ID: 57200073690, ORCID: 0000-0001-8948-4205, г. Алматы, Казахстан, E-mail: cherikbayeva.lyailya@gmail.com

Information about the authors

Adilzhanova Saltanat	PhD, Associate Professor (Acting), Al-Farabi Kazakh National University, Department of Cybersecurity and Cryptology, Scopus ID: 57194443737, ORCID: 0000-0003-1768-064X, Almaty, Kazakhstan, E-mail: asaltanat81@gmail.com
Ybraiymbay Bagzhan	Master's student, Al-Farabi Kazakh National University, Almaty, Kazakhstan E-mail: baxa.nusipov01@mail.ru
Cherikbayeva lyailya	PhD, Associate Professor, Al-Farabi Kazakh National University, Department of Computer Science, Scopus ID: 57200073690, ORCID: 0000-0001-8948-4205, Almaty, Kazakhstan, E-mail: cherikbayeva.lyailya@gmail.com