

**Ш. Ж. МУСИРАЛИЕВА<sup>1</sup>, Г. Б. БАЙСПАЙ<sup>1\*</sup>, А. К. БЕКЕТОВА<sup>1</sup>**

<sup>1</sup>*Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы*

**ӘЛЕУМЕТТІК ЖЕЛІЛЕРДЕГІ КРИМИНАЛДЫҚ АҚПАРАТТАРДЫ  
ТАРАТУ ТОРАПТАРЫН СӘЙКЕСТЕНДІРУ ӘДІСІН ЗЕРТТЕУ ЖӘНЕ ҚҰРУ**

*Мақалада криминалдық ақпаратты тарату тораптарының қарым-қатынастарын графтық визуализациялау үшін алгоритм мен бағдарламалық қамтамасыз етуді әзірлеу қарастырылған. Желідегі қауымдастықтағы кілтті және ықпалды әсер етушілерді анықтау үшін әр түрлі әлеуметтік желілерді талдау әдістерін қолдану зерттелді. Графты талдау кезінде әлеуметтік желілерді талдау әдістерінің әртүрлі метрикалары бойынша талдау жүргізілді және дайын датасеттермен әдіс тиімділігі салыстырылды.*

**Түйін сөздер:** *әлеуметтік желілерді талдау әдісі, криминалдық ақпарат, тораптарды сәйкестендіру.*

**Кіріспе.** Соңғы 10 жылда бірнеше ұйымдасқан топтар, соның ішінде лаңкестер, белсенділер әлеуметтік желілерді өз идеяларын, жоспарларын жеткізу немесе қылмыстар туралы мақтану және хабарламалар тарату үшін пайдаланды. Криминология саласындағы сарапшылардың пікірінше, желілік әлемде ұйымдасқан кибер-қылмыскерлердің белсенділігі қарқынды дамып келеді [1-2].

Соның салдарынан соңғы жылдары экстремизм мәселесінің шиеленісуі байқалады, қазіргі уақытта оны Қазақстанның ұлттық қауіпсіздігіне қатер төндіретін және мемлекеттік маңызы бар мәселе ретінде қарастыруға болады. Қазіргі жағдайда маңызды екі міндетті атап өту керек, олардың шешімін әлеуметтік желідегі белгілі бір параметрлерді талдау арқылы табуға болады. Бірінші міндет – пайдаланушылардың белгілі бір тобында көшбасшыларды анықтау және екіншісі – профильдерді анықтау міндеті.

Желілерді талдау және модельдеу үшін әлеуметтік желілерді талдау (ӘЖТ) әдісі қолданылды. Алгоритмді әзірлеудің мақсаты ұйымдасқан топтардағы негізгі ойыншыларды, негізінен белсенділерді анықтауда қолдануға болатын ӘЖТ метрикасын зерттеу болып табылады. Алынған нәтижелер әдістің дұрыс жұмыс істеуін және орташа мәні 85% болатын нәтижелердің сенімділігін растайды.

**Алдыңғы зерттеулерге шолу.** Мақалада [3] авторлар қатысушылардың салыстырмалы бірлестігі негізінде желілерде ажыратылған қауымдастықтарды анықтау бойынша зерттеу нәтижелерін ұсынады. Бұл мақалада авторлар бөлек қауымдастықтарды анықтайтын DCD\_RAM (бөлінген қауымдастықты анықтау) деп аталатын гибриді жүйені ұсынады. Ол ішінара желіге орталықтандырылған, иерархиялық орталықтандырылған, шыңға орталықтандырылған және топтық орталықтандырылған тәсілдердің негізінде жатқан әдістерге негізделген. [4] еңбекте авторлар көп міндетті Гаусс копуласының үлгілерін пайдалана отырып, жасырын әлеуметтік желілердегі ықпалды түйіндерді табу мүмкіндігін талқылады. Қолданыстағы көптеген әдістер

---

\* E-mail корреспондирующего автора: [gulshat.bgb1@gmail.com](mailto:gulshat.bgb1@gmail.com)

желінің құрылымы априори толығымен белгілі деген болжамға негізделген. Дегенмен, көптеген қолданбаларда желі құрылымы ақпаратты таратудың негізгі құбылысын түсіндіру үшін қол жетімді емес. [5] ғылыми жұмыста авторлар әлеуметтік желілерді талдау арқылы киберқауіптерді анықтауды зерттеді. Мақалада киберқауіптерді анықтау үшін қолданылатын әлеуметтік желілерді талдаудың негізгі әдістеріне қысқаша шолу берілген. Әлеуметтік желілерге қауіптердің негізгі түрлері көрсетілген. Әлеуметтік желілерді талдаумен байланысты графиктер теориясының және деректерді өңдеудің негізгі әдістері сипатталған.

Мақалада [6] авторлар Facebook әлеуметтік желісіндегі белсенділердің онлайн топтарындағы негізгі қолданушыларды анықтауды зерттейді. Олар өз жұмыстарында Facebook желісіндегі белсенді топтағы пайдаланушылар арасындағы өзара әрекеттесу динамикасын түсіну үшін ӘЖТ әдістерін пайдаланады. Интернеттегі жиһадшылардың өшпенділік сөзін автоматтандырылған анықтау еңбегінде [7] жұмыста авторлар қылмыстық ұйымдардың ықпалды мүшелерінің қысқаша тізімін жасау және олардың маңызды байланыс арналарын анықтау әдісін ұсынады. Авторлардың пікірінше, қылмыстық ұйымда жеңіл жұмыс істейтін төменгі деңгейдегі қылмыскерлер тұтқынға алынады, ал жоғары деңгейдегі қылмыскерлер әдетте назардан тыс қалып жатады. [8] авторлар табиғи тілді өңдеу және машиналық оқыту әдістерін пайдалана отырып, 80%-дан астам дәлдікпен интернеттегі жиһадшылдық өшпенділік сөзін автоматты түрде анықтайтын жүйені әзірледі. Жүйе 2014 жылдың қазанынан 2016 жылдың желтоқсанына дейін жиналған 45 000 бұрыс ниетті Twitter хабарламаларының корпусында оқытылған.

Мақаланың негізгі материалы. Әлеуметтік желінің белсенді пайдаланушыларының байланыстарын графикалық визуализациялауға арналған алгоритм мен бағдарламалық қамтамасыз етуді әзірлеу үшін ең алдымен қауымдастықтарды таңдау туралы шешім қабылдау қажет болды. Бұл топтардың ақпараты мен контингенті визуализацияны құру кезінде пайдаланылады. Әрекет етуші пайдаланушылардың байланысын көрсететін жақсы және талданатын визуализация жасау үшін қазақтілді аудитория арасында белсенді қолданылатын әлеуметтік желі түрін таңдау міндеті қойылды. Зерттеу үшін пайдаланылған желілік белсенділердің деректер жинағы «В контакте» онлайн әлеуметтік желісіндегі діни топтардың жазбаларынан тұрады. Топтар негізінен үгітке қатысты ақпарат алмасуға және бірнеше қозғалыстарды насихаттауға бағытталған. Келесі қадам – топтарды тізімдеу. Жұмысқа Қазақстан Республикасының аумағында тыйым салынған топтар таңдалды. Іздестіру нәтижесінде Қазақстан Республикасының аумағында таралуына тыйым салынған тек 76 топ анықталды.

Желілерді талдау және модельдеу үшін әлеуметтік желіні талдау әдісі қолданылды. Әлеуметтік желілерді талдау – бұл графтар теориясының тұжырымдамаларын пайдалана отырып, әлеуметтік құрылымдарды зерттеу үшін қолданылатын әдіс. ӘЖТ әдістері әлеуметтік топтардың құрылымы мен мінез-құлқын зерттеу мен талдауда әсіресе пайдалы болып шықты. Әлеуметтік желіні талдау әдетте желінің құрылымдық қасиеттерін талдайтын статикалық әдістерді және/немесе уақыт бойынша әртүрлі желілік процестерді модельдеу үшін статистикалық әдістерді қолданатын динамикалық әдістерді қолдану арқылы нақты желілерді зерттеу үшін қолданылады. Сонымен қатар, орталықтылық көрсеткіштері сияқты ӘЖТ метрикасын пайдала-

ну қауымдастықтың құрылымын және желідегі негізгі қатысушыларды жақсырақ түсінуге мүмкіндік береді [9].

Жұмыстың мақсаты ұйымдасқан топтардағы негізгі ойыншыларды, криминалдык ақпаратты тарату тораптарын, негізінен белсенділерді анықтауға көмектесетін ЭЖТ көрсеткіштерін зерттеу болып табылады. Веб-форумдарды ұлттық және халықаралық белсенді топтар қозғалыстарды насихаттау және үгіт материалдарын тарату үшін жиі пайдаланады. Осы белсенді топтардың кейбірі бейбіт акцияларды ұйымдастырса, кейбіреулері мақсатты ұйымдар үшін кедергі мен қаржылық шығынға әкелуі мүмкін дұшпандық қозғалыстарға айналған.

Мәліметтерді визуализациялау және талдау мәселесі ақпараттың толып жатқан заманында өте маңызды. Ақпаратты қолмен талдау үшін автоматты талдау құралдарын да, визуализация құралдарын да пайдалана білу маңызды. Бұл жағдайда әдейі экстремистік мәтіндері бар топтардан ең ықпалды адамдарды таба білу керек. Деректерді талдау және визуализациялау әдістерінің алуан түрлілігі бар, бірақ графтар мен графтардағы алгоритмдерді пайдалана отырып, деректерді талдау мен визуализацияны таңдау туралы шешім қабылданды. Зерттеу жұмысында деректерді визуализациялау және талдау 4 бөліктен тұрады: мәліметтерді жинау, мәліметтерден граф салу, графты талдау және графты визуализациялау. Осылайша, авторлар ВКонтакте желісіндегі топтардың жазбаларының деректерін талдады. Бұл ретте екі түрлі граф құрастырылды.

Қауымдастықтағы жазбалар негізінде қолданушылардың графын құру.

*Деректерді жинау.* Үтірмен бөлінген топтар тізімін енгізу және осы топтардан қажетті жазбаларды қамтитын уақыт кезеңін көрсету арқылы пайдаланушылардың графын алуға болады. Мұнда деректерді жинау кезінде белгілі бір уақыт аралығында көрсетілген топтардың жазбалары, сондай-ақ пікір қалдырған пайдаланушылар туралы ақпарат жиналды. Атап айтқанда, тізімдегі әрбір топ үшін келесі қадамдардан тұратын `get_posts_if_reply` әдісі іске қосылды:

1. `Get_posts` әдісі арқылы топтың барлық жазбаларын алу. `get_posts` әдісі - жарияланым күні бойынша кему ретімен сұрыпталған хабарламалар тізімінде қажетті жазбалар қатарда пайда болатын жазбаны табу үшін екілік іздеу алгоритмін пайдалану. Осылайша, авторлар соңғысынан бастап барлық жазбаларды алудан гөрі жақсы өнімділікті қамтамасыз ете алды. Орташа алғанда, алгоритм қажетті жазбаны табуға  $\log_2 n$  уақыт жұмсайды, мұнда  $n$  - топтағы барлық жазбалардың саны.

2. Барлық хабарламаларды алғаннан кейін әрбір пост үшін оның барлық пікірлері `get_post_weights_if_reply` әдісімен алынады (1-сурет). Сонымен қатар, әрбір пікір үшін оның ішкі пікірлері (яғни, түсініктеме ағындары) да алынады.

Келесі кезекте осы деректер негізінде граф құрастырылады. Графты визуализациялау сұрауы қайта шақырылғанда көп уақытты қажет етпеуі үшін мәліметтер базасын пайдалану жоспарлануда.

***Посттардың астындағы пікірлерге негізделген графты құрастыру.***

Мұндағы пайдаланушы шын болады, ал жазбалар астындағы пікірлердің жалпы саны оның салмағы болып табылады. Шындардың арасындағы қабырғалар салмағы – пайдаланушылардың пікірлердегі өзара әрекеттесулерінің саны (яғни, бір пайдаланушыдан екіншісіне жауаптар саны немесе пайдаланушының басқа пайдаланушының

```

def get_post_weights_if_reply(self, postId, groupId):
    weightsList = []

    i = 0
    while True:
        addedToWeights = self.vk_api.wall.getComments(owner_id=groupId, post_id=postId, count=100,
                                                    offset=i * 100, v=5.92)['items']

        weightsList = weightsList + addedToWeights
        if len(addedToWeights) < 100:
            break
        i += 1
    comments = {}
    for comment in weightsList:
        nested_comments = self.get_thread(comment, postId, groupId)
        for key in nested_comments:
            if key in comments:
                comments[key] += nested_comments[key]
            else:
                comments[key] = nested_comments[key]
    return comments

def get_posts_if_reply(self, group, start_date, end_date):
    posts = self.get_posts(group, start_date, end_date, '')
    group = self.vk_api.groups.getById(group_id=group, v=5.92)
    for i in range(len(posts)):
        try:
            posts[i]['comments'] = self.get_post_weights_if_reply(posts[i]['id'], group_id)
        except:
            weight = {}
            posts[i]['comments'] = weight
    return posts

```

Сурет 1 – get\_posts\_if\_reply коды

түсініктеме ағынына қатысуы). Тиісінше, егер пайдаланушылар бір-бірімен әрекеттеспесе, онда қабырға болмайды.

Құрылған желіні талдау үшін NetworkX кітапханасының көмегімен граф салынды.

Графты талдау кезінде графтардың әртүрлі қасиеттері есептелді, мысалы: Degree Centrality, Closeness Centrality, Betweenness Centrality, Chi Squared, шыңдар саны, қабырға саны және графтың тығыздығы. Бұл қасиеттерді графтың оң жағынан көруге болады (2-сурет).



2-сурет – Топтар арасындағы байланыстар

Визуализация алгоритмін жасау үшін қылмыстық ұйымдардың ықпалды мүшелерінің қысқаша тізімін құру және олардың маңызды байланыс арналарын анықтау сынды әртүрлі әдістер зерттелді [3-10].

Нәтижесінде авторлар келесі тұжырымға келді: қылмыстық ұйымда жеңіл жұмыстарды орындайтын төмен деңгейдегі қылмыскерлер көбінесе қамауға алынады, ал жоғары деңгейдегі қылмыскерлер, әдетте, назардан тыс қалады. Бірақ тергеушілер ең ықпалды жоғары дәрежелі мүшелерді анықтап, олардың байланыс арналарын бақылай алмаса, қылмыстық ұйымдардың жұмысына нұқсан келтіру мүмкін емес. Желілік талдауды ең ықпалды қылмыскерлерді және желідегі маңызды байланыс арналарын анықтау үшін қолдануға болады, бірақ желідегі барлық түйіндер мен сілтемелерді тексеру көп еңбекті және көп уақытты қажет етеді. Авторлар жоғары деңгейдегі қылмыскерлерді тиімді түрде анықтай алатын және қылмыстық ұйымдағы маңызды байланыс арналарының қысқаша тізімін жасай алатын алгоритм жасады.

Авторлар жоғары деңгейдегі қылмыскерлер тарататын ақпарат ағынының жылдамдығының өзгеруі төменгі деңгейдегі қылмыскерлерге қарағанда баяу екенін байқады. Бұл зерттеушілерді командалар тізбегі жоғарылаған сайын ақпарат ағынының жылдамдығының тұрақтылығы артады деген болжамға алып келді. Яғни, ықпалды көшбасшылар ақпаратты аз ықпалдыларға қарағанда тұрақты таратады деп болжауға болады. Авторлар әдісі желі түйіндерінің кси-квадрат ( $\chi^2$ ) мәндерін есептеу арқылы жоғарыда келтірілген гипотеза негізінде қылмыстық ұйымның жоғарғы басшыларын анықтады. Жоғары  $\chi^2$  түйіндерімен ұсынылған қылмыскерлер ең жоғары көшбасшылар болып саналады. Ақырында, бұл әдіс осы аға басшылардан келетін маңызды байланыс арналарын анықтайды. Бұл арналарда қылмыстық ұйым туралы маңызды ақпарат болуы мүмкін.

Көптеген қасиеттерді NetworkX кітапханасынан алуға болады, бірақ Chi Squared алу арнайы алгоритм арқылы қолмен жүзеге асырылды. Ол үшін келесі алгоритм жүргізілді:

1. Әр шың үшін осы шыңның көршілерінен бастап соңын табуға дейінгі барлық жолдар табылады. Бұл ретте әрбір қадамда жолдағы келесі шыңды таңдау кезінде betweenness centrality ең жоғары мәні бар шың таңдалады.

2. Әрі қарай, әр шың үшін жолдардың әр деңгейіндегі максималды мән табылады. Мұнда жол деңгейі жолдың тереңдігін білдіреді (яғни, шыңның өзі - 0, ал көршісінің деңгейі - 1).

3. Әр жол үшін оның betweenness centrality қасиеті табылады, бұл оның шыңдарының betweenness centrality қосындысы.

4. Әрі қарай, әр жол үшін оның жергілікті Chi Squared көрсеткіші табылады.

5. Барлық жолдардың Chi Squared жиынтығы қосылып, сомасы сол шыңға беріледі.

Графтың осы қасиеттеріне сүйене отырып, графтың ең ықпалды шыңдарын табуға болады (3-сурет). Мысалы, ең үлкен Chi Squared, Closeness Centrality, Betweenness Centrality мәні бар пайдаланушыларды таңдау.



```
def fill_json_with_data(json_of_graph, graph):
    betweenness centrality, closeness centrality, chi_squared, significant_paths = data_from_graph(graph)
    print(betweenness centrality)
    json_of_graph["chi_squared"] = list((k: [k, v] for k, v in
        sorted(chi_squared.items(), key=lambda item: item[1],
            reverse=True)[:3]).items())
    json_of_graph["degree centrality"] = list((k: [k, v] for k, v in
        sorted(nx.degree centrality(graph).items(), key=lambda item: item[1],
            reverse=True)[:3]).items())
    json_of_graph["closeness centrality"] = list((k: [k, v] for k, v in sorted(closeness centrality.items(),
        key=lambda item: item[1], reverse=True)[
            :3]).items())
    json_of_graph["betweenness centrality"] = list((k: [k, v] for k, v in sorted(betweenness centrality.items(),
        key=lambda item: item[1],
            reverse=True)[
            :3]).items())
    print(json_of_graph["betweenness centrality"])
    json_of_graph["number_of_nodes"] = graph.number_of_nodes()
    json_of_graph["number_of_edges"] = graph.number_of_edges()
    json_of_graph["density"] = nx.density(graph)
```

Сурет 3 – Граф қасиеттерін табу

Әдістің өнімділігін тексеру үшін авторлар Кребстің 9/11 деректер жинағы, Caviar және ISIS Twitter деректер жинағын салыстырмалы түрде пайдалып, әртүрлі деректер жинақтарымен жұмыс істеді [11-13].

Krebs 9/11 деректер жинағы 11 қыркүйек оқиғасына қатысқан террористердің өзара әрекеттесуінің қысқаша мазмұны болып табылады. 9/11 бұл – 2001 жылы 11 қыркүйекте таңертең Америка Құрама Штаттарына жасалған төрт үйлестірілген лаңкестік шабуылдар сериясы. Krebs 9/11 деректер жинағы террористік шабуылдар жасады деп айыпталған адамдар арасындағы өзара әрекеттесуді көрсететін желіні қамтиды. Желіде қаскүнемдікке қатысқан лаңкестерді бейнелейтін 62 түйін бар. Ол террористердің өзара әрекетін бейнелейтін 153 сілтемені (қабырға) қамтиды. Түйіннің орташа дәрежесі – 4,9. Бір айлық тергеуден кейін Мохамед Аттаның қастандық жетекшісі екені «жалпыға белгілі» болды, ал Бен Ладен видеода Аттаның көшбасшылығын растады. Жарияланған диаграммаға қарасақ, оның ең көп байланыстары бар. 1-кестеде авторлар Atta желіні орталықтандырудың барлық көрсеткіштері – дәрежесі, жақындығы және аралығы бойынша ең жоғары ұпай жинап отырғанын байқады.

Кесте 1 – Krebs 9/11 dataset-імен әдіс тиімділігін тексеру

Chi squared		Betweenness centrality		Closeness centrality		Number of neighbours	
Djamel Benghal	3.26242172276	Mohamed Atta	0.5116174688	Mohamed Atta	0.4436090225	Mohamed Atta	15
Marwan Al-Shehhi	3.1787786902	Essid Sami Ben Khemail	0.2542463332	Marwan Al-Shehhi	0.3806451612	Marwan Al-Shehhi	12
Mohamed Atta	2.9242827813	Lofu Raissi	0.2395438900	Ziad Jarrah	0.3757961783	Essid Sami Ben Khemail	11
Nawaf Alhazmi	2.7732422698	Zacarias Moussaoui	0.2302941749	Lofu Raissi	0.3757961783	Nawaf Alhazmi	9
Hamza Alghamdi	2.6955048954	Hani Hanjour	0.2119382014	Ramzi Bin al-Shibh	0.3641975308	Ramzi Bin al-Shibh	9
Saeed Alghamdi*	2.5973693307	Nawaf Alhazmi	0.1443558908	Zacarias Moussaoui	0.3511904761	Djamel Benghal	9
Kamel Daoudi	2.5139378624	Ziad Jarrah	0.1318250552	Essid Sami Ben Khemail	0.3511904761	Ziad Jarrah	8
Hani Hanjour	2.4232179264	Djamel Benghal	0.1083576855	Mustafa Ahamed al-Hisawi	0.3410404624	Zacarias Moussaoui	8
Zacarias Moussaoui	2.3930157510	Ahmed Al Haznawi	0.1041901439	Said Bahaji	0.3352272727	Hani Hanjour	7
Rayed Mohammed Abdullah	2.3594769868	Marwan Al-Shehhi	0.0778938251	Imad Eddin Baraat Yarkas	0.3352272727	Said Bahaji	7

Degrees желі көрсеткіші желідегі Atta әрекетін көрсетеді. Жақындық оның желідегі басқаларға қол жеткізу және не болып жатқанын бақылау мүмкіндігін өлшейді, сонымен қатар, желідегі ағынды бақылауды көрсетеді – ол желіде брокер рөлін атқарады. Бұл көрсеткіштер оның көшбасшы мәртебесін растайды [11].

Caviar деректер қорымен әдіс тиімділігін және ISIS Twitter деректер жиынын қалай пайдаланатынын тексеру кезінде нәтижелер 94% дәлдікке ие болды. Әдісті 9/11 Кребс деректер жинағымен сынау кезінде қастандық жетекшісі Мохамед Аттаның Chi квадраттық ұпайы 2,924 болды, бұл орташа көрсеткіш. Авторлар осы әдіспен жұмыс істегенде деректердің дәлдігін арттырғысы келеді және қазіргі уақытта олар өз зерттеулерін жалғастырып жатыр.

**Қорытынды.** Зерттеу аясында белсенді қолданушылардың және ақпаратты тарату тораптарының қарым-қатынастарын графтық визуализациялау үшін алгоритм мен бағдарламалық камтамасыз етуді әзірлеу қарастырылды. Әлеуметтік желіні талдау әдістері мен визуализация кезеңдері талданды. Желідегі белсенді топтардағы кілтті және ықпалды әсер етушілерді анықтау үшін әр түрлі ӘЖТ әдістерін қолдану қарастырылды. Пайдаланушы графтары топтардағы жазбаларға, жазбалар астындағы пікірлерге негізделген. Графты талдау кезінде графтың әртүрлі қасиеттері есептелді, мысалы, Degree Centrality, Closeness Centrality, Betweenness Centrality, Chi Squared, шыңдар саны, қабырға саны және графтың тығыздығы.

Алғыс. Берілген мақала ҚР ЦДИАӨМ тапсырысы бойынша ғарыштық қызмет және ақпараттық қауіпсіздік саласындағы қолданбалы ғылыми зерттеулер бағытындағы “Мәтіндегі экстремистік бағытты анықтау үшін веб-ресурстардағы семантикалық талдау модельдерін, алгоритмдерін құрастыру және кибер-криминалистика құрал-жабдықтарын әзірлеу” жобасы аясында жазылды, ЖТН АР06851248.

## ӘДЕБИЕТ

1 Torregrosa J., Thorburn J., Raúl Lara-Cabrera, Camacho D. & Humberto Trujillo M. Linguistic analysis of pro-ISIS users on Twitter // Behavioral Sciences of Terrorism and Political Aggression. – 2019. – P.171-185.

2 Чесноков В.О. Применение алгоритма выделения сообществ в информационном противоборстве в социальных сетях // Вопросы кибербезопасности. – 2017. – №1 (19). – С. 37-44.

3 Taha K. Disjoint community detection in networks based on the relative association of members // IEEE Transactions on Computational Social Systems. – 2018. – P. 1-15.

4 Qunwei L., Kailkhura B., Thiagarajan J., Zhang Zh., Varshney P.K. Influential Node Detection in Implicit Social Networks using Multi-task Gaussian Copula Models // Journal of Machine Learning Research. – 2016. – No. 55. P. 27-37.

5 Kirichenko L., Radivilova T., Carlsson A. Detecting cyber threats through social network analysis: short survey // SocioEconomic Challenges. – 2017. – Vol. 1. P.20-34.

6 Nough M., Nurse J. Identifying Key-Players in Online Activist Groups on Facebook Social Network // IEEE Computer Society. – 2015. – P. 969-978.

7 Taha K., Yoo P.D. Shortlisting the influential members of criminal organizations and identifying their important communication channels // IEEE Transactions on Information Forensics and Security. – 2019. – Vol. 14. No. 8. P. 1988-1999.

8 Smedt T., Pauw G., Van O. P. Automatic Detection of Online Jihadist Hate Speech // Computational linguistics & psycholinguistics technical report series. – 2018. – P. 1-31.

9 Basu A. Social network analysis: A methodology for studying terrorism // Social Networking, ser. Intelligent Systems Reference Library. – 2014. – Vol. 65. P. 215–242.

10 Г.Б. Байспай, К. Багитова, Ш.Ж. Мусиралиева, А. Курманкожаева, Идентификация ключевых пользователей в социальных сетях по методу анализа социальных сетей, Вестник Казахской головной архитектурно-строительной академии, №2 (76), 2020 г.

11 Krebs's 9/11 dataset. - URL: <https://sites.google.com/site/ucinetsoftware/datasets/covert-networks/911hijackers> (дата обращения: 10.04.2022 г.).

12 Caviar dataset. - URL: <https://sites.google.com/site/ucinetsoftware/datasets/covert-networks/caviar> (дата обращения: 10.04.2022 г.).

13 How ISIS Uses Twitter dataset. – URL: <https://www.kaggle.com/fifthtribe/how-isis-uses-twitter> (дата обращения: 10.04.2022 г.).

## REFERENCES

1 Torregrosa J., Thorburn J., Raúl Lara-Cabrera, Camacho D. & Humberto Trujillo M. Linguistic analysis of pro-ISIS users on Twitter // Behavioral Sciences of Terrorism and Political Aggression. – 2019. – P.171-185.

2 Шесноков В.О. Применение алгоритма выделения сообществ в информационном противоборстве в социальных сетях // Вопросы кибербезопасности. – 2017. – №1 (19). – С. 37-44.

3 Taha K. Disjoint community detection in networks based on the relative association of members // IEEE Transactions on Computational Social Systems. – 2018. – P. 1-15.

4 Qunwei L., Kailkhura B., Thiagarajan J., Zhang Zh., Varshney P.K. Influential Node Detection in Implicit Social Networks using Multi-task Gaussian Copula Models // Journal of Machine Learning Research. – 2016. – No. 55. P. 27-37.

5 Kirichenko L., Radivilova T., Carlsson A. Detecting cyber threats through social network analysis: short survey // SocioEconomic Challenges. – 2017. – Vol. 1. P.20-34.

6 Nouh M., Nurse J. Identifying Key-Players in Online Activist Groups on Facebook Social Network // IEEE Computer Society. – 2015. – P. 969-978.

7 Taha K., Yoo P.D. Shortlisting the influential members of criminal organizations and identifying their important communication channels // IEEE Transactions on Information Forensics and Security. – 2019. – Vol. 14. No. 8. P. 1988-1999.

8 Smedt T., Pauw G., Van O. P. Automatic Detection of Online Jihadist Hate Speech // Computational linguistics & psycholinguistics technical report series. – 2018. – P. 1-31.

9 Basu A. Social network analysis: A methodology for studying terrorism // Social Networking, ser. Intelligent Systems Reference Library. – 2014. – Vol. 65. P. 215–242.

10 Г.Б. Байспай, К. Багитова, Ш.Ж. Мусиралиева, А. Курманкожаева, Идентификация ключевых пользователей в социальных сетях по методу анализа социальных сетей, Вестник Казахской головной архитектурно-строительной академии, №2 (76), 2020 г.

11 Krebs's 9/11 dataset. - URL: <https://sites.google.com/site/ucinetsoftware/datasets/covert-networks/911hijackers> (дата обращения: 10.04.2022 г.).

12 Caviar dataset. - URL: <https://sites.google.com/site/ucinetsoftware/datasets/covert-networks/caviar> (дата обращения: 10.04.2022 г.).

13 How ISIS Uses Twitter dataset. - URL: <https://www.kaggle.com/fifthtribe/how-isis-uses-twitter> (дата обращения: 10.04.2022 г.).



**Ш. Ж. МУСИРАЛИЕВА, Г. Б. БАЙСПАЙ, А. К. БЕКЕТОВА**

*Казахский национальный университет имени аль-Фараби, Алматы*

**ИССЛЕДОВАНИЕ И РАЗРАБОТКА МЕТОДА ВЫЯВЛЕНИЯ УЗЛОВ  
РАСПРОСТРАНЕНИЯ КРИМИНАЛЬНОЙ ИНФОРМАЦИИ  
В СОЦИАЛЬНЫХ СЕТЯХ**

*В статье предусмотрена разработка алгоритмов и программного обеспечения для графической визуализации взаимосвязи криминальных информационных сетей. Было изучено использование различных методов анализа социальных сетей для выявления ключевых и влиятельных лиц, оказывающих влияние в онлайн-сообществе. В ходе анализа графа был проведен анализ разных метрик методов анализа социальных сетей и проведено сравнение эффективности метода с готовыми данными.*

**Ключевые слова:** метод анализа социальных сетей, криминальная информация, идентификация узлов.

**SH. ZH. MUSSIRALIYEVA, G. B. BAISPAY, A. K. BEKETOVA**

*Al-Farabi Kazakh National University, Almaty*

**RESEARCH AND CREATION OF A METHOD FOR IDENTIFYING INFLUENTIAL  
SPREADERS OF CRIMINAL INFORMATION IN A SOCIAL NETWORK**

*The article provides for the development of algorithms and software for graphical visualization of the interconnection of criminal information networks. The use of various social network analysis techniques to identify key and influential spreaders in an online community has been explored. During the analysis of the graph, an analysis of various metrics of social network analysis methods was carried out and a comparison was made of the effectiveness of the method with ready-made data.*

**Key words:** social network analysis method, criminal information, node identification.