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

ӘОЖ 004.056
ҒТАХА 81.93.29
https://doi.org/10.53364/24138614_2026_40_1_13

С. А. Адилжанова[1], **А. Е. Рахыш**[1*]
[1]Әл-Фараби атындағы Қазақ Ұлттық университеті, Қазақстан, Алматы

[*]*E-mail: rakhysh_aigerim3@live.kaznu.kz*

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНДАҒЫ КИБЕРҚАУІПСІЗДІК ИНЦИДЕНТТЕРІН МАТЕМАТИКАЛЫҚ МОДЕЛЬДЕУ

Аңдатпа. *Бұл мақалада Қазақстан Республикасындағы киберомнциденттердің уақыттық динамикасы зерттеліп, алдыңғы қатарлы цифрлық мемлекеттермен (АҚШ, Сингапур) салыстырмалы талдау жүргізілді. Зерттеудің әдістемелік негізі ретінде уақыттық қатарларды талдаудың эконометрикалық құралдары: толықтырылған Дикки-Фуллер тесті (ADF), Йохансен (Johansen) коинтеграциялық тесті және Векторлық авторегрессия (VAR) моделі қолданылды. KZ-CERT деректеріне (2015–2025 жж.) жүргізілген талдау нәтижесінде ботнет желілерінің таралуы стационарлы және тұрақты жоғары деңгейде екені анықталды. Вирустар мен фишингтік шабуылдардың да өсімі байқалды. АҚШ (FBI IC3) және Сингапур (CSA) есептерімен салыстыру барысында Қазақстанда инфрақұрылымдық және техникалық сипаттағы қауіптердің басым екендігі, ал дамыған елдерде әлеуметтік инженерия мен мақсатты шабуылдардың үлесі жоғары екендігі айқындылды. Python программалау тіліндегі (pandas, statsmodels) есептеулер негізінде 2026–2028 жылдарға қысқа мерзімді болжам жасалып, ұлттық киберқауіпсіздік жүйесін жетілдіру бойынша ғылыми негізделген ұсыныстар берілді.*

Түйін сөздер: *киберқауіпсіздік, математикалық модельдеу, VAR моделі, ADF тесті, ботнеттер, фишинг, салыстырмалы талдау.*

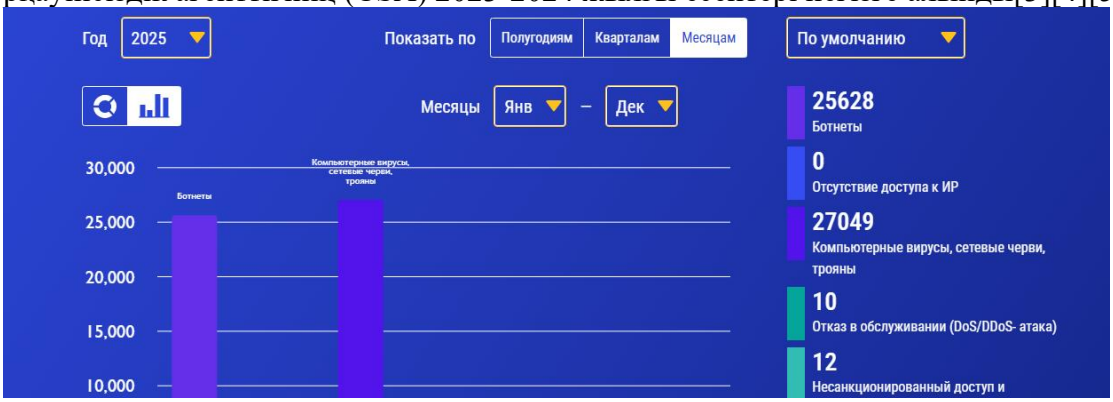
Кіріспе.

Қазіргі заманда ақпараттық жүйелердің жетілдірілуі, жасанды интеллект сияқты ірі технологиялық ашылулар адам өміріне тікелей әсер етуде. Әсіресе, мемлекеттік маңызы бар кибер-физикалық жүйелердің жаппай цифрландыру, атап айтқанда онлайн банкинг, электрондық үкімет, телекоммуникациялық инфрақұрылымдардың цифрлы ортаға көшуі сәйкесінше, кибершабуылдардың да легін арттырды. Кибершабуылдар ұлттық қауіпсіздікке өз қатерін төндіруі мүмкін[1].

Қазақстан Республикасында ақпараттық-коммуникациялық жүйені қорғау «Киберқауіпсіздік тұжырымдамасы» (Қазақстанның киберқалқаны) саясаты арқылы жүзеге асырылғанымен, бұл бағыттағы ғылыми жұмыстардың едәуір бөлігі қолжетімді емес[2]. Мемлекеттік инфрақұрылым нысандарына қатысты статистикалық материалдар құпия болғандықтан, киберқауіпсіздік жағдайын бағалау ашық, қолжетімді және жанама ақпараттарға сүйенеді.

Ашық дереккөздерден ең сапалы мәліметтерді Ұлттық компьютерлік оқиғаларға әрекет ету қызметы (KZ-CERT) тарапынан жарияланған статистикалық мәліметтерден табуға болады(1-сурет). Сайтта кибероқиғалардың әр жылдардағы динамикасы көрсетілген. Салыстырмалы талдау үшін АҚШ-тың Федералдық Тергеу Бюросының

Интернеттегі қылмыстарға шағымдану орталығы (FBI IC3) және Сингапурдың Киберқауіпсіздік агенттігінің (CSA) 2023-2024 жылғы есептері негізге алынды[3][4][5].



Сурет 1 – K z-cert сайтындағы статистикалық мәліметтер

Киберқауіп динамикасы уақыт бойынша өзгеріп, құбылып отырады. Ботнеттер, вирустар, зиянды бағдарламалардың таралуы, фишингтік шабуылдар, қызмет көрсетуден бас тарту (Denial of Service – DoS/DDoS) сияқты кибершабуылдар бір-бірімен байланысты динамикалық жүйе қалыптастырады.

Мұндай динамикалық жүйеге негізделген статистикалық мәліметтерді математикалық модельдер тұрғызу арқылы талдау жақсы нәтиже береді. Оның ішінде ADF (Augmented Dickey-Fuller) тесті, Johensen коинтеграциялық моделі, VAR(Vector AutoRegression) математикалық модельдері киберқауіпсіздік көрсеткішінің уақытқа байланысты қасиеттерін, ұзақ мерзімді байланыстарын анықтауға және оларды болжауға мүмкіндік береді.

Зерттеудің мақсаты соңғы онжылдықтағы Қазақстан Республикасындағы кибероқиғаларды уақыттық динамика бойынша талдап, негізгі қауіп түрлерінің арасындағы байланысты анықтау. Зерттеу дәл әрі нақты болуы үшін KZ-CERT сайтынан алынған статистикалық мәліметтердің барлығы нормализацияланды. Стационарлығы ADF тесті арқылы, ұзақ мерзімді тәуелділіктер Johensen әдісімен, болжамдар VAR моделі арқылы есептелді.

Зерттеудің ғылыми жаңалығы - Қазақстанның киберқауіпсіздік жағдайын динамикалық тұрғыдан талдап, ботнет, вирус, фишинг шабуылдары арасындағы байланысты сандық түрде дәлелдеу. Алынған нәтижелер ұлттық киберқауіпсіздік жүйесін бағалау, тәуекел индексін қалыптастыру үшін тәжірибелік маңызға ие.

Материалдар мен зерттеу әдістері.

Зерттеуде Қазақстан Республикасындағы киберқауіпсіздік инциденттерінің уақыттық динамикасын сандық тұрғыдан талдау және негізгі қауіп түрлерінің өзара байланысын анықтау үшін эконометрикалық модельдеу әдістері қолданылды. Зерттеуге пайдаланылатын деректер 1-кестеде көрсетілген.

Кесте 1 – Kz-cert сайтынан алынған статистикалық деректер

Көрсеткіш / Жыл	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
Ботнеттер	17150	18959	22899	17724	17300	12670	4 304	2 194	4 040	10676	25628
Интернет ресурстарға қолжетімділіктің болмауы	0	0	1 065	797	1 075	2 937	1 959	1 258	1 090	0	0
Компьютерлік вирустар, желілік құрттар, трояндар	120	114	360	313	409	2500	11923	10869	21940	16177	27049
Қызмет көрсетуден бас тарту (DoS/DDoS-шабуыл)	21	10	43	42	201	290	264	218	152	22	10
Рұқсатсыз қол жеткізу және мазмұнын түрлендіру	503	1 336	915	1 082	258	293	272	407	329	43	12

Интернет желісіндегі фишинг	195	128	106	199	883	1 392	658	1 242	2 160	680	1 077
Қалған инциденттер	0	0	0	0	0	0	0	466	4 770	415	212
Барлығы	17989	20547	25388	20157	20126	20082	19380	16654	34481	28013	53988

Жиналған деректер базасымен жұмыс жасау үшін оларды нормализациялау қажет, себебі, DDoS, ботнет шабуылдарының мәні үлкен, ал DoS шабуылының мәні олармен салыстырғанда аз. Егер деректерді модельге енгізсек, үлкен мәндер кіші шамаларды басып кетеді.

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \quad (1)$$

Мұндағы X-бастапқы уақыттық қатардың мәні, X_{min}, X_{max} – қатардың ең кішкентай және ең үлкен мәндері.

Кесте 2 – Нормализацияланған статистикалық деректер

Жыл	Ботнеттер	ИР-ға қолжетімсіздік	Вирустар	DoS/DDoS	Рұқсатсыз қол жеткізу	Фишинг	Қалған инциденттер
2015	0.669	0.000	0.004	0.072	0.377	0.090	0.000
2016	0.740	0.000	0.004	0.034	1.000	0.059	0.000
2017	0.894	0.363	0.013	0.148	0.685	0.049	0.000
2018	0.692	0.271	0.012	0.145	0.810	0.092	0.000
2019	0.675	0.366	0.015	0.693	0.193	0.409	0.000
2020	0.494	1.000	0.092	1.000	0.219	0.645	0.000
2021	0.168	0.667	0.441	0.910	0.204	0.305	0.000
2022	0.086	0.428	0.402	0.752	0.305	0.575	0.098
2023	0.158	0.371	0.811	0.524	0.246	1.000	1.000
2024	0.417	0.000	0.598	0.076	0.032	0.315	0.087
2025	1.000	0.000	1.000	0.034	0.009	0.499	0.044

ADF (Augmented Dickey–Fuller) тесті, Johansen коинтеграциялық талдауы және VAR (Vector AutoRegression) моделі киберқауіпсіздік көрсеткіштерінің уақыттық динамикасын зерттеуде маңызды эконометрикалық әдістер болып табылады. Бұл тәсілдер зерттеу барысында деректердің статистикалық қасиеттерін, олардың ұзақ мерзімді және қысқа мерзімді байланыстарын, сондай-ақ өзара әсер ету бағыттарын анықтау мақсатында қолданылады.

ADF тестінің негізгі мақсаты – уақыттық қатардың стационарлық сипатын тексеру. Киберқауіпсіздік саласында бұл көрсеткіштер, мысалы ботнеттер, фишинг шабуылдары немесе зиянды бағдарламалардың таралуы, уақыт бойынша айтарлықтай өзгерістерге ұшырайды және көбінесе өсу немесе төмендеу трендін көрсетеді. Стационарлық қатар дегеніміз – уақыт бойынша өзгеріссіз қатар. Егер қатар стационарлы болмаса, онда оның болжамдық қасиеттері сенімсіз болады. Осыны тексеру үшін ADF тесті қолданылады[6]. Бұл тест кездейсоқ секірістер мен жүйелі өсудің немесе кемудің бар-жоғын айқындайды. Киберқауіпсіздік көрсеткіштері көбіне экспоненциалды өсуге бейім болғандықтан, олардың стационарлығын тексеру модельдеу алдында деректерді дұрыс құрылымдау үшін қажет.

Зерттеуде ADF тесті 2015–2025 жылдар аралығындағы Қазақстандағы негізгі киберқауіп көрсеткіштерінің — ботнеттер, вирустар, фишинг, DDoS және рұқсатсыз қол жеткізу — стационарлық дәрежесін анықтау үшін қолданылды. Әр көрсеткіштің уақыт бойынша трендтік мінез-құлқын бағалау арқылы киберқауіптердің динамикалық табиғатын, яғни тұрақты немесе экспоненциалды өсу үрдісін анықтау мақсат етілді.

$$\Delta Y_t = \alpha + \gamma Y_{t-1} + \sum_{i=1}^{p} \delta_i \Delta Y_{t-1} + \varepsilon_t \quad (2)$$

Мұндағы : α -тұрақты компонент, γ бірлік түбір параметрі, δ_i лагтар бойынша түзетуші коэффициенттер, ε_t кездейсоқ қате.

Johansen коинтеграциялық тесті бірнеше уақыттық қатардың ұзақ мерзімді статистикалық тәуелділігін анықтау үшін қолданылады. Мысалы, ботнеттердің көбеюі мен фишинг оқиғаларының жиілеуі бір-бірімен байланысты болуы мүмкін, себебі олар ортақ киберқауіп экожүйесінің элементтері. Егер әр қатар жеке алғанда стационарлы болмаса, бірақ олардың сызықтық комбинациясы стационарлы болса, онда бұл қатарлар коинтеграцияланған деп есептеледі. Johansen әдісі көп айнымалылы жүйелердегі коинтеграциялық векторларды анықтауға мүмкіндік береді және олардың арасындағы ұзақ мерзімді тепе-теңдік байланысын сипаттайды. Бұл тәсіл α және β параметрлерінің көмегімен жүйенің теңгерімге қайтарылу жылдамдығын бағалауға мүмкіндік береді. Киберқауіпсіздік тұрғысынан алғанда, мұндай талдау әртүрлі қауіп түрлерінің өзара байланысын, мысалы зиянды бағдарламалардың артуының фишинг және DDoS шабуылдарына ұзақ мерзімді әсерін анықтауға жағдай жасайды. Осылайша, Johansen тесті зерттелетін жүйенің ұзақ мерзімді теңгерімді дамуын статистикалық негізде дәлелдеуге мүмкіндік береді.

$$\Delta Y_t = \Pi Y_{t-1} + \sum_{i=1}^{p-1} \Gamma_i \Delta Y_{t-i} + \varepsilon_t \qquad (3)$$

Мұндағы Y_t – көпөлшемді уақыттық қатар векторы, Γ_i қысқа мерзімді динамиканы сипаттайтын коэффициенттер, ε_t кездейсоқ қателер векторы, П ұзақ мерзімді тәуелділікті сипаттайтын матрица.

VAR моделі бірнеше айнымалының өзара динамикалық тәуелділігін талдау үшін қолданылады. Бұл модельде барлық айнымалылар эндогенді, яғни әрбір көрсеткіш басқа көрсеткіштердің кешігу мәндері арқылы түсіндіріледі. VAR моделі уақыт бойынша өзара әсер ету бағытын және осы әсердің қарқындылығын бағалауға мүмкіндік береді. Модельдің жалпы түрі векторлық авторегрессия теңдеулері жүйесі арқылы сипатталады, мұнда әр айнымалының ағымдағы мәні оның өзге айнымалылардың кешіктірілген мәндерінен тәуелді болады[7]. Киберқауіпсіздік контекстінде VAR моделі ботнеттердің көбеюі фишинг немесе вирустардың таралуына қалай әсер ететінін және бұл өзара байланыстардың уақытша лагтар арқылы қалай жүзеге асатынын анықтауға мүмкіндік береді. VAR нәтижелерінің негізінде қай айнымалылар жетекші, ал қайсысы жауап беруші факторлар екені айқындалады. Бұл өзара тәуелділіктерді талдау арқылы киберқауіптердің эволюциясын болжауға және ұлттық қауіпсіздік жүйесінің әлсіз тұстарын сандық тұрғыдан анықтауға болады.

Нәтижелер және оларды талқылау.

2015–2025 жылдардағы деректерде орташа мән оң және нөлден айтарлықтай алшақ (мысалы, ботнеттер, вирустар мыңдық шамаларда) және бірақ жылдық өсім немесе уақыттық тренд сызықтық сипатта емес (бірнеше жылда күрт секіру бар) болғандықтан ADF тестінің константалық моделі таңдалды. Бұл жағдайда қатар нөл маңында тербелмейді, бірақ анық тренд те байқалмайды.

Барлық есептеулер Python программалау тілінде жүзеге асырылып, деректерді өңдеу және модельдеу үшін pandas, numpy және statsmodels кітапханалары қолданылды[8].

```
result = adfuller(series, regression='c', autolag='AIC')
output = {
    "Көрсеткіш": series_name,
    "ADF статистикасы": round(result[0], 4),
    "p-мән": round(result[1], 4),
    "Лаг саны": result[2],
    "Бақылау саны": result[3],
    "Стационарлық": "Иә" if result[1] < 0.05 else "Жоқ"
}
return output
```

Сурет 2 – ADF моделінің реализациясы

ADF тестінің нәтижелері (2015-2025):

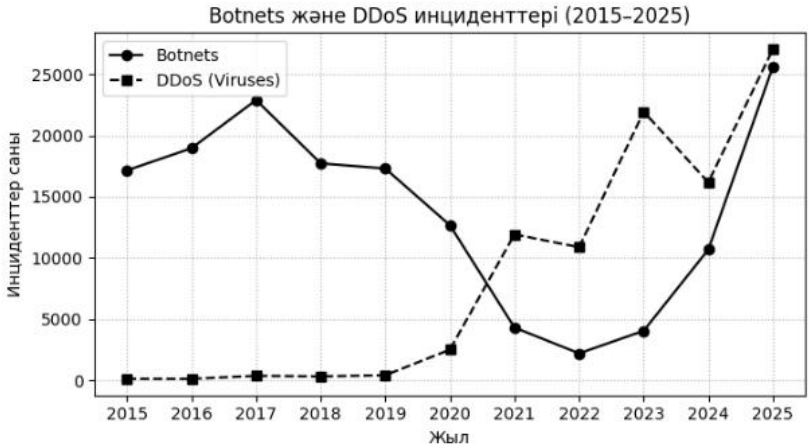
Көрсеткіш	ADF статистикасы	p-мән	Лаг саны	Бақылау саны	Стационарлық
Botnets	-6.0884	0.0000	3	7	Иә
Access_Failure	-2.6339	0.0862	3	7	Жоқ
Viruses	-0.7486	0.8337	2	8	Жоқ
DDoS	-7.3711	0.0000	3	7	Иә
Unauthorized	-2.6511	0.0829	3	7	Жоқ
Phishing	-2.4985	0.1158	3	7	Жоқ
Other	20.5358	1.0000	2	8	Жоқ

Сурет 3 – ADF моделі бойынша нәтижелер

Сурет 3-те ADF тестінің сандық нәтижелері берілген. Нәтижелер бойынша Botnets және DDoS қатарлары үшін p-мән 0,05-тен төмен, бұл олардың стационарлы екенін көрсетеді.

Ал Viruses, Phishing және басқа айнымалылар үшін p-мән 0,05-тен жоғары болып, олардың бірлік түбірге ие екенін, яғни стационарлы емес екенін дәлелдейді. Бұл көрсеткіштерде ұзақ мерзімді трендтің бар екенін білдіреді.

Аталған айырмашылық киберқауіп түрлерінің даму табиғаты әртүрлі екенін көрсетеді: кейбір қауіптер тұрақты деңгейде сақталса, басқалары экспоненциалды өсімге бейім. Бұл ботнеттер мен қызмет көрсетуден бас тарту шабуылдарының жиілігі соңғы онжылдықта белгілі бір диапазонда тербеліп отырған, бұл олардың статистикалық тұрақтылығын көрсетеді.



Сурет 4 – Botnet және DDoS көрсеткіші

Сурет 4-те Botnet және DDoS уақыттық динамикасы графикалық түрде ұсынылған. Қатарлардың тербеліс амплитудасы шектеулі диапазонда сақталған. Бұл олардың дисперсиясының тұрақтылығын және жүйелі экспоненциалды трендтің жоқтығын

көрсетеді. Аталған киберқауіптердің графиктері ADF тесті нәтижелерімен сәйкес келеді және бұл қауіптердің статистикалық тұрақтылығын растайды.

Сонымен қатар, көрсеткіштердің белгілі бір деңгейден төмен түспеуі желілік инфрақұрылымда тұрақты осалдықтардың бар екенін көрсетеді.

Ал қалған көрсеткіштер — Access_Failure, Viruses, Unauthorized, Phishing және Other — үшін алынған p-мәндер 0,05-тен жоғары, сондықтан бұл қатарлар стационарлы емес. Бұл олардың уақыт бойынша орта мәні мен дисперсиясы өзгеретінін, яғни қатарларда айқын тренд бар екенін білдіреді. Мұндай нәтижелер аталған бағыттарда киберқауіптердің біртіндеп артып келе жатқанын көрсетеді. Мысалы, вирустар мен фишинг шабуылдары жыл сайын тұрақты өсіп, ақпараттық инфрақұрылымның осал тұстарын айқындайды.

Johansen коинтеграциялық тесті (Botnets, Viruses, Phishing):

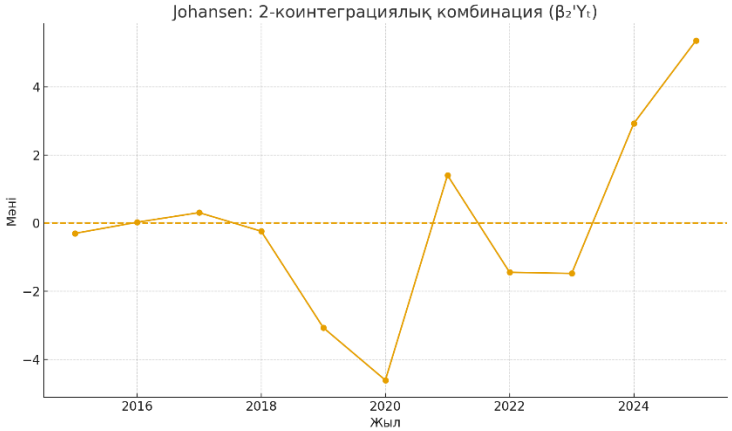
	Trace Statistic	5% Critical (Trace)	Max-Eig Statistic	5% Critical (Max-Eig)
r ≤ 0	327.0273	29.7961	310.8562	21.1314
r ≤ 1	16.1711	15.4943	12.8135	14.2639
r ≤ 2	3.3576	3.8415	3.3576	3.8415

Сурет 5 – Johensen тесті бойынша алынған коинтеграциялық деректер

Сурет 5-те Johansen коинтеграциялық тестінің Trace және Max-Eigenvalue статистикалары ұсынылған. Бұл Botnets, Viruses және Phishing қатарлары арасында кемінде бір коинтеграциялық вектор бар екенін білдіреді. Яғни, қатарлар жеке-жеке стационарлы болмаса да, олардың белгілі бір сызықтық комбинациясы стационарлы сипатқа ие.
Бұл нәтижелер аталған қауіп түрлерінің ұзақ мерзімді өзара тәуелділігін дәлелдейді.

Атап айтқанда, r ≤ 0 және r ≤ 1 гипотезалары үшін Trace статистикасы сәйкесінше 327,03 және 16,17 мәндерін берсе, олардың 5 пайыздық критикалық мәндері 29,79 және 15,49 деңгейінде. Сол сияқты, Max-Eigenvalue статистикасы бойынша да 310,86 және 12,81 мәндері есептеліп, алғашқы екі жағдайда критикалық мәндерден асып түскен. Бұл Johansen тестінің нөлдік гипотезасын теріске шығарады.

Сонымен қатар, аталған көрсеткіштер ұзақ мерзімді перспективада бірге өсіп, уақыт өте келе ортақ тепе-теңдік күйге ұмтылады. Мұндай байланыс олардың өзара тәуелділігін және киберқауіпсіздік экожүйесінде бірігіп әрекет ететінін білдіреді.



Сурет 6 – Johensen тесті бойынша алынған коинтеграциялық деректердің графигі

Сурет 6-да коинтеграциялық байланыстардың графикалық интерпретациясы берілген. Қатарлардың уақыт бойынша параллель қозғалысы олардың ұзақ мерзімді теңгерімді траекториясын көрсетеді. Графиктен кейбір кезеңдерде ауытқулар болғанымен, қатарлар уақыт өте ортақ динамикалық аймаққа қайта оралатыны байқалады. Бұл α параметрі арқылы сипатталатын тепе-теңдікке қайту механизмінің бар екенін білдіреді.

Киберқауіпсіздік тұрғысынан бұл ботнет, вирус және фишинг белсенділігінің бір экожүйелік модельге бағынатынын көрсетеді.

ADF тесті, Johansen коинтеграциясы және VAR моделі өзара логикалық байланыста қолданылады[9]. Алдымен ADF тесті арқылы әрбір қатардың стационарлығы тексеріледі. Егер қатарлар стационарлы емес болса, онда олардың айырмалары алынады немесе Johansen тесті арқылы ұзақ мерзімді байланыс бар-жоғы анықталады. Егер коинтеграция бар болса, онда VECM (Vector Error Correction Model) моделі қолданылады, ал егер коинтеграция анықталмаса, VAR моделі қолданылады. Осылайша, ADF тесті деректердің тұрақтылық деңгейін, Johansen тесті ұзақ мерзімді байланыстарды, ал VAR моделі қысқа мерзімді динамикалық әсерлерді бағалауға бағытталған[10].

Модельдің параметрлері statsmodels кітапханасының VAR.fit() процедурасы арқылы бағаланды. Нәтижесінде алынған коэффициенттер Botnets және Viruses қатарларының өздерінің өткен мәндеріне және бір-біріне тәуелділігінің жоғары екенін көрсетті. Phishing айнымалысы көбіне вирустардың динамикасына тәуелді, бұл екі көрсеткіш арасында байланыс бар екенін білдіреді.

VAR моделінің негізінде 2026–2028 жылдарға қысқа мерзімді болжам жасалды. Болжам айырма арқылы есептеліп, кейіннен бастапқы деңгейге жинақталды (cumulative sum).

```
=== 2026-2028 болжам (деңгейге жинақталған) ===
      Botnets  Viruses  Phishing
2026  40923.9  16028.7   -1324.3
2027  62133.1  25809.9    -739.4
2028  81744.7  13573.0   -3669.0
```

Сурет 7 – VAR моделі бойынша болжам

Сурет 8 – VAR болжамы: 2026-2028 жыл

Сурет 8-де 2026–2028 жылдарға арналған қысқа мерзімді болжам нақты интерпретацияланған. Ботнеттер мен вирустар бойынша өсу қарқыны сақталып, жүйенің тұрақсыздық деңгейінің жоғарылайтынын көрсетеді. Фишингтің динамикасы баяулау траекториясына өтеді, алайда коинтеграциялық байланыс салдарынан оның толық төмендеуі күтілмейді.

Киберқауіпсіздік саласында бұл әдістердің ғылыми маңызы үлкен. Олар статистикалық құрылымын, өзара тәуелділігін және эволюциялық даму үрдістерінің байланысын зерттеуге мүмкіндік береді. Нәтижесінде олардың ұзақ мерзімді және қысқа мерзімді әсерлерін бөлуге болады. Бұл нәтижелер кейінгі кезеңде киберқауіп деңгейін болжау және тәуекел индекстерін есептеу үшін қолданылады. Осылайша, ADF, Johansen

және VAR модельдері киберқауіпсіздік деректерін талдау мен болжаудың ғылыми және практикалық негізін құрайды.

Кесте 3 – Қазақстан, АҚШ, Сингапурдың салыстырмалы кестесі

Көрсеткіштер (Инцидент түрі)	Қазақстан (KZ-CERT, болжамды деректер)	АҚШ (FBI IC3 есебі)	Сингапур (CSA есебі)
Фишинг (Phishing)	1077 (өсу тенденциясы байқалады)	~298000 (доминантты киберқылмыс түрі)	4100 (52%-ға төмендеу тіркелген)
Ботнеттер	25628 (стационарлы, жоғары деңгей)	Нақты сан көрсетілмеген (инфрақұрылымдық шығындар басым)	70200 (тазарту шаралары нәтижесінде 14%-ға азайған)
Вирустар (Malware/Viruses)	27049 (тұрақты өсім)	Тікелей шағымдар аз, бірақ Ransomware (бопсалаушы вирустар) басым	Тұрақты деңгейде сақталған

Зерттеу барысында жүргізілген ADF тестінің нәтижесі бойынша Қазақстандағы ботнеттер саны стационарлы сипатқа ие. Бұл көрсеткіш Сингапурдың статистикасымен сәйкес келеді, онда да ботнеттер саны жоғары (70 200 инцидент). Қазақстанда ботнеттердің стационарлы болуы IoT құрылғылары мен желілік периметрді қорғауда жүйелі осалдықтардың бар екенін көрсетеді.

АҚШ статистикасында фишинг ең көп тіркелген киберқылмыс түрі (барлық шағымдардың ~34%). Сингапурда, керісінше, қауіпсіздік шараларының күшеюіне байланысты фишинг әрекеттерінің саны екі есеге жуық азайған. Ал Қазақстандағы VAR моделінің болжамы бойынша, фишинг көрсеткіші тұрақтылыққа ұмтылғанымен, вирустармен коинтеграциялық байланыста дамып келе жатқаны байқалады. Дамыған елдерде фишинг жасанды интеллектпен бірігіп үлкен қауіп төндіруде. Қазақстанда фишингтің вирустар динамикасына тәуелді болуы шабуылдардың көбінесе техникалық сипатта (мысалы, вирус тарату мақсатында) жүзеге асырылатынын дәлелдейді.

Қазақстандық деректерде вирустар категориясы бойынша тұрақты өсім тіркелді . Бұл АҚШ пен Сингапурдағы трендтерден өзгеше, себебі аталған елдерде классикалық вирустардан гөрі, мақсатты бопсалаушы бағдарламалар (Ransomware) үлкен қауіп әкелуде.

Қорытынды.

Зерттеу нәтижелері Қазақстан Республикасындағы киберқауіпсіздік жағдайының қазіргі деңгейін кешенді түрде бағалауға және оның даму үрдістерін анықтауға мүмкіндік берді.

Ұлттық KZ-CERT орталығының деректері негізінде жүргізілген эконометрикалық модельдеуді пайдаланып, (ADF, Johansen, VAR) Қазақстандағы киберқауіп көрсеткіштерінің уақыттық динамикасын сандық тұрғыда бағаладық. Нәтижелер бойынша ботнеттер мен DDoS шабуылдары стационарлы сипатта болып, олардың жиілігі салыстырмалы тұрақтылық көрсеткен, ал вирустар мен фишинг шабуылдарында тұрақты өсім байқалды. Johansen коинтеграциялық талдауы ботнеттер, вирустар және фишинг көрсеткіштері арасында ұзақ мерзімді тепе-теңдік байланыс бар екенін дәлелдеді, ал VAR моделі бұл көрсеткіштердің өзара әсер ету бағытын және ықтимал тәуелділіктерін, болжамын айқындады.

Дамыған елдерде (АҚШ, Сингапур) киберқылмыс көбінесе қаржылық алаяқтық пен күрделі әлеуметтік инженерияға негізделсе, Қазақстанда техникалық сипаттағы жаппай шабуылдар (ботнеттер, вирустар) басым. Алынған нәтижелер ұлттық киберқауіпсіздік

стратегиясын қайта қарастыру қажеттігін көрсетеді. Атап айтқанда, ботнеттер мен зиянды бағдарламалардың стационарлы және жоғары деңгейде сақталуы желілік периметрді қорғау жүйелерін, IoT құрылғыларының қауіпсіздігін және автоматтандырылған аномалия анықтау алгоритмдерін жетілдіруді талап етеді. Сонымен қатар, вирустар мен фишинг сияқты киберқауіптердің коинтеграциялық байланысы кешенді қарсы әрекет ету архитектурасын әзірлеудің маңыздылығын айқындайды.

Әдебиеттер тізімі

1. Raval, K. J., Jadav, N. K., Rathod, T., Tanwar, S., Vimal, V., & Yamsani, N. (2024). A survey on safeguarding critical infrastructures: Attacks, AI security, and future directions. International Journal of Critical Infrastructure Protection, 44, Article 100647. https://doi.org/10.1016/j.ijcip.2023.100647
2. Қазақстан Республикасының «Қазақстанның киберқалқаны» киберқауіпсіздік тұжырымдамасын бекіту туралы: Қазақстан Республикасы Үкіметінің 2017 жылғы 30 маусымдағы № 407 қаулысы [Электрондық ресурс] // ҚР НҚА ақпараттық-құқықтық жүйесі «Әділет». – URL: https://adilet.zan.kz/kaz/docs/P1700000407 (жүгіну күні: 19.12.2025).
3. KZ-CERT Ұлттық компьютерлік оқиғаларға әрекет ету қызметі. Ақпараттық қауіпсіздік инциденттерінің статистикасы [Электрондық ресурс]. – Астана: Мемлекеттік техникалық қызмет, 2025. – Кіру режимі: https://www.kz-cert.kz/ (жүгіну күні: 19.12.2025).
4. Federal Bureau of Investigation (FBI). Internet Crime Report 2023 [Электрондық ресурс] / Internet Crime Complaint Center (IC3). – Washington, D.C., 2024. – 35 б. – URL: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (жүгіну күні: 19.12.2025).
5. Cyber Security Agency of Singapore (CSA). Singapore Cyber Landscape 2023 [Электрондық ресурс]. – Singapore: CSA, 2024. – 48 б. – URL: https://www.csa.gov.sg/News-and-Events/Press-Releases/2024/singapore-cyber-landscape-2023 (accessed: 19.12.2025).
6. Ahmed, Y., Azad, M. A., & Asyhari, T. (2024). Rapid Forecasting of Cyber Events Using Machine Learning-Enabled Features. Information (Switzerland), 15(1), 36. https://doi.org/10.3390/info15010036
7. Landauer, M., Skopik, F., Stojanović, B., Flatscher, A., & Ullrich, T. (2025). A review of time-series analysis for cyber security analytics: From intrusion detection to attack prediction. International Journal of Information Security, 24*(3)*. https://doi.org/10.1007/s10207-024-00921-0
8. Seabold S. Statsmodels: Econometric and Statistical Modeling with Python / S. Seabold, J. Perktold // Proceedings of the 9th Python in Science Conference / ed. by S. van der Walt, J. Millman. – Austin, TX, 2010. – Б. 92-96.
9. Kaiser, F., Budig, T., Goebel, E., Fischer, T., Muff, J., Wiens, M., & Schultmann, F. (2021). Attack Forecast and Prediction (using Vector Autoregression). Proceedings of the 28th C&ESAR. CEUR Workshop Proceedings. https://doi.org/10.5445/IR/1000142504
10. Amoawah, N. M. (2025). Modeling the impact of data breaches on stock volatility using financial time series and event-based risk models. World Journal of Advanced Research and Reviews. https://doi.org/10.5281/zenodo.17322417

References

1. Raval, K. J., Jadav, N. K., Rathod, T., Tanwar, S., Vimal, V., & Yamsani, N. (2024). A survey on safeguarding critical infrastructures: Attacks, AI security, and future directions. International Journal of Critical Infrastructure Protection, 44, Article 100647. https://doi.org/10.1016/j.ijcip.2023.100647
2. On Approval of the Cybersecurity Concept “Cyber Shield of Kazakhstan”: Resolution of the Government of the Republic of Kazakhstan No. 407 dated June 30, 2017 [Electronic resource] // Information and Legal System of Regulatory Legal Acts of the Republic of Kazakhstan “Adilet”. – URL: https://adilet.zan.kz/kaz/docs/P1700000407 (accessed: 19.12.2025).

3. KZ-CERT National Computer Emergency Response Team. Information Security Incident Statistics [Electronic resource]. – Astana: State Technical Service, 2025. – Access mode: https://www.kz-cert.kz/ (accessed: 19.12.2025).

4. Federal Bureau of Investigation (FBI). Internet Crime Report 2023 [Electronic resource] / Internet Crime Complaint Center (IC3). – Washington, D.C., 2024. – 35 p. – URL: https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf (accessed: 19.12.2025).

5. Cyber Security Agency of Singapore (CSA). Singapore Cyber Landscape 2023 [Electronic resource]. – Singapore: CSA, 2024. – 48 p. – URL: https://www.csa.gov.sg/News-and-Events/Press-Releases/2024/singapore-cyber-landscape-2023 (accessed: 19.12.2025).

6. Ahmed, Y., Azad, M. A., & Asyhari, T. (2024). Rapid Forecasting of Cyber Events Using Machine Learning-Enabled Features. Information (Switzerland), 15(1), 36. https://doi.org/10.3390/info15010036

7. Landauer, M., Skopik, F., Stojanović, B., Flatscher, A., & Ullrich, T. (2025). A review of time-series analysis for cyber security analytics: From intrusion detection to attack prediction. International Journal of Information Security, *24*(1), Article 3. https://doi.org/10.1007/s10207-024-00921-0

8. Seabold, S. (2010). Statsmodels: Econometric and Statistical Modeling with Python / S. Seabold, J. Perktold // Proceedings of the 9th Python in Science Conference / ed. by S. van der Walt, J. Millman. – Austin, TX. – pp. 92–96.

9. Kaiser, F., Budig, T., Goebel, E., Fischer, T., Muff, J., Wiens, M., & Schultmann, F. (2021). Attack Forecast and Prediction (using Vector Autoregression). Proceedings of the 28th C&ESAR. CEUR Workshop Proceedings. https://doi.org/10.5445/IR/1000142504

10. Amoawah, N. M. (2025). Modeling the impact of data breaches on stock volatility using financial time series and event-based risk models. World Journal of Advanced Research and Reviews. https://doi.org/10.5281/zenodo.17322417

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ИНЦИДЕНТОВ КИБЕРБЕЗОПАСНОСТИ В РЕСПУБЛИКЕ КАЗАХСТАН

Аннотация. *В данной статье исследуется временная динамика кибер-инцидентов в Республике Казахстан и проводится сравнительный анализ с развитыми цифровыми государствами (США, Сингапур). Методологической основой исследования послужило использование эконометрических инструментов анализа временных рядов: расширенного теста Дики-Фуллера (ADF), теста коинтеграции Йохансена и модели векторной авторегрессии (VAR). Анализ данных KZ-CERT (2015–2025 гг.) показал, что распространенность ботнет-сетей стационарна и находится на стабильно высоком уровне. Также наблюдался рост вирусных и фишинговых атак. При сравнении с отчетами из США (FBI IC3) и Сингапура (CSA) было выявлено, что в Казахстане преобладают угрозы инфраструктурного и технического характера, в то время как в развитых странах высока доля социальной инженерии и целенаправленных атак. На основе расчетов, выполненных в языке программирования Python (pandas, statsmodels), был составлен краткосрочный прогноз на 2026–2028 годы и даны научно обоснованные рекомендации по совершенствованию национальной системы кибербезопасности.*

Ключевые слова: *кибербезопасность, математическое моделирование, модель VAR, тест ADF, ботнеты, фишинг, сравнительный анализ.*

MATHEMATICAL MODELING OF CYBERSECURITY INCIDENTS IN THE REPUBLIC OF KAZAKHSTAN

Abstract. *This article examines the temporal dynamics of cyber incidents in the Republic of Kazakhstan and provides a comparative analysis with developed digital states (the United States*

and Singapore). The study's methodological basis is the use of econometric tools for time series analysis: the augmented Dickey-Fuller (ADF) test, the Johansen cointegration test, and the vector autoregressive (VAR) model. An analysis of KZ-CERT data (2015–2025) revealed that the prevalence of botnet networks is stationary and remains at a consistently high level. An increase in virus and phishing attacks was also observed. A comparison with reports from the United States (FBI IC3) and Singapore (CSA) revealed that in Kazakhstan, threats of an infrastructural and technical nature predominate, while developed countries have a high share of social engineering and targeted attacks. Based on calculations performed in the Python programming language (pandas, statsmodels), a short-term forecast for 2026–2028 was compiled and scientifically based recommendations for improving the national cybersecurity system were provided.

Keywords: *cybersecurity, mathematical modeling, VAR model, ADF test, botnets, phishing, comparative analysis.*

Авторлар туралы мәлімет

Адилжанова Салтанат Альмуханбетовна	PhD (Ақпараттық қауіпсіздік жүйелері), доцент м.а., Ақпараттық технологиялар және жасанды интеллект факультеті, Киберқауіпсіздік және криптология кафедрасы, Алматы, Қазақстан, ORCID: https://orcid.org/0000-0003-1768-064X, e-mail: asaltanat81@gmail.com
Рахыш Айгерім Ерғализы	2-курс докторант, ақпараттық қауіпсіздік жүйелері мамандығы, Ақпараттық технологиялар және жасанды интеллект факультеті, киберқауіпсіздік және криптология кафедрасы, Алматы, Қазақстан, ORCID: https://orcid.org/0009-0005-0748-3724, e-mail: rakhysh_aigerim3@live.kaznu.kz

Сведение об авторах

Адилжанова Салтанат Альмуханбетовна	PhD (системы информационной безопасности), и.о. доцента, Факультет информационных технологий и искусственного интеллекта, Кафедра кибербезопасности и криптологии, Алматы, Казахстан ORCID: https://orcid.org/0000-0003-1768-064X, e-mail: asaltanat81@gmail.com
Рахыш Айгерім Ерғалиқызы	докторант 2-го года обучения, специализация: системы информационной безопасности, Факультет Информационных технологий и искусственного интеллекта, Кафедра кибербезопасности и криптологии, Алматы, Казахстан ORCID: https://orcid.org/0009-0005-0748-3724 e-mail: rakhysh_aigerim3@live.kaznu.kz

Information about the authors

Adilzhanova Saltanat Almukhanbetovna	PhD (Information Security Systems), Acting Associate Professor, Faculty of Information Technologies and Artificial Intelligence, Department of Cybersecurity and Cryptology, Almaty, Kazakhstan, ORCID: https://orcid.org/0000-0003-1768-064X, e-mail: asaltanat81@gmail.com
Rakhysh Aigerim Yergalikyzy	2nd year PhD student, majoring in information security systems, Faculty of Information Technologies and Artificial Intelligence, Department of Cybersecurity and Cryptology, Almaty, Kazakhstan, ORCID: https://orcid.org/0009-0005-0748-3724 e-mail: rakhysh_aigerim3@live.kaznu.kz