

ӘОЖ 621.39:004.05

DOI 10.52167/1609-1817-2025-138-3-344-354

К.К. Макулов¹, Л.М. Кыдыралина², А.К. Абуова², Н.К. Құрбаниязов⁴, М.А. Лахно⁵

¹Yessenov University, Ақтау, Қазақстан

²Shakarim University, Семей, Қазақстан

³International University of Transport and Humanities, Алматы, Қазақстан

⁴Farabi University, Алматы, Қазақстан

⁵National University of Bioresources and Environmental Management of Ukraine,
Киев, Украина

E-mail: lazat_75@mail.ru

ОҚУШЫЛАРДЫҢ ЦИФРЛЫҚ ІЗДЕРІН ТАЛДАУ НЕГІЗІНДЕ КИБЕРҚАУІПСІЗДІК ЖӘНЕ КИБЕРҚАУІПТІ МІНЕЗ-ҚҰЛЫҚ ҮЛГІЛЕРІН ЗЕРТТЕУ

Аңдатпа. Мақалада цифрлық іздерді секвенциалды талдау негізінде пайдаланушылардың киберқауіпсіздік мінез-құлқының максималды дәйекті үлгілерін(паттерн) алу әдісі университеттің кибернетикалық білім беру жүйесінің (УКББЖ) ақпараттық қауіпсіздігін (АҚ) қамтамасыз етуде бірқатар артықшылықтарға ие екендігі көрсетілген. Атап айтқанда, цифрлық іздің дәйекті талдау негізінде пайдаланушылардың киберқауіпсіздік тәртібінің максималды ретті үлгілерін алу әдісіне сүйене отырып, УКББЖ-да пайдаланушылардың аномальды мінез-құлқын анықтауға болады. Бұл жалпы УКББЖ-ның ақпараттық қауіпсіздігіне және оның жеке құрамдас бөліктеріне, мысалы, оқу пәндері мен студенттердің цифрлық егіздері (ЦЕ) үшін ықтимал қауіптерді көрсетуі мүмкін. Цифрлық іздің дәйекті талдауы жүйеге Ақпараттық қауіпсіздікке жаңа немесе бұрын белгісіз қауіптерді анықтауға мүмкіндік беретіні анықталды, өйткені УКББЖ және оның қауіпсіздік контурлары оқу пәндерінің цифрлық егіздерімен өзара әрекеттесу кезінде пайдаланушылардың мінез-құлқы үлгілеріндегі өзгерістерге тез бейімделе алады. Пайдаланушылардың киберқауіпті мінез-құлқының дәйекті үлгілерін (паттерндерін) зерделеу арқылы жүйені пайдаланудың типтік сценарийлерін анықтауға болатыны көрсетілген, бұл пайдаланушының қалыпты әрекетін қалыпсыздан анықтауға көмектеседі.

Түйінді сөздер: ақпараттық қауіпсіздік, кибернетикалық білім беру жүйесі, цифрлық іздер, цифрлық егіздер, мінез-құлқы үлгілері.

Кіріспе.

Өткен ғасырдың соңы мен жаңа 21 ғасырдың басы оқу үдерістерін цифрландыруға байланысты білім беру саласына жаңа инновациялық тәсілдер әкелді. Бүгінгі таңда білім беру саласына [1] байланысты жаңа ақпараттық технологиялар (АТ): жасанды интеллект (ЖИ) және машиналық оқыту белсенді дамып келеді; толықтырылған шындық (AR) және виртуалды шындық (VR); блокчейн технологиялары; Интернет заттары технологиясы (IoT); бұлтты технологиялар; гибридтік оқыту және онлайн білім беру; бейімделген білім беру платформалары; академиялық пәндер мен студенттердің цифрлық егіздері; Үлкен деректердің аналитикасы және т.б. Бұл технологиялар мен IT трендтері қазірдің өзінде көптеген университеттерде енгізілуде және білім беру саласында белсенді дамып келеді, бұл оқытуды қолжетімді, жекелендірілген және тиімді етеді.

Атап айтқанда, университеттердің оқу үдерісіне оқу пәндері мен студенттердің цифрлық егіздерін (ЦЕ) енгізудің бірегейлігі мен жаңашылдығы дербестендірілген және бейімделген білім беру тәжірибесін құруда жатыр. Мысалы, [2] ойынша, білім беруде цифрлық оқытуды пайдалану тұжырымдамасы: оқытуды жекелендіруге; оқу пәндерін нақты студенттер тобының немесе жеке қажеттіліктеріне және ерекшеліктеріне бейімдеу; оқу процестерін оңтайландыру; студенттер арасында да, мұғалімдер мен студенттер арасында да өзара әрекеттестік деңгейін арттыру; деректерді қорғаудың жоғары деңгейін қамтамасыз ету және т.б.

"Оқу пәнінің цифрлық егізі" және "студенттің цифрлық егізі" ұғымдарының қалай ерекшеленетінін, сондай-ақ бұл екі ұғым университеттердің кибернетикалық білім беру жүйелерінде (УКББЖ) цифрлық егізді қорғауды қамтамасыз етумен байланысты мәселені шешу контекстінде қалай өзара байланысты екенін қарастырайық.

[3] сәйкес, академиялық пәннің цифрлық егізі – оқу пәні мазмұнының виртуалды моделі, оқу материалын, оның ішінде оқу бағдарламаларын, оқыту мен тестілеуге арналған материалдарды электронды түрде көрсету үшін пайдалануға болады. Бұл тиімді оқыту үшін ұйымдастырылған және құрылымдалған курстың немесе пәннің цифрлық түрі. Студенттің цифрлық егізі, керісінше, оқушының виртуалды бейнесі немесе профилі болып табылады, ол олардың оқу процесі, өнімділігі, оқу қалауы, оқу стилі және т.б. туралы деректерді қамтуы мүмкін. Бұл профиль оқуды жекелендіру, курстарды бейімдеу және студенттің білім беру тәжірибесін жақсарту үшін пайдаланылады.

Бұл екі тұжырымдаманың арасындағы байланыс академиялық пәннің сандық егіздерінің студенттің цифрлық егіздерінің пайда болуына әсер етеді. Оқу пәнінің цифрлық егіздерінде берілген ақпарат студенттің қажеттіліктеріне, білім деңгейіне және қалауына негізделген жекелендірілген оқу тәжірибесін құру үшін пайдаланылады. Бұл сандық профильге негізделген әрбір жеке студент үшін материалдарды, оқыту әдістерін, бағаларды және т.б. бейімдеуді қамтуы мүмкін.

Бұл цифрлық егіздерді қорғау маңызды, себебі оларда студенттің оқу процесі мен білім беру материалдары туралы сезімтал, кейде құпия мәліметтер бар. Мұндай деректердің бұзылуы әртүрлі құпиялылық қауіптеріне, соның ішінде алаяқтық немесе студенттер мен оқытушылардың жеке ақпаратына рұқсатсыз қол жеткізу мүмкіндігіне әкелуі мүмкін.

Жұмыстың бірінші бөлімінде көрсетілгендей, математикалық қорғау әдістерінің аспектісінде цифрлық егіздер, деректерді қауіпсіз беру мен сақтауды қамтамасыз ету үшін криптографиялық хаттамаларды, ауытқуларды анықтау үшін машиналық оқыту алгоритмдерін және студенттер мен оқу пәндерінің цифрлық егіздеріне бағытталған кибершабуылдардан қорғауды, цифрлық іздерді талдау әдістерін және т. б. пайдалануға болады.

Жұмыста шешілген сыйлықтар контекстінде, Оқу пәнінің цифрлық егіздері, студенттің цифрлық егіздері және цифрлық іздерді талдауарасындағы байланыс цифрлық іздерді талдауды студенттің, оқу пәнінің және/немесе бүкіл оқу орнының дәлірек және толық цифрлық егізін жасау үшін пайдалануға болады (соңғы тапсырма өте көп ресурстарды қажет етеді және қымбат).

Жұмыстың бірінші бөлімінде жоғарыда көрсетілгендей, оқушының цифрлық егіздігі сандық іздерді талдау арқылы дәлірек болуы мүмкін, оның ішінде оның оқу жүйесіндегі белсенділігі, тапсырмаларға жауаптары, әртүрлі оқу материалдарына жұмсалған уақыты және т.б. Сол сияқты, курстың цифрлық егізін студенттердің цифрлық іздерін талдау арқылы жақсартуға болады, курстар мен материалдарды олардың қажеттіліктері мен оқу стиліне сәйкес келтіруге мүмкіндік береді.

Цифрлық іздерді талдау, мысалы, университеттерде оқу процесін жақсартуға ғана емес, кибернетикалық білім беру жүйелеріндегі цифрлық егіздердің қауіпсіздік деңгейін арттыруға мүмкіндік береді. [4, 5] сәйкес, сандық іздерді талдау әдістері мен құралдары арқылы УКББЖсандық егіздердің қауіпсіздік дәрежесін арттыруға көмектеседі:

Аномалияны анықтау. Сандық іздер талдауы ықтимал қауіпсіздік қауіптерін көрсететін пайдаланушы немесе жүйе әрекетіндегі ауытқуларды анықтай алады. Бұл сандық егіздерге рұқсатсыз кіруді болдырмауға және ықтимал шабуылдарға тез жауап беруге көмектеседі.

Қорғаныс жүйелерін күшейту. Сандық іздерді талдау деректерін пайдалана отырып, УКББЖ-нің ақпараттық қауіпсіздік мамандары оны қорғау әдістерін жақсартып алады. Мысалы, қауіпсіздік шараларын күшейтетін студенттер мен оқу пәндерінің цифрлық егіздеріне күдікті әрекеттерді немесе шабуылдарды анықтайтын Машиналық оқыту алгоритмдерін жасауға болады.

УКББЖ-дегі ақпараттық қауіпсіздік оқиғаларының алдын алу. Сандық іздерді талдау ықтимал қауіпсіздік оқиғаларын болжауға көмектеседі, бұл УКББЖ-нің ақпараттық қауіпсіздік жүйесіне деректердің бұзылуын болдырмау немесе студенттерге де, оқу пәндеріне де, жалпы УКББЖ-ге де сандық егіздерге рұқсатсыз қол жеткізу үшін алдын ала шаралар қабылдауға мүмкіндік береді.

Ақпараттық қауіпсіздікті бұзбай жекелендіруді жақсарту. Цифрлық іздерді талдау арқылы студенттерге олардың оқу қажеттіліктері мен қалауларын ескере отырып, ақпараттық қауіпсіздіктің жоғары деңгейін және олардың цифрлық егіздерін қорғауды қамтамасыз ете отырып, жекелендірілген білім беру тәжірибесін жасауға болады.

Білім беру пәндерінің цифрлық егіздерін және студенттердің цифрлық егіздерін қорғау мәселелері және цифрлық іздерді талдау тапсырмалары студенттердің мінез-құлық үлгілерін зерттеу қажеттілігімен байланысты екенін ескеру қажет. Осылайша, оқушылардың сандық іздері мен олардың мінез-құлық заңдылықтарын талдау білім беру жүйесіндегі оқушы әрекетінің типтік сипаттамалары мен әдеттегі заңдылықтарын анықтауға ғана емес, сонымен бірге қалыптан тыс мінез-құлық үлгілерін егжей-тегжейлі талдауға мүмкіндік береді. Бұл аномальды мінез-құлық сандық егіздердің қауіпсіздігіне әлеуетті қауіп төндіретінін көрсетуі мүмкін. Мысалы, егер студенттің есептік жазбасы кенеттен әдеттен тыс әрекет үлгілерін көрсете бастаса, бұл рұқсатсыз кіру әрекетін көрсетуі мүмкін.

Жоғарыда айтылғандардың бәрі біздің осы бағыттағы зерттеулерге деген қызығушылығымызды тудырды.

Зерттеудің мақсаты. Студенттер оқу пәндерінің цифрлық егіздерімен өзара әрекеттесу кезінде ақпараттық қауіпсіздікті жақсарту үшін цифрлық іздерді дәйекті талдау негізінде пайдаланушылардың киберқауіпсіздік әрекетінің максималды дәйекті үлгілерін алу әдісін қолдану мүмкіндіктерін талдау.

Материалдар мен тәсілдер.

Пайдаланушылардың мінез-құлық үлгілерін оның ақпараттық қауіпсіздігі (АҚ) контекстінде сипаттауға байланысты математикалық есептеулерді ұсынбас бұрын, төменде қолданылатын терминологияға қысқаша тоқталайық.

Пайдаланушының мінез-құлық үлгілері УКББЖ-мен әрекеттесу кезінде пайдаланушылар көрсететін әрекеттердің типтік үлгілері немесе сипаттамалары деп есептейміз. Ақпараттық қауіпсіздік және/немесе кибернетикалық қауіпсіздік (КҚ) контекстінде үлгіні талдау маңызды болуы мүмкін. Кейбір типтік үлгілер 1-кестеде көрсетілген.

1 кесте - УКББЖ қауіпсіздігіне әсер етуі мүмкін әдеттегі пайдаланушы мінез-құлқының мысалдары

№	Үлгінің шартты атауы	Сипаттама
1	Қол жеткізу жиілігі және әдеттегі белсенділік аралықтары	Пайдаланушылар әдетте УКББЖ-ге кірудің белгілі бір уақыт шеңберіне ие. Кіру жиілігінің қалыптан тыс өзгеруі УКББЖ-дағы шоттардың бұзылуын көрсетуі мүмкін.
2	Әдеттегі сұраныстар мен операциялары	УКББЖ-де пайдаланушылардың әдеттегі сұраныстарын зерттеу аномальды немесе күдікті әрекеттерді анықтауға ықпал етеді. Мысалы, УКББЖ есептік жазбасының параметрлерін алдын-ала рұқсатсыз өзгерту әрекеттері есептік жазбаның бұзылуын көрсетуі мүмкін.
3	Орналасқан жері және құрылғылары	Пайдаланушылар әдетте қай жерден және қандай құрылғылардан УКББЖ-ге кіретінін талдау ауытқуларды анықтауға көмектеседі. Мысалы, УКББЖ-ге ерекше географиялық орындардан немесе типтік емес құрылғыдан кіру.
4	Пайдаланушының қауіпсіздік оқиғаларына реакциясы	УКББЖ пайдаланушылары парольді өзгерту, екі факторлы аутентификация және т.б. туралы сұрауларға қалай жауап береді. Ақпараттық қауіпсіздік шаралары олардың қауіпсіздік туралы хабардарлығын және/немесе қауіптердің болуын көрсетуі мүмкін.
	Т.б	

Содан кейін, пайдаланушы УКББЖ-бен әрекеттескенде Ақпараттық қауіпсіздік оқиғасы осы жүйедегі Ақпараттық қауіпсіздікке әсер етуі мүмкін кез келген оқиға немесе әрекет болып табылады. Ақпараттық қауіпсіздік оқиғалары атрибуттардың бос емес бірегей жиынтықтарымен сипатталады. Мұндай атрибуттарға, мысалы, 1-кестеге сәйкес мыналарды жатқызуға болады: пайдаланушы, құрылғы, уақыт, оқиға түрі. Оқиға түріне байланысты қосымша (арнайы атрибуттар) сияқты. Біз барлық тіркелген оқиғалардың жиынтығын E арқылы белгілейміз, яғни: $E = \{e_1, \dots, e_n\}$, мұндағы $\{e_i\}, i = \overline{1, n}$ – УКББЖ-дағы ақпараттық қауіпсіздіктің жекелеген оқиғалары; n – E қуаты.

Moodle (оқыуды басқару жүйесі (LMS)) сияқты УКББЖ-дегі пайдаланушы сеансы пайдаланушы УКББЖ-мен өзара әрекеттесетін уақыт кезеңін білдіреді. Сеанс пайдаланушы УКББЖ жүйесіне кірген кезде басталады (яғни, аутентификация) және пайдаланушы жүйеден шыққанда немесе пайдаланушының белгілі бір уақыт әрекетсіздігіне байланысты сеансты автоматты түрде аяқтағанда аяқталады. Ақпараттық қауіпсіздік (және/немесе кибернетикалық қауіпсіздік) тұрғысынан сеанс өте маңызды, өйткені белсенді сеанс кезінде құпия деректерге қол жеткізу, ақпаратты беру, операцияларды орындау және т.б. қоса алғанда, әртүрлі әрекеттер жүзеге асырылуы мүмкін.

Біз S арқылы барлық тіркелген сессиялардың жиынтығын белгілейміз, яғни $S = \{s_1, \dots, s_m\}$, мұндағы $\{s_i\}, i = \overline{1, m}$ – УКББЖ-дағы жекелеген сессиялар; m – S қуаты.

Сондай-ақ, сессияны E элементтерін қайталаусыз орналастыру ретінде сипаттауға болады: $s_i = \langle e_{i1}, \dots, e_{ij} \rangle$, мұндағы $\{e_{ij}\}, i = \overline{1, m}, j = \overline{1, h_i}$ – бір i -сессиясы аясындағы ақпараттық қауіпсіздіктің жеке оқиғасы; $h_i - s_i$ орналастыру қуаты.

Көп E УКББЖ-де пайдаланушы белсенділігі негізінде алынған сеанстардың барлық жинақтарын біріктіру нәтижесінде құрылады. Содан кейін Ақпараттық қауіпсіздік оқиғасы орын алса, ол кем дегенде бір сессияға жатады: $\forall e \in E, \exists s \in S, e \in s$.

E Элементтерді қайталаусыз орналастыру үшін олардың жіктелуі қажет екенін ескеріңіз. УКББЖ-дегі Ақпараттық қауіпсіздік және/немесе кибернетикалық қауіпсіздік класстарын УКББЖ-де ақпараттың тұтастығын, құпиялылығын және қолжетімділігін қамтамасыз ету үшін қолданылатын қорғау және қауіпсіздік шараларының деңгейлерін анықтайды. Содан кейін Ақпараттық қауіпсіздік оқиғаларының классын ақпараттың ерікті жиынтығы ретінде түсіндіруге болады Белгілі бір қасиеттерге немесе сипаттамаларға ие болатын УКББЖ қауіпсіздік оқиғаларының ерікті жиынтығы ретінде түсіндіруге болады. $C_E = \{c_1, \dots, c_l\}, \{c_i\}$ – УКББЖ-ға тән АҚ оқиғаларының барлық белгілі бір кластарының жиынтығы болсын. Мұнда $i = \overline{1, l}$ – АҚ тәуелсіз классы; $l - C_E$ қуаты. Мысалы, УКББЖ -дағы АҚ (КҚ) класстарына мыналарға байланысты класстар жатады: аутентификация және қол жеткізуді басқару; деректерді шифрлау және қорғау; осалдықтарды басқару және шабуылдардан қорғау; ақпараттық қауіпсіздіктің аудиті мен мониторингі және т.б.

Содан кейін ақ (R) үлгісі C_E элементтерін қайталанулармен орналастыру болады: $r_i = \langle c_{i1}, \dots, c_{ij} \rangle, \{c_{ij}\}, i = \overline{1, q}, j = \overline{1, w_i}, c_{ij} \in C_E$ – ақпараттық қауіпсіздіктің i -ші үлгісі үшін жеке ақпараттық қауіпсіздік оқиғасы; $q - R$ қуаты; $w_i - r_i$ мощность размещения.

Немесе басқаша айтқанда w_i - УКББЖ АҚ үлгісіндегі оқиғалар жиынтығы. Біз пайдаланушылардың мінез-құлық үлгілері цифрлік іздерді талдауға негізделуі мүмкін деп санаймыз, яғни. пайдаланушылардың УКББЖ-мен өзара әрекеттесуі туралы түсінік алуға мүмкіндік беретін талдау. УКББЖ ақпараттық қауіпсіздіктің әрбір оқиғасын белгілердің бос емес жиынтығы ретінде сипаттауға болады (мысалы, УКББЖ жүйесіне кірудің сәтсіз әрекеттері; әдеттен тыс тіркелгі әрекеті; аномальды трафик; УКББЖ қызметтерінің немесе қолданбаларының істен шығуы және т.б.). Сәйкесінше, мұндай бос емес жиын немесе ақпараттық қауіпсіздік оқиғасының атрибуттарының жиынтығы E жиын объектісіне тән болады. Біз E - дегі барлық нысандар мен S - дегі белгілер әр түрлі деп санаймыз.

УКББЖ АҚ оқиғаларының атрибуттарының жиындары жүйенің контекстіне және ерекшеліктеріне байланысты өзгеруі мүмкін екенін ескеріңіз, дегенмен, УКББЖ -да жазылған АҚ оқиғаларының көпшілігіне тән бірнеше жалпы атрибуттар бар: уақыт белгілері (Қай уақытта және күні АҚ оқиғасы орын алды); оқиға көзі (пайдаланушы, қолданба, құрылғы және т.б.); оқиға түрі (мысалы, кіру әрекеті, параметрлерді өзгерту және т.б.); маңыздылық деңгейі; оқиға нәтижесі; қосымша атрибуттар. Бұл атрибуттардың көпшілігі УКББЖ пайдаланушылардың цифрлық іздерін талдау негізінде белгіленуі мүмкін.

Ақпараттық қауіпсіздікте дәйекті талдау қауіпсіздікті басқару жүйесінде болып жатқан оқиғалар тізбегіндегі заңдылықтар мен шаблондарды (үлгілерді) анықтауға бағытталған. УКББЖ-да ақпараттық қауіпсіздік оқиғаларының реттілігінде үлгілерді іздеу әдісі УКББЖ пайдаланушысының бұрынғы әрекеттері негізінде ықтимал кейінгі ықтимал ақпараттық қауіпсіздік оқиғаларын талдау және болжау үшін пайдаланылуы

мүмкін. Яғни, УКББЖ-дағы пайдаланушы әрекетінің киберқауіпсіз (немесе қауіпті) үлгілерімен байланысты нақты цифрлық іздер талданады. Әдістің негізгі мәні келесідей:

1-кезең. Мәліметтерді алу. Біріншіден, ақпараттық қауіпсіздік оқиғалары туралы, оның ішінде цифрлық іздер негізінде деректерді жинау қажет. Бұл деректерге аудит журналдары, жүйе журналдары, қатынас деректері және басқа ақпараттық ресурстар кіруі мүмкін.

2-кезең. Тізбек түрінде бейнелеу. Ақпараттық қауіпсіздік оқиғасының деректері реттіліктерге түрлендіріледі (мысалы, ассоциация ережелері түрінде), мұнда әрбір ақпараттық қауіпсіздік оқиғасы пайдаланушы мінез-құлық үлгілерінің реттілігінің элементі ретінде ұсынылады. Мысалы, кіру әрекеттері талданса, пайдаланушының әрбір кіру әрекеті реттілікте бөлек элемент болады.

3-кезең. Үлгілер мен заңдылықтарды шығару. Әрі қарай, УКББЖ пайдаланушылардың киберқауіпсіздік (киберқауіпті) мінез-құлқының жиі кездесетін үлгілерін, оқиғалар тізбегін немесе олардың комбинацияларын анықтау үшін реттілік талдау әдістері қолданылады. Мұны әр түрлі алгоритмдер, мысалы, реттілікпен өндіру немесе жиі қосалқы іздеу алгоритмдері арқылы жасауға болады.

4-кезең. Үлгіні құру және УКББЖ-ге пайдаланушы әрекетінің үлгілерін болжау. Анықталған үлгілердің негізінде болашақ оқиғаларды болжау үшін немесе УКББЖ пайдаланушыларының киберқауіпсіздік (киберқауіпті) мінез-құлқының аномальды үлгілерін анықтау үшін пайдалануға болатын модельдер құрастырылған.

5-кезең. Бағалау және оңтайландыру. Ақпараттық қауіпсіздік оқиғаларының тізбегіндегі үлгілерді іздеу әдісі модельдерді тұрақты бағалауды және оңтайландыруды талап етеді, өйткені пайдаланушылар мен УКББЖ әрекеті уақыт өте келе өзгеруі мүмкін.

Нәтижелер.

Осы жұмыстың аясында біз УКББЖ-дағы пайдаланушылардың цифрлық іздерін дәйекті талдаудың мақсаты берілген пайдаланушы сессиясында ақпараттық қауіпсіздік оқиғаларының сыныптарының жиі кездесетін ішкі тізбектерін алу екенін атап өтеміз. Сондықтан [6-10] жұмыстарға сүйене отырып, біз сеанс кезінде УКББЖ-да қолданушылардың киберқауіпсіз (киберқауіпті) мінез-құлық үлгілерін іздеудің кеңейтілген моделін ұсынамыз. $\chi_p^{s'}$ үлгісінің i -ші ассоциативті белгісінің мүшелік функциясының мәні (R) деп алайық. Бұл мәнді s' бөлек сеанстағы P қайталанбайтын реттелген оқиғалардың саны ретінде есептеуге болады. Яғни, S' – УКББЖ-дағы барлық сақталған пайдаланушы сеанстарының жиынтығы (киберқауіпсіз (киберқауіпті) мінез-құлық критерийлері бойынша сүзгілеуден және жіктеуден кейін). Онда $S' = \{s'_1, \dots, s'_m\}$ яғни $\{s'_i\}$, $i = \overline{1, m}$ – жеке сессия; m – S' қуаты.

[6, 7] сәйкес деректерді талдаудағы ассоциация ережелері деректер жиынының әртүрлі элементтері арасындағы ассоциациялар туралы жалпылама мәлімдемелер болып табылады. Сонда АҚ УКББЖ сипаттамаларының жиыны бойынша $A = (X, Y)$ ассоциативті ережесі бойынша функцияларды сипаттайтын тәуелділіктерді қабылдаймыз: $\sup(X \Rightarrow Y)$ – қолдау, $\text{conf}(X \Rightarrow Y)$ – сенімділік. УКББЖ жүйесінде пайдаланушылардың цифрлық іздерін талдау кезінде ақпараттық қауіпсіздік талдаушылары әртүрлі ақпараттық қауіпсіздік әрекеттері немесе оқиғалары арасындағы үлгілер мен қатынастарды анықтау үшін байланыстыру ережелерін қолдана алады. Қауымдастық ережелеріндегі қолдау ($\text{Support} - \sup(X \Rightarrow Y)$) белгілі бір элементтер жиынының (немесе ақпараттық қауіпсіздік оқиғаларының) жалпы деректер

жинағында бірге пайда болу жиілігін анықтайды. Ол жалпы деректерде осы жиынның пайда болу жиілігі ретінде өлшенеді. Қолдау неғұрлым көп болса, бұл жиынтық бірлестік ережелерін қалыптастыру үшін соғұрлым маңызды болады. Сәйкесінше, сенімділік ($Confidence - conf(X \Rightarrow Y)$) элементтердің бірінші жинағы кездескен кезде ереженің қаншалықты жиі ақиқат болатынын көрсетеді, яғни. сенімділік бірінші жиынның кездескенін ескере отырып, екінші жиынның пайда болу ықтималдығы ретінде анықталады. 2-кестеде біз УКББЖ пайдаланушыларының киберқауіпті және киберқауіпсіз мінез-құлқын сипаттайтын осындай ассоциация ережелерінің бірнеше мысалдарын келтіреміз. Бұл ұғымдарды ақпараттық қауіпсіздік (КҚ) УКББЖ үлгілеріне қолдану пайдаланушы әрекеттерінің реттілігін талдауды қамтиды.

2 кесте – УКББЖ-дағы пайдаланушылардың киберқауіпті және киберқауіпсіз мінез-құлқын сипаттайтын ассоциация ережелерінің мысалдары

Киберқауіпті мінез-құлықтың ассоциативті ережелерінің мысалы:	Киберқауіпсіз мінез-құлықтың ассоциативті ережелерінің мысалы:
<p>Паттерн: Пайдаланушы УКББЖ-да белгісіз көздерден келген хаттардағы тіркемелерді жиі ашады. Бірлесу ережесі: Егер пайдаланушы УКББЖ ішінде белгісіз жіберушілерден тіркемелерді ашса, олар жүйеге қауіп төндіруі мүмкін. Қолдау (sup): 70% Сенімділік ($conf$): 80%</p>	<p>Паттерн: Пайдаланушы әрқашан сеансты аяқтайды және жұмысты аяқтағаннан кейін УКББЖ-дан шығады. Бірлесу ережесі: Пайдаланушы жұмысын аяқтаған болса, ол сеансты аяқтап, жүйеден шығады. Қолдау (sup): 80% Сенімділік ($conf$): 90%</p>
<p>Паттерн: Пайдаланушы УКББЖ-дағы қауіпті әрекеттер туралы ескертулерді елемейді. Қауымдастық ережесі: Пайдаланушы ескертулерді елемейтін болса, қауіпті әрекет қауіп артады. Қолдау (sup): 65% Сенімділік ($conf$): 75%</p>	<p>Паттерн: Пайдаланушы құпия деректерге қол жеткізбес бұрын әрқашан УКББЖ көмегімен аутентификацияланады. Қауымдастық ережесі: Егер пайдаланушы құпия деректерге қол жеткізсе, онда ол аутентификацияланады. Қолдау (sup): 75% Сенімділік ($conf$): 85%</p>

Мысалы, УКББЖ жүйесіне әдеттегі қауіпсіз кіру үлгілерін немесе аномальды пайдаланушы әрекетін көрсететін әрекеттер тізбегін анықтау $sup(X \Rightarrow Y)$ және $conf(X \Rightarrow Y)$ көмегімен сіз ең маңызды ақпараттық қауіпсіздік үлгілерін таңдай аласыз және УКББЖ-дағы ықтимал қауіптерді анықтай аласыз. $A = (X, Y)$ қолдауы мен сенімділігі жоғарыда талқыланған көптеген U мүмкіндіктерін қолдауға негізделген. УКББЖ-да киберқауіпсіз (киберқауіпті) пайдаланушы әрекетінің дәйекті үлгілерін табумен байланысты тапсырма sup және $conf$ үшін берілген шекті мәннен жоғары қолдауы бар максималды тізбектерді анықтау болып табылады. Ақпараттық қауіпсіздік оқиғаларын жіктеу үшін ереженің сенімділігін есептеу қажет, яғни $conf(X \Rightarrow Y) = \max f(E \rightarrow C_E)$.

УКББЖАҚ контекстінде АҚ оқиға үлгісінің ұзақтығы мен сессияның ұзақтығы біз үшін маңызды. Бұл параметрлер қол жеткізуді басқару, аутентификация және УКББЖқауіпсіздігі үшін маңызды болуы мүмкін. Қысқа сеанстар қауіпсіздікті жақсартады, себебі олар шабуылдаушы тіркелгі деректерін басып алу немесе жүйеге қол жеткізу уақытын қысқартады, ал ұзақ сеанстар пайдаланушылар үшін ыңғайлы, бірақ осалдықтарды тудыруы мүмкін. Ақпараттық қауіпсіздік оқиғаларының үлгісінің

ұзақтығын анықтау ақпараттық қауіпсіздік жүйелерін тиімді бақылау үшін де маңызды. Бұл параметр ақпараттық қауіпсіздік инциденттерін анықтау және шабуылдың алдын алу жүйесіне (IDS/IPS) белгілі мінез-құлық үлгілеріне немесе белгілі оқиғалардың сипаттамаларына негізделген УКББЖ-тегі белгілі сценарийлерді немесе ауытқуларды тануға және оларға жауап беруге көмектесе алады..

$\sup(X \Rightarrow Y) s' - \gamma_p^{s'}$ бөлек сессияда үлгілердің (r) пайда болу саны бойынша көрсетейік, яғни.:

$$\gamma_p^{s'} = \frac{(\chi_p^{s'} \cdot z)}{d}, 0 \leq \gamma_p^{s'} \in \mathbb{R} \leq 1, \quad (1)$$

мұндағы z – УКББЖ-дағы ақпараттық қауіпсіздік оқиғасының үлгісінің ұзақтығы;
 d – УКББЖ-дағы пайдаланушы сеансының ұзақтығы.

KOSU-дағы ақпараттық қауіпсіздік оқиғасының үлгісінің ұзақтығы әдетте оқиғаның өзін немесе УКББЖ-дағы қауіпсіздікке қатысты ақпарат бөлігін көрсететін таңбалардың, байттардың немесе биттердің санымен анықталатынын ескеріңіз. Бұл нақты параметрлердің жиынтығы, оқиғалар тізбегі немесе қауіпсіздікті бақылау жүйесінде бақыланатын немесе жазылған нақты деректер болуы мүмкін, мысалы, IDS/IPS - Splunk, Suricata және т.б. арқылы). Тиісінше, УКББЖ-дағы пайдаланушы сеансының ұзақтығы (УКББЖ-дағы сеанс ұзақтығы әдетте пайдаланушы УКББЖ-да қосылып немесе белсенді болып қалатын және, мысалы, минуттармен немесе сағаттармен өлшенетін уақыт кезеңі ретінде анықталады, немесе әрекеттерде, мысалы, УКББЖ-ға сұраулар саны немесе пайдаланушы әрекеті).

Белгілі бір УКББЖ пайдаланушысы үшін, мысалы, күнтізбелік жыл немесе бөлек семестрдегі сеанстардың саны әртүрлі болуы мүмкін. Осыған сәйкес қолдау мәнін жинақтау қажеттілігі туындайды [7]. УКББЖ-да пайдаланушының киберқауіпті әрекетінің үлгісіне жалпы қолдауды сипаттайтын мәнді келесідей есептеуге болады:

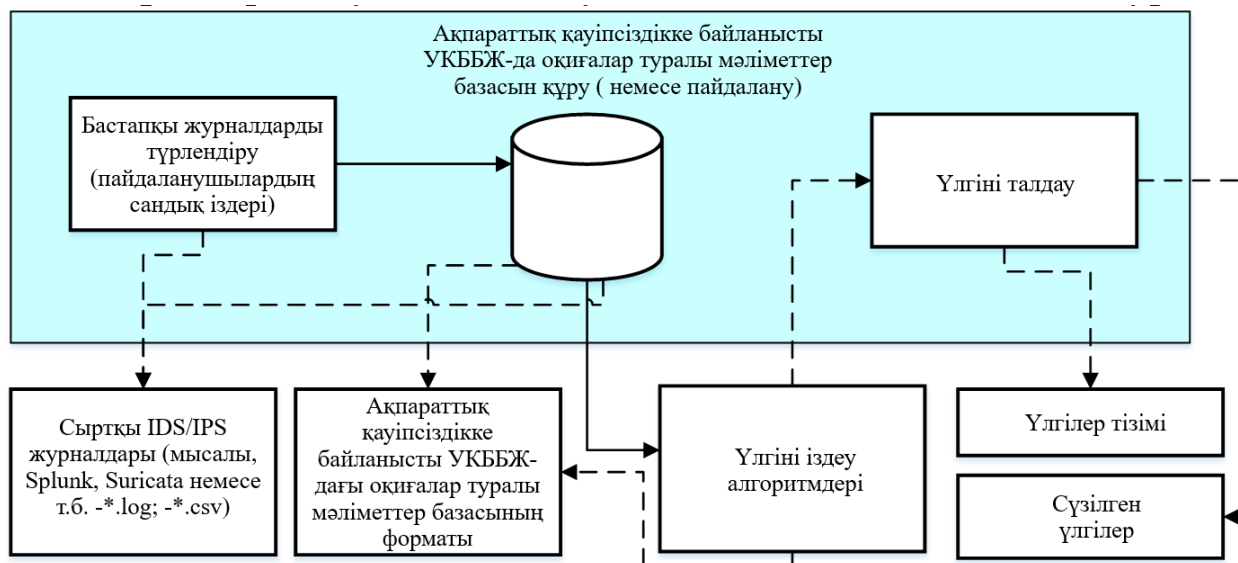
$$\gamma_p^{s'} = \sum_{i=1}^m \left(\left(\frac{\chi_p^{s'} \cdot z}{d_i} \right) \cdot \left(\frac{d_i}{n'} \right) \right) \leq \gamma_p^{s'} \in \mathbb{R} \leq 1, \quad (2)$$

мұндағы n' – мысалы, семестр немесе оқу жылы (жіктеу және сүзгілеуден кейін) ішінде УКББЖ-дағы пайдаланушы сессияларының жалпы саны.

Талқылау.

Тәуелділіктер (1) және (2) УКББЖ-дағы киберқауіпті (киберқауіпсіз) пайдаланушы әрекетінің әртүрлі дәйекті үлгілерін қолдау мәнін анықтауға мүмкіндік береді. Бұл қолдаудың мәнін сеанс кезінде УКББЖ-дағы пайдаланушының киберқауіпсіз (киберқауіпті) мінез-құлық үлгісінің мазмұнының үлесі ретінде сипаттауға мүмкіндік береді.

УКББЖ-да олардың цифрлық іздерін талдау негізінде киберқауіпсіздік (киберқауіпті) пайдаланушы әрекетінің үлгілерін алу және талдау схемасы келесідей болады, 1 суретті қараңыз.



1 сурет – Олардың цифрлық іздерін талдау негізінде УКББЖ-дағы киберқауіпсіздік (киберқауіпті) пайдаланушы әрекетінің үлгілерін алу және талдау схемасы

Осылайша, цифрлық іздерді секвенциялық талдау әдісін пайдалану УКББЖ АҚ жүйесінің АҚ қатерлерін уақтылы анықтау және оларға жауап беру қабілетін жақсартады, сондай-ақ УКББЖ-дағы пайдаланушылардың іс-әрекеттері туралы категориялық деректерді тиімдірек өңдеуге және талдауға мүмкіндік береді.

Қорытынды.

Зерттеу барысында цифрлық іздерді дәйекті талдау (digital traces) негізінде пайдаланушылардың киберқауіпсіздік мінез-құлқының максималды дәйекті үлгілерін алу әдісі университеттің кибернетикалық білім беру жүйесінің (УКББЖ) ақпараттық қауіпсіздігін (АҚ) қамтамасыз етуде бірқатар артықшылықтарға ие екендігі анықталды. Атап айтқанда, цифрлық іздерді дәйекті талдауы негізінде пайдаланушылардың киберқауіпсіздік әрекетінің максималды дәйекті үлгілерін алу әдісіне негізделген жұмыста ұсынылған тәсілді қолдану пайдаланушының аномальды әрекетін анықтауға мүмкіндік береді. Бұл УКББЖ ақпараттық қауіпсіздігіне ықтимал қауіптерді көрсетуі мүмкін. Цифрлық іздерді дәйекті талдау жүйеге жаңа немесе бұрын белгісіз ақпараттық қауіпсіздік қатерлерін анықтауға мүмкіндік беретіні анықталды, өйткені УКББЖ және оның қауіпсіздік циклдері пайдаланушы мінез-құлқындағы өзгерістерге тез бейімделе алады. Пайдаланушылардың киберқауіпті мінез-құлқының дәйекті үлгілерін зерделеу арқылы жүйені пайдаланудың типтік сценарийлерін анықтауға болатыны көрсетілген, бұл пайдаланушының қалыпты әрекетін қалыпсыздан анықтауға көмектеседі.

ӘДЕБИЕТТЕР

- [1] Miroshnikova, T. (2020). Innovative Technologies in Education. In E3S Web of Conferences (Vol. 210, p. 18135). EDP Sciences.
- [2] Zacher, S. (2020). Digital twins for education and study of engineering sciences. International Journal on Engineering, Science and Technology, 2(2), 61-69.
- [3] Kartashova, L. A., Gurzhii, A. M., Zaichuk, V. O., Sorochan, T. M., & Zhuravlev, F. M. (2020). Digital twin of an educational institution: an innovative concept of blended learning. In Proceedings of the symposium on advances in educational technology, aet. 300-309.

[4] Smirnov, I. (2018, June). Predicting PISA scores from students' digital traces. In Proceedings of the International AAAI Conference on Web and Social Media (Vol. 12, No. 1).

[5] Ye, D., & Pennisi, S. (2022). Using trace data to enhance Students' self-regulation: A learning analytics perspective. *The Internet and Higher Education*, 54, 100855.

[6] Kureychik, V. V., Bova, V. V., & Kravchenko, Yu. A. (2020). Metod poiska posledovatelnykh patternov povedeniya polzovateley v internet-prostranstve. *Izvestiya Yuzhnogo federalnogo universiteta. Tekhnicheskie nauki*, (4 (214)), 6-21.

[7] Wedyan S. Review and Comparison of Associative Classification Data Mining Approaches, *International Journal of Computer, Information, Systems and Control Engineering*, 2014, Vol. 8, pp. 34-45.

[8] Husák, M., Kašpar, J., Bou-Harb, E., & Čeleda, P. (2017, August). On the sequential pattern and rule mining in the analysis of cyber security alerts. In Proceedings of the 12th International Conference on Availability, Reliability and Security (pp. 1-10).

[9] Buczak, A. L., Berman, D. S., Yen, S. W., Watkins, L. A., Duong, L. T., & Chavis, J. S. (2017, April). Using sequential pattern mining for common event format (CEF) cyber data. In Proceedings of the 12th annual conference on cyber and information security research (pp. 1-4).

[10] Hossain, M., Sattar, A. S., & Paul, M. K. (2019, December). Market basket analysis using apriori and FP growth algorithm. In 2019 22nd international conference on computer and information technology (ICCI) (pp. 1-6). IEEE.

Kariyrbek Makulov, candidate of economic sciences, Yessenov University, Aktau, Kazakhstan, kaiyrbek.makulov@yu.edu.kz

Lazat Kydyralina, PhD, Shakarim University, Semey, Kazakhstan, lazat_75@mail.ru

Akbala Abuova, PhD, associate professor, International University of Transport and Humanities, Almaty, Kazakhstan, abuovaakbala@gmail.com

Nurgazy Kurbaniyazov, doctoral student, Farabi University, Almaty, Kazakhstan, kurbaniyazov.nk@gmail.com

Miroslav Lahno, master, National University of Bioresources and Environmental Management of Ukraine, Kiev, Ukraine, lvaua21@gmail.com

STUDYING PATTERNS OF CYBERSECURITY AND CYBERDANGEROUS BEHAVIOR OF STUDENTS BASED ON THE ANALYSIS OF THEIR DIGITAL TRACES

Abstract. The article shows that the method of obtaining the maximum consistent patterns of cybersecurity behavior of users based on sequential analysis of digital traces (DT) has a number of advantages in ensuring information security (IS) of the cybernetic educational system of the University (CESU). In particular, based on the method of obtaining the maximum consistent patterns of cybersecurity behavior of users based on the sequential analysis of the DT, it is possible to detect abnormal user behavior in the CESU. And this may indicate potential threats to the information security of the CESU as a whole, and its individual components, for example, such as digital twins (DT) of academic disciplines and students. It is established that a consistent analysis of the DT will allow the system to detect new or previously unknown threats to information security, since the CESU and its security contours will be able to quickly adapt to changes in user behavior patterns when interacting with digital counterparts of academic disciplines. It is shown that by studying consistent patterns of cyber-

dangerous user behavior, it is possible to identify typical scenarios of using the system, which helps to identify normal user behavior from abnormal.

Keywords: information security, cybernetic educational system, digital footprints, digital twins, patterns of behavior

Кайырбек Макулов, к.э.н., Yessenov University, Актау, Қазақстан,
kaiyrbek.makulov@yu.edu.kz

Лазат Кыдыралина, PhD, Shakarim University, Семей, Қазақстан,
lazat_75@mail.ru

Ақбала Абуова, PhD, ассоциированный профессор, International University of Transport and Humanities, Алматы, Қазақстан, abuovaakbala@gmail.com

Нургазы Курбаниязов, докторант, Farabi University, Алматы, Қазақстан,
kurbaniyazov.nk@gmail.com

Мирослав Лакно, магистр, National University of Bioresources and Environmental Management of Ukraine, Киев, Украина, lvaua21@gmail.com

ИЗУЧЕНИЕ ПАТТЕРНОВ КИБЕРБЕЗОПАСНОГО И КИБЕРОПАСНОГО ПОВЕДЕНИЯ СТУДЕНТОВ НА ОСНОВЕ АНАЛИЗА ИХ ЦИФРОВЫХ СЛЕДОВ

Аннотация. В статье показано, что метод получения максимальных последовательных паттернов кибербезопасного поведения пользователей на основе секвенциального анализа цифровых следов (ЦС) обладает рядом преимуществ в обеспечении информационной безопасности (ИБ) кибернетической образовательной системы университета (КОСУ). В частности, на базе метода получения максимальных последовательных паттернов кибербезопасного поведения пользователей на основе секвенциального анализа ЦС можно обнаруживать аномальное поведение пользователей в КОСУ. А это может указывать на потенциальные угрозы для ИБ КОСУ в целом, и ее отдельных компонентов, например, таких, как цифровые двойники (ЦД) учебных дисциплин и студентов. Установлено, что последовательный анализ ЦС позволит системе обнаруживать новые или ранее неизвестные угрозы ИБ, поскольку КОСУ и ее контуры безопасности смогут оперативно адаптироваться к изменениям в шаблонах поведения пользователей при взаимодействии с цифровыми двойниками учебных дисциплин. Показано, что путем изучения последовательных паттернов киберопасного поведения пользователей, можно выявлять типичные сценарии использования системы, что способствует выявлению нормального поведения пользователей от аномального.

Ключевые слова: информационная безопасность, кибернетическая образовательная система, цифровые следы, цифровые двойники, паттерны поведения

Қабылданған күні: 2024 жылғы 18 қыркүйек
Рецензиядан өткен күні: 2025 жылғы 12 ақпан
Мақұлданған күні: 2025 жылғы 04 мамыр