

А.Кушубек^{1*}, Б.Шарипбеков², Б.Рахимов³, С.Сантеева⁴, А.Шайханова⁵
^{1,2,3,4,5}ҚР ҒЖБМ «Ұлттық тестілеу орталығы» ШЖҚ РМК, Астана қ, Қазақстан Республикасы
*e-mail: b.sharipbekov@testcenter.kz

¹ORCID 0009-0006-2436-314X, ²ORCID 0009-0006-4551-1957, ³ORCID 0009-0001-3609-960X

⁴ORCID 0000-0001-9426-6704, ⁵ORCID 0000-0001-6006-4813

ІТ-ИНФРАҚҰРЫЛЫМДАРДЫҢ АҚПАРАТТЫҚ ҚАУІПСІЗДІГІН БАСҚАРУДА ЖАСАНДЫ ИНТЕЛЛЕКТ НЕГІЗІНДЕГІ ЛОГ ТАЛДАУ ЖӘНЕ АВТОМАТТАНДЫРЫЛҒАН ӘРЕКЕТ ЕТУ АРХИТЕКТУРАЛАРЫНА ШОЛУ

Соңғы он жылда киберқауіпсіздік саласы елеулі өзгерістерге ұшырады: технологиялардың қарқынды дамуымен қатар жаңа қатерлердің саны да артып келеді. Ұйымдар инсайдерлік қауіптерге, онлайн тыңшылыққа, зиянды бағдарламаларға және деректердің сыртқа ағуына бір мезгілде тап болуда. Кәсіпорын қызметі өзара байланысқан ақпараттық жүйелерге сүйенетіндіктен, кибершабуыл бүкіл жұмыс процесін бұзып, айтарлықтай қаржылық шығынға әкелуі мүмкін. Осыған байланысты компаниялар құпия деректері мен сандық меншігін қорғауда алдын алу шараларына көбірек көңіл бөлуде. Мақалада жасанды интеллект технологияларын пайдалана отырып, ІТ инфрақұрылымның ақпараттық қауіпсіздігін орталықтандырып басқару әдістері мен архитектурасы қарастырылады. Қауіпсіздік оқиғаларын жинап, өзара байланыстыру үшін SIEM жүйелерін қолдануға, сондай-ақ аномалияларды анықтап, оқиғаларды талдайтын интеллектуалды алгоритмдерді біріктіруге басты назар аударылады. Оқиғаларды басқару жүйесін, жасанды интеллект модулін және автоматтандырылған жауап беруге арналған SOAR платформасын біріктіретін архитектура жобасы ұсынылады. Журнал талдауына негізделген қатерлерді анықтау мен азайтудың практикалық сценарийлері, қорғаныс шараларын автоматтандыру мүмкіндіктері талданады. Нәтижелер интеллектуалды талдау мен процестерді автоматтандыру оқиғаларды анықтау тиімділігін арттырып, ақпараттық қауіпсіздік мамандарының жұмыс жүктемесін азайтып, жауап беру уақытын қысқартатынын көрсетеді.

Түйін сөздер: киберқауіп шабуылдар, ақпараттық қауіпсіздік, SIEM, жасанды интеллект, SOAR, автоматтандыру, қауіпсіздік оқиғалары.

Кіріспе

Технологиялардың үздіксіз дамуы жаңа киберқауіптердің пайда болуын күн санап арттырып келеді. Осының салдарынан киберқауіпсіздік саласы соңғы онжылдықта түбегейлі өзгерді. Бүгінде әрбір ұйым бірнеше тәуекелге бір мезгілде тап болады: инсайдерлік қауіптер, онлайн тыңшылық, компьютерлік вирустар және деректердің рұқсатсыз сыртқа ағуы. Кәсіпорындардың қызметі технологиялар мен өзара байланысқан ақпараттық жүйелерге тәуелді болғандықтан, кибершабуыл ықтималдығы да, оның операциялық қызмет пен қаржылық нәтижелерге тигізетін әсері де арта түсуде. Мұндай жағдай тиімді қорғаныс шараларын талап етеді - сондықтан кәсіпорындар құпия деректері мен сандық меншігін қорғауға белсенді кірісуде [1].

Бұл зерттеу SIEM, SOAR және жасанды интеллект технологияларын қамтитын заманауи ақпараттық қауіпсіздік жүйелерін кешенді талдауды мақсат етеді: олардың негізгі сипаттамалары, артықшылықтары, енгізудің озық тәжірибелері мен қолданыстағы шектеулері қарастырылады. Мақалада ұйымдарды заманауи киберқауіптерден қорғауды күшейту үшін SIEM және SOAR шешімдерін жасанды интеллектпен біріктірудің маңызы зерделенеді. Осы жүйелердің жалпы киберқауіпсіздік архитектурасындағы рөлі, сондай-ақ мониторинг, оқиғаларды корреляциялау және оларға жауап беру процестерін автоматтандыру мүмкіндіктері талданады.

Ұйым инфрақұрылымын кибершабуылдардан қорғау бүгінде әлемдік ауқымдағы басым міндетке айналды. Қатерлер күрделене түскен сайын, дәстүрлі қауіпсіздік шараларының жеткіліксіз болатыны айқындала бастады.

Зерттеу материалдары мен әдістері

Жасанды интеллект (AI) пен машиналық оқытуды (ML) қолдану қауіптерді ерте кезеңде анықтауға мүмкіндік береді әрі анықтау мен жауап беру жүйелерінің мүмкіндіктерін едәуір кеңейтеді. Жүйе архитектурасы бірнеше ақпараттық технологияны өзара біріктіруге негізделген. SIEM (Security Information and Event Management) жүйелері желіден, серверлерден және цифрлық құрылғылардан (endpoint) журналдарды орталықтандырып жинап, талдау үшін қолданылады. SOAR (Security Orchestration, Automation and Response) инциденттерге автоматтандырылған жауап беру әрекеттерін орындайды. Жасанды интеллект алгоритмдері SIEM арқылы анықталған инциденттерге сұрау салып талдау жасайды және қолданушыға түсінікті жауап қалыптастырады [2]. Талдау мен жауап беру процесі бірнеше кезеңнен тұрады.

Нәтижелер және талқылау

Деректерді жинау. SIEM жүйелері цифрлық инфрақұрылымның барлық деңгейінен оқиғаларды жинайды - желілік белсенділіктен бастап инфрақұрылым жүйелерінің қауіпсіздік журналдарына дейін.

Нақты уақыттағы талдау. Жасанды интеллект компоненттері кіріс деректерін өңдеп, қауіп-қатер мен ауытқуларды алдын ала болжайтын тенденцияларды іздейді.

Автоматтандырылған жауап беру. SOAR платформалары алдын ала жазылған сценарийлерге (playbooks) сәйкес әрекет етеді - мысалы, бұзылған жүйелерді оқшаулайды немесе зиянды IP мекенжайларын блоктайды. Сонымен қатар олар жүйе компоненттері арасындағы байланысты қамтамасыз етеді.

Жасанды интеллект қауіпсіздік сценарийлерін - фишинг, зиянды бағдарлама, инсайдерлік қауіп және DDoS шабуылдарын - модельдеу тиімділігін айтарлықтай арттырды. Анықтау дәлдігі белгілі қауіптер үшін 95%-ға, ал белгісіз (нөлдік күн) шабуылдар үшін 87%-ға жетеді. Жауап беру жылдамдығы да өзгерді: SOAR-да AI қолдану оқиғаға жауап беру уақытын орта есеппен 60%-ға қысқартып, әрекетті бірнеше секунд ішінде орындауға мүмкіндік береді. Бұған қоса, модельдердің дәлдігі жалған дабылдарды шамамен 40%-ға азайтады — бұл аналитиктерді біртекті тексерістен босатып, күрделірек міндеттерге көңіл бөлуге мұрса береді [2].

Осы артықшылықтарға қарамастан, мұндай жүйелерді енгізу бірқатар қиындыққа тап болады. Біріншіден, деректер сапасы: жүйенің тиімділігі векторлық базаға енгізілген деректердің сапасына тікелей тәуелді, ал дұрыс форматталмаған деректер қауіпке әрекет ету ықтималдығын төмендетуі мүмкін. Екіншіден, жасанды интеллектке бағытталған қарсыласу шабуылдары (adversarial attacks): шабуылдаушылар арнайы дайындалған деректерді енгізіп, AI алгоритмдерін алдауға тырысуы ықтимал. Үшіншіден, ресурс сыйымдылығы: күрделі модельдерді оқыту мен орналастыру елеулі есептеу қуатын талап етеді.

Осы мәселелерді шешу үшін жобада жүктемелерді бөліп өңдеу, деректерді кеңейту әдістерін (data augmentation) енгізу және манипуляцияға төзімді «тұрақты» модельдер жобалау ұсынылады. Мұндай тәсіл ақпараттық инфрақұрылымның шабуылдарға жалпы төзімділігін арттырып қана қоймайды, ұйымдарға үздіксіз өзгеріп отыратын киберқауіпсіздік ландшафтына бейімделуге де жол ашады [2].

Аталған жұмыстарды жүргізудегі өзекті мәселелердің бірі — журнал деректерін талдау. Журнал көздері әртүрлі болуы мүмкін: жұмыс станциялары, серверлер, firewall-дар, желілік құрылғылар, түрлі ақпараттық жүйелер және басқалары. Әр жүйенің журналы өзіндік

форматта жазылатындықтан, талдау алдында оны алдымен өңдеп, содан кейін деректерді векторлық базаға енгізу қажет.

Дәстүрлі талдаудың негізгі мәселелері:

1. Алдын ала өңдеудің күрделілігі. Көптеген жүйе көп сатылы өңдеуді қажет етеді. Мұнда талдау кезеңін - өңделмеген журналдарды құрылымдық деректерге түрлендіруді - дұрыс жасамау қателіктер мен ақпарат жоғалуына әкеледі [3].

2. Шабуыл деректерінің тапшылығы. Нақты жағдайда жүйенің қалыпты жұмысы туралы дерек көп, ал аномалиялар мен шабуыл мысалдары сирек кездеседі. Осы теңгерімсіздік инцидентті болған сәтте талдауды қиындатады [3].

3. Үздіксіз оқытудың болмауы. Қолданыстағы алгоритмдер сарапшылар жаңа қауіп түрлерін анықтаған кезде жеткілікті жылдам жаңартылмайды - бұл олқылық жаңа қатерлерге осал тұс қалдырады [3].

Жоғарыда аталған мәселелерді шешу үшін ұсынылып жүрген тәсілдермен таныстым. Ұсынылатын модель - журнал талдауының барлық кезеңін бір жерде орындайтын біртұтас жүйе. Ол бірнеше маңызды бөліктен құралады.

Күрделі журнал талдауының орнына модель «шикі» деректермен тікелей жұмыс істейді: таңбаларды тікелей сандық форматқа түрлендіреді. Бұл жүйе жұмысын жеңілдетіп қана қоймай, талдау барысында жиі кездесетін қателерді де болдырмайды. Модельдің өзегі - трансформатор. Ол журнал жолдарын талдап, олардың құрылымын түсінеді әрі мәтін бөліктері арасындағы тәуелділіктерді табады. Зейін механизмі оған журналдың қай бөлігі маңызды екенін ажыратуға көмектеседі. Ең соңында қарапайым жіктеуіш түр - ол логтың қалыпты ма, әлде аномалия ма екенін шешеді.

Модель екі кезеңде оқытылады. Біріншісі - қалыпты журналдарда өзін-өзі оқыту. Мұнда модель тек әдеттегі журналдармен жұмыс істейді, шабуыл имитацияланбайды. Ауытқуларды тани білуі үшін қалыпты журналдарға арнайы өзгеріс енгізіледі: таңбалар қосылады, ауыстырылады немесе жойылады. Осылайша модель нендей журналдардың ерекше саналатынын үйренеді. Екіншісі - кері байланыс арқылы қосымша оқыту. Мамандар нақты шабуылдарды тауып, оларды белгілегенде модель толық оқытылады. Нәтижесінде инциденттерді анықтау дәлдігі артады, ал модель өз қателерінен сабақ алып, уақыт өте жетіле түседі [3].

Мұндай тәсіл әртүрлі журнал көздері бар ортада талдау жүйесін құрудың басты кедергісін шешеді — күрделі алдын ала өңдеуді де, шабуыл туралы белгіленген деректердің үлкен көлемін де қажет етпейді. Сонымен қатар ол қауіпсіздік жүйесіне өзгермелі қауіп ландшафтымен бірге дамуға мүмкіндік беріп, икемділікті қамтамасыз етеді.

Қауіпсіздікті басқарудың тиімді архитектурасы бүгінде үш компонентке негізделеді [4] (1-сурет):

1. SIEM (Security Information and Event Management) - бүкіл инфрақұрылымнан оқиғаларды нақты уақытта орталықтандырып жинап, корреляциялайтын жүйе.

2. Жасанды интеллект (AI) - классикалық әдістер таба алмайтын жасырын үлгілер мен ауытқуларды анықтау үшін терең оқыту алгоритмдерін қолданатын компонент.

3. SOAR (Security Orchestration, Automation and Response) - жауап беру сценарийлерін (playbooks) автоматты орындап, қауіпсіздік маманының күнделікті операцияларға араласуын азайтады.

Кең тараған шешімдердің бірі - ELK-стекке негізделген Elastic Security платформасы (1-сурет). Ол журналдарды орталықтандырып жинауды, сақтауды және талдауды қамтамасыз етеді, әрі аномалияларды анықтау үшін кіріктірілген AI механизмдерін пайдаланады [5]. Бұл тәсіл жобалада ұсынылған архитектураға жақын: онда да орталықтандырылған журнал талдауы мен AI компоненті қатар қолданылады.

Оның жұмысы келесідей:

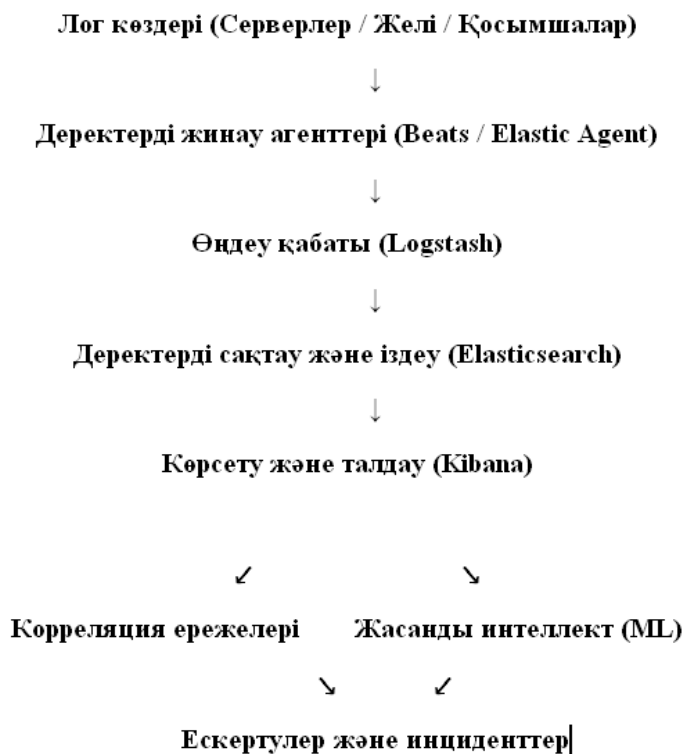
1. Логтарды орталықтандырылған жинау (Beats / Agent)

2. Elasticsearch-та сақтау және өңдеу

3. Kibana арқылы визуализация

4. Ережелер мен кірістірілген машиналық оқыту негізінде талдау

Ерекшелігі – кірістірілген машиналық оқыту механизмдері қолданылса, шектеуі – AI алдын ала анықталған алгоритмдермен шектелген.



1-сурет – ELK-стек архитектурасы

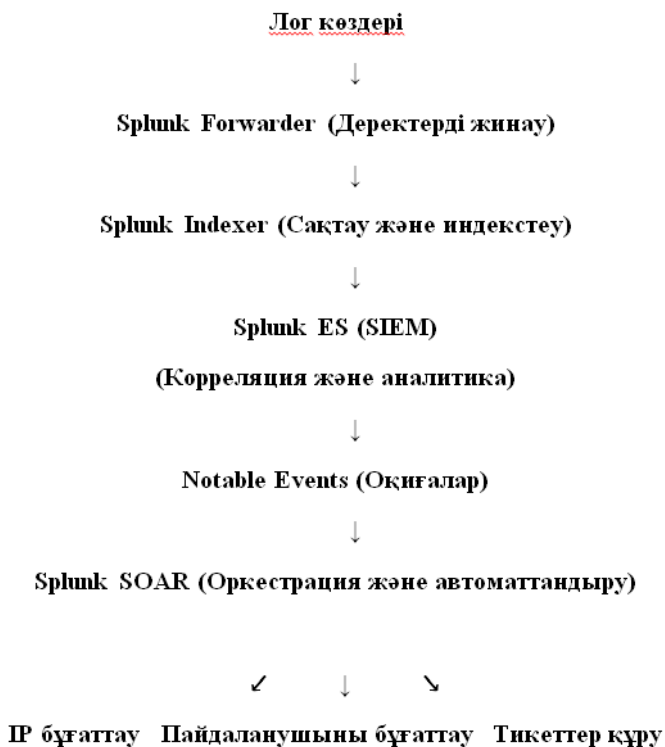
Кең қолданыстағы тағы бір шешім - SIEM мен SOAR интеграциясын жүзеге асыратын Splunk Enterprise Security және Splunk SOAR біріктірілген жүйесі (2-сурет). Ол қауіпсіздік оқиғаларын талдаумен шектелмейді: playbooks арқылы оқиғаларға автоматты түрде жауап та береді [6]. Дәл осы мүмкіндік жобада ұсынылған жүйенің автоматтандырылған жауап беру тұжырымдамасына толық сәйкес келеді. Жұмыс принципі мынадай:

1. Логтар Splunk Universal Forwarder арқылы жиналып, Indexer-ге жіберіледі.

2. Деректер Parsing және Normalization (CIM – Common Information Model) арқылы бір форматқа келтіріледі.

3. Корреляция механизмдері күдікті әрекеттерді анықтайды. Нәтижесінде инциденттер қалыптасады. Инциденттер Splunk SOAR-ға беріледі. SOAR ішінде playbooks (алдын ала жазылған конфигурациялар) арқылы автоматты әрекеттер орындалады.

Ерекшелігі – икемді корреляция және қуатты автоматтандыру жүйесін қолдануда болса, кемшілігі – AI негізінен статистика мен алдын ала модельдерге тәуелді болады.



2-сурет – Splunk Enterprise Security және Splunk SOAR

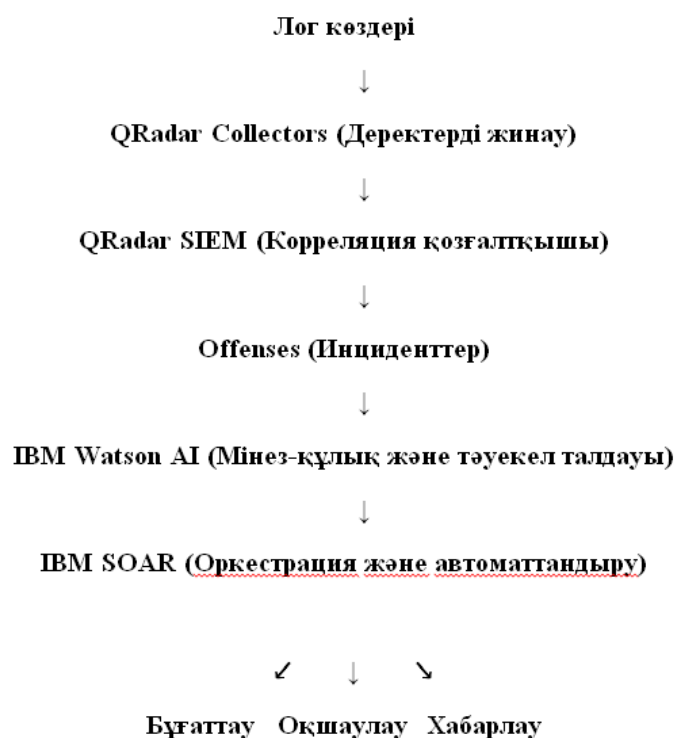
IBM QRadar жүйесі IBM SOAR-мен біріктіріліп, SOC құруға арналған корпоративтік шешім ретінде ұсынылады (3-сурет). Ол қауіпті анықтау дәлдігін арттыру үшін оқиғалар корреляциясын, мінез-құлық талдауын және AI (IBM Watson) интеграциясын қатар пайдаланады [7]. Жұмыс принципі мынадай:

1. Логтар QRadar Event/Flow Collectors арқылы жиналады, содан кейін деректер DSM (Device Support Module) көмегімен парсингтен өтеді.

2. Correlation Engine (CRE rules) оқиғалар арасындағы байланысты тауып, соның негізінде инциденттер қалыптастырады. Тереңірек талдау үшін User Behavior Analytics (UBA) қосымша қолданылады.

3. IBM Watson AI тәуекелді бағалап, талдау жүргізеді. Одан кейін инциденттер IBM SOAR-ға жіберіліп, автоматты әрекеттер орындалады.

Жүйенің басты артықшылығы - күрделі корреляция мен мінез-құлық талдауы, ал негізгі шектеуі - жабықтығы және баптауының күрделілігі.

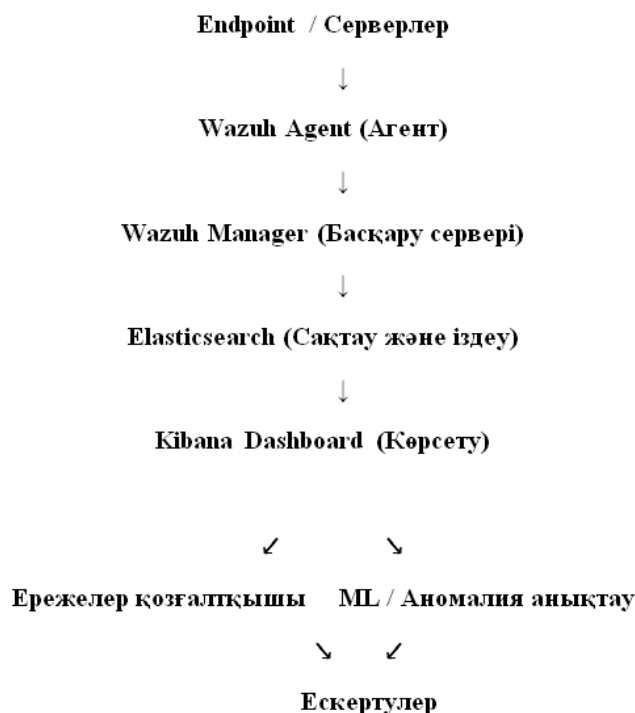


3-сурет – IBM QRadar жүйесі

Ашық бастапқы кодты (open-source) шешімдердің ішінен Wazuh жүйесін бөле айтқан жөн (4-сурет) [11]. Ол Elastic Stack негізінде құрылған, журнал талдауын, интрузияларды анықтауды және машиналық оқыту механизмдерімен интеграцияны қолдайды. Практикалық тұрғыдан бұл шешім ELK базасында іске асыруға ең жақын жүйе. Жұмыс принципі мынадай [8]:

1. Логтар endpoint-тардан Wazuh Agent арқылы жиналып, Wazuh Manager ішінде өңделеді.
2. Rules Engine (XML rules) шабуылдарды анықтайды. Оған қосымша File Integrity Monitoring мен Rootcheck қолданылады.
3. Нәтижелер Kibana/Wazuh Dashboard арқылы ақпараттық қауіпсіздік маманына ұсынылады.

Жүйенің басты артықшылығы - ашық бастапқы коды әрі IDS пен SIEM-нің біріктірілуі, ал негізгі шектеуі - кеңейтілген AI функционалының әзірге жасалмауы [9].

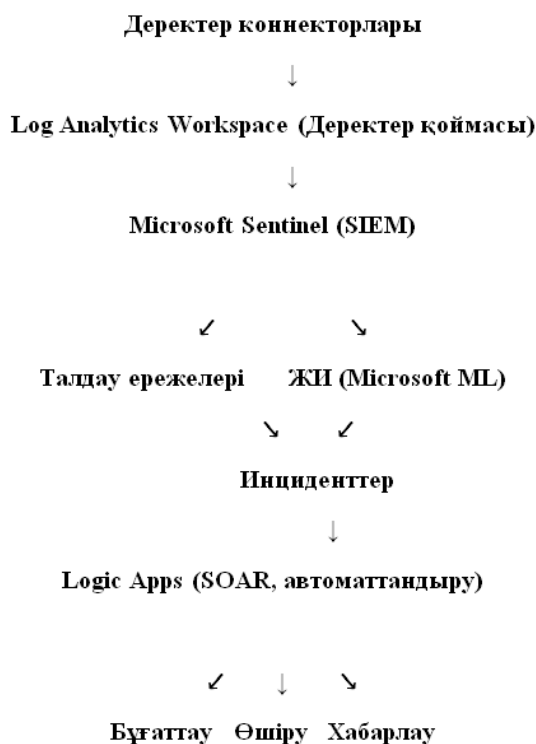


4-сурет – Wazuh лог талдау жүйесі

Бұлтты орта инфрақұрылымдарында Microsoft Sentinel жүйесі белсенді қолданылады, ол SIEM және SOAR функцияларын біріктіреді, сонымен қатар оқиғаларды талдау және жауап беруді автоматтандыру үшін кіріктірілген AI модельдерін қолданады (5-сурет) [15]. Жұмыс принципі келесідей [10]:

1. Деректер Data Connectors (Azure, Office 365, Syslog, API) арқылы жиналады.
2. Логтар Log Analytics Workspace ішінде сақталады, KQL (Kusto Query Language) арқылы талдау жүргізіледі.
3. Analytics Rules инциденттерді анықтайды, UEBA (User Entity Behavior Analytics) қолданушы әрекетін талдайды.
4. Инциденттер SOAR арқылы өңделеді, автоматты әрекеттер (response actions) орындалады.

Ерекшелігі – бұлтты орталарда жиі қолданылады және жақсы масштабталатын шешім, шектеуі – Microsoft экожүйесіне тәуелді [12].



5-сурет – Microsoft Sentinel бұлтты ақпараттық қауіпсіздікті қамтамасыз ету жүйесі

Заманауи зерттеулер, сонымен қатар, үлкен тілдік модельдерге (LLM) негізделген тәсілдердің дамуын көрсетеді. Мысалы, жобада LLaMA сияқты модельдерді қолдану журналдарды талдауға, оқиғаларды түсіндіруге және жауап беру бойынша ұсыныс жасауға мүмкіндік беретіні атап өтіледі [13]. Бұл бағыт бүгінде айрықша өзекті: AI дәл журнал талдауы үшін қолданылады әрі жобада ұсынылған архитектурамен үйлеседі.

Аталған зерттеуде күрделі талдауды қажет етпей-ақ ауытқуларды анықтауға мүмкіндік беретін журнал талдау тәсілі де ұсынылған. Бұл журналды талдау міндеттерінде AI қолданудың тиімділігін тағы бір рет растайды.

Заманауи жүйелердің тағы бір маңызды буыны - Shuffle секілді SOAR платформалары арқылы жүзеге асатын жауап беруді автоматтандыру [14]. Мұндай платформа автоматты жауап беру сценарийлерін іске қосуға мүмкіндік береді: IP мекенжайларын бұғаттау, пайдаланушыларды өшіру, хабарландыру жіберу және басқа да әрекеттер.

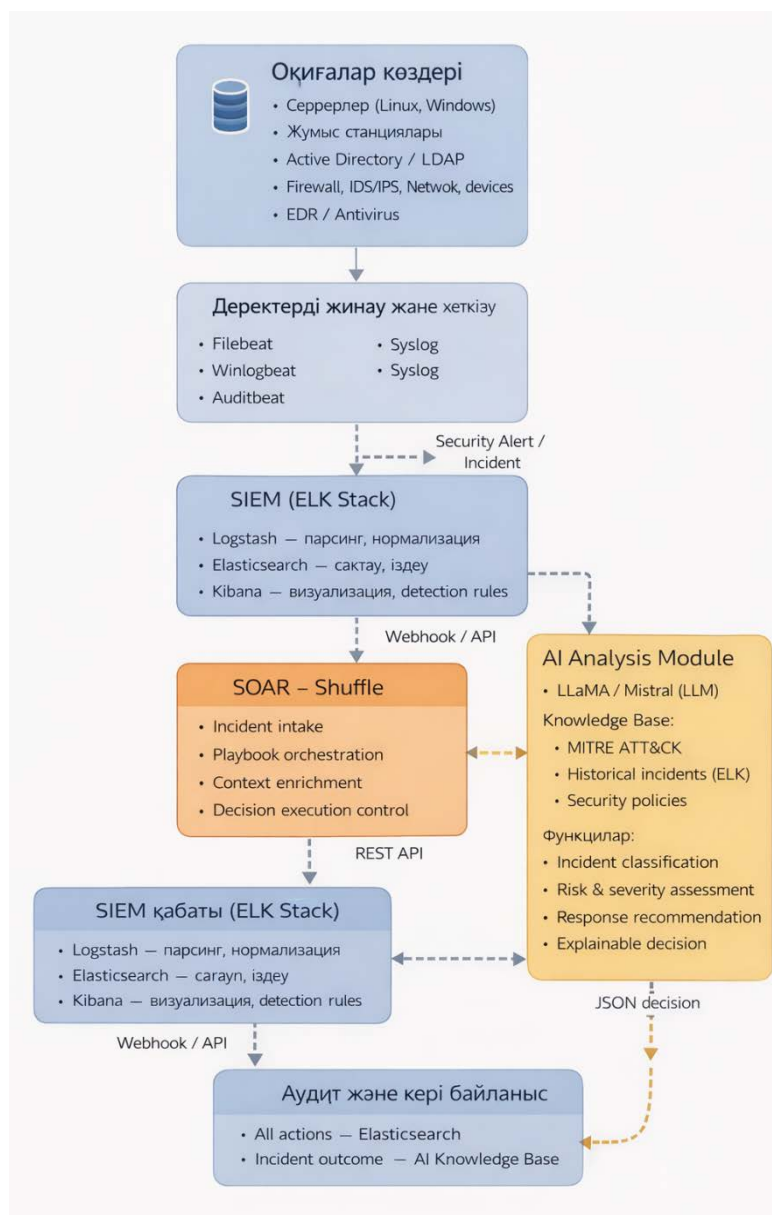
Қорыта айтқанда, қолданыстағы шешімдерді талдау қазіргі ақпараттық қауіпсіздік жүйелерінің SIEM, жасанды интеллект және SOAR-ды қамтитын архитектураға сүйенетінін көрсетеді. Дегенмен көп жағдайда жүйеге дайын модельдер енгізіліп, олар алдын ала анықталған алгоритмдермен шектеледі. Ал арнайы оқытылған модельдерді пайдалану талдау мен автоматтандыру мүмкіндіктерін айтарлықтай кеңейтеді.

Жасалатын жұмыс келесі қадамдардан тұрады (6-сурет):

1. Логтар SIEM жүйесінен (SIEM жүйесі ретінде ELK) алынады.
2. Деректер алдын ала өңдеуден өтеді (parsing, оқиға түріне байланысты жіктеу).
3. SIEM жүйесіндегі ережелер базасы embedding-ке айналып, Qdrant ішіне векторлық мәнге жазылады.
4. Similarity search (деректер арасынан ең ұқсасын табу әдісі) арқылы ұқсас инциденттер табылады.
5. LLM (LLaMA) логтарды семантикалық деңгейде талдайды. Инциденттің мәні, себебі және тәуекелі анықталады. Модель қолданушыға арнап ұсыныстар (recommendations) генерациялайды.

6. Нәтиже SOAR жүйесіне жіберіледі.

Осының нәтижесінде контекстік және семантикалық талдау жүргізіледі, бұл кез келген цифрлық ортаға бейімделгіш және интеллектуалды жүйе ретінде жүзеге асады.



6-сурет – Жоба архитектурасы

Логтар SIEM жүйесінен (ELK) орталықтандырылып жинақталады да, API арқылы жасанды интеллект модуліне жіберіледі. Мұнда SIEM тек дерек көзі рөлін атқарады - осының арқасында қолданыстағы инфрақұрылымды өзгертпей-ақ интеграция жасауға болады әрі жүйе әртүрлі SIEM платформаларымен қатар жұмыс істей алады.

Деректер алдын ала өңделгендіктен, классикалық SIEM-дегідей толық parsing (grok, regex) қажет емес. Жеткілікті болатыны - бірнеше негізгі өріс: уақыт белгісі (timestamp), дерек көзінің IP мекенжайы (source IP) және хабарлама (message). Оның үстіне жүйе raw logs форматымен де жұмыс істей алады, бұл енгізуді жеделдетіп, форматқа тәуелсіздік береді.

Келесі кезеңде логтар embedding форматына түрленеді - әрбір лог жазбасы векторға айналады. Бұл үшін арнайы embedding модельдері қолданылады, нәтижесінде логтар

синтаксис бойынша емес, мағынасы бойынша талданады. Осындай тәсіл әртүрлі форматта жазылған ұқсас шабуылдарды тануға және артық шуды сүзуге мүмкіндік береді.

Барлық embedding деректері Qdrant векторлық деректер базасында сақталады. Әр лог үшін embedding пен metadata (IP, уақыт, пайдаланушы) қатар жазылып, индекстеу арқылы жоғары жылдамдықты іздеу қамтамасыз етіледі. Осылайша тарихи контекст жинақталып, жүйені масштабтауға жол ашылады.

Жаңа логтар түскенде similarity search механизмі іске қосылады: жаңа лог embedding-ке айналады, Qdrant ішінен оған ең ұқсас жазбалар табылып, бұрынғы инциденттермен салыстырылады. Дәл осы қадам unknown attack detection мүмкіндігін береді, жалған позитивтерді азайтады және контекстке негізделген талдау жасауға мүмкіндік ашады.

Одан әрі LLM (мысалы, LLaMA) арқылы семантикалық талдау жүргізіледі. Модель логтарды мәтін ретінде оқып, prompt негізінде шабуыл түрін, қауіптілік деңгейін және оның себептерін анықтайды. Талдау сапасын арттыру үшін модельге контекст ретінде ұқсас логтар қоса беріледі - бұл нәтижені түсіндірмелі түрде ұсынуға көмектеседі.

Нәтижесінде жүйе инцидент түрін (мысалы, Brute Force немесе SQL Injection), негізгі себебін (root cause) және тәуекел деңгейін (low, medium, high) айқындайды. Мұндай құрылымдалған әрі түсінікті ақпарат SOC аналитиктеріне инциденттерді басымдыққа қарай сұрыптауды жеңілдетеді.

Осы деректерге сүйене отырып, жасанды интеллект ұсыныстарды автоматты қалыптастырады - IP мекенжайды бұғаттау, пайдаланушыны өшіру немесе қосымша тексеру жүргізу сияқты әрекеттерді нұсқайды. Бұл аналитиктердің жүктемесін жеңілдетеді, әрекет ету уақытын қысқартады және стандартты процестерді автоматтандыруға мүмкіндік береді.

Соңғы кезеңде барлық нәтиже SOAR жүйесіне (мысалы, Shuffle) жіберіледі. Онда алдын ала анықталған playbook-тар іске қосылып, автоматты әрекеттер орындалады. Соның арқасында процесс толық автоматтандырылып, қауіпке әрекет ету уақыты айтарлықтай қысқарады әрі инциденттер тез оқшауланады.

ELK, SOAR және AI негізіндегі орталықтандырылған басқару архитектурасы қазіргі киберқауіптерге қарсы күрестегі күрделі мәселелерге кешенді, тиімді шешім ұсынады. Мұндай тәсіл ұйымдарға қауіптерді дер кезінде анықтауға, оларға жауап беруге және ақпараттық активтерін қорғауға мүмкіндік береді.

Қорытынды

Қорыта айтқанда, жасанды интеллектке негізделген SIEM жүйелері қауіптерді алдын ала болжай алатындықтан, дәстүрлі құралдармен салыстырғанда тәуекелді әлдеқайда төмендетеді. Мұндай интеллектуалды жүйелер қауіпті ерте кезеңде анықтауда, жауап беруді жеделдетуде және операциялық тиімділікті автоматты арттыруда өзін тиімді құрал ретінде көрсетті. Олар үлкен көлемді деректерді талдап, ауытқуларды тауып, көп еңбекті талап ететін біртекті міндеттерді автоматтандырады - осылайша қауіпсіздік мамандарын стратегиялық шешім қабылдауға босатады. Зиянды бағдарламаларды талдаудан бастап осалдықтарды басқаруға дейінгі кең ауқымды жұмысты осындай жүйелер атқара алады.

Сонымен қатар AI-мен жұмыс істейтін SIEM жүйелері дамып келе жатқан қауіптерге қарсы кешенді қорғаныс қызметін атқарады. Оларды енгізу арқылы ұйымдар үнемі өзгеріп отыратын киберландшафтта сенімділігін нығайтып, күрделі қатерлерді дер кезінде аулай алады әрі тәуекелге төзімділігін арттырады.

Әдебиеттер тізімі

1. Vardalachakis M., Vasilakis M., Tampouratzis M. A Comprehensive Analysis of Features, Benefits, Challenges, and Best Practices of Security Information and Event Management (SIEM) Solutions //

Computer Sciences & Mathematics Forum. – 2025. – Vol. 12, № 1. – Art. 18. – <https://doi.org/10.3390/cmsf2025012018>

2. Singh S. et al. A future-proof approach to cybersecurity compliance: The power of AI and ML in SIEM, SOAR and cloud SOC. – ResearchGate, 2024. – P. 2–6.

3. Pan J. AI based Log Analyser: A Practical Approach // arXiv preprint arXiv:2203.10960. – 2022. – <https://doi.org/10.48550/arXiv.2203.10960>

4. Ramakrishnan S., Chittibala D. R. Enhancing Cyber Resilience: Convergence of SIEM, SOAR, and AI in 2024 // International Journal of Computing and Engineering. – 2024. – Vol. 5, № 2. – P. 36–44. – <https://doi.org/10.47941/ijce.1754>

5. da Silva G. R., de Oliveira B. M. C., Braga R. Comparison of Machine Learning and the ELK Stack for Automated Cyber Attack Detection: A Comparative Approach // 12th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2025), Nice, France. – 2025. – P. 14–20. – https://doi.org/10.48545/advance2025-fullpapers-1_2.

6. Sahay R., Sumasadan M., Eapen B., Meng W., Al Mamu M. R. Enhancing Threat Hunting with Splunk and Generative AI for Automated Security Operations // Research Square (preprint). – 2025. – <https://doi.org/10.21203/rs.3.rs-7515771/v1>

7. Alliouche R., Chenni H. Toward Intelligent Cyber Defense: A Comprehensive Study of SOAR Technologies for AI-Based DDoS Detection. – ResearchGate, 2025. – P. 12–13..

8. Patel D. G., Pujari S. R. AI-driven incident response in cloud security // International Journal of Science and Research Archive. – 2025. – Vol. 15, № 3. – P. 1463–1475. – <https://doi.org/10.30574/ijrsra.2025.15.3.1742>

9. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey // ACM Computing Surveys. – 2009. – Vol. 41, № 3. – Art. 15. – <https://doi.org/10.1145/1541880.1541882>

10. Dakić V., Morić Z., Kapulica A., Regvart D. Leveraging Microsoft Sentinel and Logic Apps for Automated Cyber Threat Response // Edelweiss Applied Science and Technology. – 2024. – Vol. 8, № 6. – P. 4319–4348. – <https://doi.org/10.55214/25768484.v8i6.2933>

11. Habibzadeh A., Rahnama-Moghadam S., Beheshti A. Large Language Models for Security Operations Centers: A Comprehensive Survey // arXiv preprint. – 2025. – arXiv:2509.10858. – <https://doi.org/10.48550/arXiv.2509.10858>

12. Loumachi F. Y., Ghanem M. C., Ferrag M. A. Advancing Cyber Incident Timeline Analysis Through Retrieval-Augmented Generation and Large Language Models // Computers. – 2025. – Vol. 14, № 2. – Art. 67. – P. 1–42. – <https://doi.org/10.3390/computers14020067>

13. Guan W., Wang Y., Zhang X. LogLLM: Log-based Anomaly Detection Using Large Language Models // arXiv preprint. – 2024. – arXiv:2411.08561. – <https://doi.org/10.48550/arXiv.2411.08561>

14. Saha D., Tarek S., Yahyaei K., Saha S. K., Zhou J., Tehranipoor M., Farahmandi F. LLM for SoC Security: A Paradigm Shift // IEEE Access. – 2024. – Vol. 12. – P. 155498–155521. – <https://doi.org/10.1109/ACCESS.2024.3427369>

15. Tendikov N., Rzayeva L., Saoud B., Shayea I., Azmi M. H., Myrzatay A., Alnakhli M. Security Information Event Management Data Acquisition and Analysis Methods with Machine Learning Principles // Results in Engineering. – 2024. – Vol. 22. – Art. 102254. – <https://doi.org/10.1016/j.rineng.2024.102254>

A.Kushubek, B.Sharipbekov, B.Rakhimov, S. Santeeva, A.Shaihanova

A REVIEW OF ARTIFICIAL INTELLIGENCE-BASED LOG ANALYSIS AND AUTOMATED RESPONSE ARCHITECTURES IN IT INFRASTRUCTURE INFORMATION SECURITY MANAGEMENT

The cybersecurity industry has undergone significant changes over the past decade: along with the rapid development of technologies, the number of new threats is also increasing. Organizations are simultaneously faced with insider threats, online espionage, malware, and data leakage. Since the activities of an enterprise rely on interconnected information systems, a cyberattack can disrupt the entire workflow and cause significant financial losses. In this regard, companies are increasingly paying attention to preventive measures to protect their confidential data and digital property. The article considers methods and architecture for centralized management of information security of IT infrastructure using artificial

intelligence technologies. The main focus is on the use of SIEM systems to collect and correlate security events, as well as the integration of intelligent algorithms for detecting anomalies and analyzing events. An architectural project is proposed that combines an event management system, an artificial intelligence module, and a SOAR platform for automated response. Practical scenarios for detecting and mitigating threats based on log analysis, as well as the possibilities of automating protective measures, are analyzed. The results show that intelligent analytics and process automation can increase the efficiency of incident detection, reduce the workload of information security professionals, and shorten response times.

Keywords: attacks, information security, SIEM, artificial intelligence, SOAR, automation, security events.

А.Кушубек, Б.Шарипбеков, Б.Рахимов, С. Сантеева, А.Шайханова

ОБЗОР АРХИТЕКТУРЫ ЛОГ-АНАЛИЗА И АВТОМАТИЗИРОВАННОГО РЕАГИРОВАНИЯ НА ОСНОВЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УПРАВЛЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ИТ-ИНФРАСТРУКТУР

За последнее десятилетие индустрия кибербезопасности претерпела значительные изменения: наряду с быстрым развитием технологий растет и число новых угроз. Организации одновременно сталкиваются с внутренними угрозами, онлайн-шпионажем, вредоносным ПО и утечками данных. Поскольку деятельность предприятия зависит от взаимосвязанных информационных систем, кибератака может нарушить весь рабочий процесс и привести к значительным финансовым потерям. В связи с этим компании все больше внимания уделяют превентивным мерам по защите своих конфиденциальных данных и цифровой собственности. В статье рассматриваются методы и архитектура централизованного управления информационной безопасностью ИТ-инфраструктуры с использованием технологий искусственного интеллекта. Основное внимание уделяется использованию SIEM-систем для сбора и сопоставления событий безопасности, а также интеграции интеллектуальных алгоритмов для обнаружения аномалий и анализа событий. Предлагается архитектурный проект, объединяющий систему управления событиями, модуль искусственного интеллекта и платформу SOAR для автоматизированного реагирования. Анализируются практические сценарии обнаружения и смягчения угроз на основе анализа журналов, а также возможности автоматизации защитных мер. Результаты показывают, что интеллектуальная аналитика и автоматизация процессов могут повысить эффективность обнаружения инцидентов, снизить рабочую нагрузку специалистов по информационной безопасности и сократить время реагирования.

Ключевые слова: атаки, информационная безопасность, SIEM, искусственный интеллект, SOAR, автоматизация, события безопасности.

References

1. Alliouche, R., & Chenni, H. (2025). Toward Intelligent Cyber Defense: A Comprehensive Study of SOAR Technologies for AI-Based DDoS Detection. ResearchGate, 12-13.
2. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), Article 15. <https://doi.org/10.1145/1541880.1541882>
3. da Silva, G. R., de Oliveira, B. M. C., & Braga, R. (2025). Comparison of Machine Learning and the ELK Stack for Automated Cyber Attack Detection: A Comparative Approach. 12th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2025), Nice, France, 14–20. https://doi.org/10.48545/advance2025-fullpapers-1_2
4. Dakić, V., Morić, Z., Kapulica, A., & Regvart, D. (2024). Leveraging Microsoft Sentinel and Logic Apps for Automated Cyber Threat Response. Edelweiss Applied Science and Technology, 8(6), 4319–4348. <https://doi.org/10.55214/25768484.v8i6.2933>
5. Guan, W., Wang, Y., & Zhang, X. (2024). LogLLM: Log-based Anomaly Detection Using Large Language Models (arXiv:2411.08561). arXiv. <https://doi.org/10.48550/arXiv.2411.08561>
6. Habibzadeh, A., Rahnema-Moghadam, S., & Beheshti, A. (2025). Large Language Models for Security Operations Centers: A Comprehensive Survey (arXiv:2509.10858). arXiv. <https://doi.org/10.48550/arXiv.2509.10858>

7. Loumachi, F. Y., Ghanem, M. C., & Ferrag, M. A. (2025). Advancing Cyber Incident Timeline Analysis Through Retrieval-Augmented Generation and Large Language Models. *Computers*, 14(2), Article 67, 1–42. <https://doi.org/10.3390/computers14020067>
8. Pan, J. (2022). AI based Log Analyser: A Practical Approach (arXiv:2203.10960). *arXiv*. <https://doi.org/10.48550/arXiv.2203.10960>
9. Patel, D. G., & Pujari, S. R. (2025). AI-driven incident response in cloud security. *International Journal of Science and Research Archive*, 15(3), 1463–1475. <https://doi.org/10.30574/ijrsra.2025.15.3.1742>
10. Ramakrishnan, S., & Chittibala, D. R. (2024). Enhancing Cyber Resilience: Convergence of SIEM, SOAR, and AI in 2024. *International Journal of Computing and Engineering*, 5(2), 36–44. <https://doi.org/10.47941/ijce.1754>
11. Saha, D., Tarek, S., Yahyaei, K., Saha, S. K., Zhou, J., Tehranipoor, M., & Farahmandi, F. (2024). LLM for SoC Security: A Paradigm Shift. *IEEE Access*, 12, 155498–155521. <https://doi.org/10.1109/ACCESS.2024.3427369>
12. Sahay, R., Sumasadan, M., Eapen, B., Meng, W., & Al Mamu, M. R. (2025). Enhancing Threat Hunting with Splunk and Generative AI for Automated Security Operations (Preprint). *Research Square*. <https://doi.org/10.21203/rs.3.rs-7515771/v1>
13. Singh, S., et al. (2024). A future-proof approach to cybersecurity compliance: The power of AI and ML in SIEM, SOAR and cloud SOC. *ResearchGate*, 2–6.
14. Tendikov, N., Rzayeva, L., Saoud, B., Shayea, I., Azmi, M. H., Myrzatay, A., & Alnakhli, M. (2024). Security Information Event Management Data Acquisition and Analysis Methods with Machine Learning Principles. *Results in Engineering*, 22, Article 102254. <https://doi.org/10.1016/j.rineng.2024.102254>
15. Vardalachakis, M., Vasilakis, M., & Tampouratzis, M. (2025). A Comprehensive Analysis of Features, Benefits, Challenges, and Best Practices of Security Information and Event Management (SIEM) Solutions. *Computer Sciences & Mathematics Forum*, 12(1), Article 18. <https://doi.org/10.3390/cmsf2025012018>

Авторлар туралы мәлімет:

Кушубек Аслан Рашидулы (автор-корреспондент) – ҚР ҒЖБМ «Ұлттық тестілеу орталығы» ШЖҚ РМК, бас сарапшы, Астана, Қазақстан, e-mail: kushubek.aslan@mail.ru

Шарипбеков Беркин Ерсейтулы – ҚР ҒЖБМ «Ұлттық тестілеу орталығы» ШЖҚ РМК, бөлім басшысы, Астана, Қазақстан, e-mail: b.sharipbekov@testcenter.kz

Рахимов Батырбек Серикович – ҚР ҒЖБМ «Ұлттық тестілеу орталығы» ШЖҚ РМК, директор орынбасары, Астана, Қазақстан, e-mail: rakhimov.batyrbek@mail.ru

Сантеева Сая Әділбайқызы – Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Ақпараттық қауіпсіздік кафедрасының аға оқытушысы, Астана, Қазақстан, e-mail: saya_santeeva@mail.ru

Шайханова Айгуль Кайрулаевна – Л.Н. Гумилев атындағы Еуразия ұлттық университеті, PhD, қауымдастырылған профессор, Ақпараттық қауіпсіздік кафедрасының профессоры, Астана, Қазақстан, e-mail: aigul.shaikhanova@gmail.com

Information about authors:

Kushubek Aslan Rashiduly (corresponding author) – Republican State Enterprise on the Right of Economic Management «National Testing Center» of the Ministry of Science and Higher Education of the Republic of Kazakhstan, Chief expert, Astana, Kazakhstan, e-mail: kushubek.aslan@mail.ru

Sharipbekov Berkin Erseituly – Republican State Enterprise on the Right of Economic Management «National Testing Center» of the Ministry of Science and Higher Education of the Republic of Kazakhstan, Department Head, e-mail: b.sharipbekov@testcenter.kz

Rakhimov Batyrbek Serikovich – Republican State Enterprise on the Right of Economic Management «National Testing Center» of the Ministry of Science and Higher Education of the Republic of Kazakhstan, Deputy Director, e-mail: rakhimov.batyrbek@mail.ru

Santeeva Saya – L.N. Gumilyov Eurasian National University, Senior Lecturer, Department of Information Security, Astana, Republic of Kazakhstan, e-mail: saya_santeeva@mail.ru

Shaikhanova Aigul – L.N. Gumilyov Eurasian National University, PhD, Associate Professor, Professor of the Department of Information Security, Astana, Republic of Kazakhstan, e-mail: aigul.shaikhanova@gmail.com

Сведения об авторах:

Кушубек Аслан Рашидулы (автор-корреспондент) – РГП на ПХВ «Национальный центр тестирования» МНВО РК, главный эксперт, Астана, Казахстан, e-mail: kushubek.aslan@mail.ru

Шарипбеков Беркин Ерсейтулы – РГП на ПХВ «Национальный центр тестирования» МНВО РК, руководитель отдела, Астана, Казахстан e-mail: b.sharipbekov@testcenter.kz

Рахимов Батырбек Серикович – РГП на ПХВ «Национальный центр тестирования» МНВО РК, заместитель директора, Астана, Казахстан, e-mail: rakhimov.batyrbek@mail.ru

Сантеева Сая Әділбайқызы – ЕНУ им. Л. Н. Гумилева, старший преподаватель кафедры информационной безопасности, Астана, Казахстан, e-mail: saya_santeeva@mail.ru

Шайханова Айгуль Кайрулаевна – ЕНУ им. Л. Н. Гумилева, PhD, ассоц. профессор, профессор кафедры информационной безопасности, Астана, Казахстан, e-mail: aigul.shaikhanova@gmail.com