

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

**Студенттер мен жас ғалымдардың
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 2025»**

**PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ҒҮЛЫМ ЖАҢЕ БІЛІМ - 2025»**

**2025
Астана**

УДК 001(06)
ББК 72я631
F96

**«GYLYM JÁNE BILIM – 2025» студенттер мен жас ғалымдардың
XX Халықаралық ғылыми конференциясы = XX Международная
научная конференция студентов и молодых ученых «GYLYM JÁNE
BILIM – 2025» = The XX International Scientific Conference for
students and young scholars «GYLYM JÁNE BILIM – 2025». – Астана:
– 3813 б. - қазақша, орысша, ағылшынша.**

ISBN 978-601-08-5373-7

**Жинаққа студенттердің, магистранттардың, докторанттардың және жас
ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті
мәселелері бойынша баяндамалары енгізілген.**

**The proceedings are the papers of students, undergraduates, doctoral students and young
researchers on topical issues of natural and technical sciences and humanities. В сборник
вошли доклады студентов, магистрантов, докторантов и молодых ученых по
актуальным вопросам естественно-технических и гуманитарных наук.**

УДК 001(06)
ББК 72я431
F96

ISBN 978-601-08-5373-7

Л.Н. Гумилев атындағы Еуразия
ұлттық университеті, 2025

		сауаттылығын арттыру	
203.	Эрболат А.	Орта мектепте нанотехнология ұғымын оқытудың тиімді әдістері	808

СЕКЦИЯ 2

СОВРЕМЕННЫЕ ИНФОРМАЦИОННЫЕ И КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Подсекция 2.1			
Цифровая трансформация образования			
204.	Адалбек Н.	«Традиционные и интеллектуальные подходы в обучении»	812
205.	Бакенова А.А.	«Цифровизация тестирования: разработка нейросетевого приложения для формирования заданий по английской грамматике»	816
206.	Бекмурат А.Е.	«Инновационные методы обучения информатике в школе на основе искусственного интеллекта»	821
207.	Назарова А.Т.	«Развитие цифровых компетенций учителей в условиях персонализированного обучения»	826
208.	Нуриева Д.Р.	«Цифровая трансформация педагогики: роль информационных технологий в повышении квалификации преподавателей»	830
209.	Абдуашимова П.М.	«Білім беру процесінде жасанды интеллект технологияларын қолданудың тиімділігі»	833
210.	Ажибаева А.Д.	«Мектеп информатикасын оқытудағы кемшіліктерді жою жолдары»	837
211.	Асылбек М.А.	«Орта мектепте білім беру үдерісінде үлкен деректерді қолдану әдістемесі»	842
212.	Аталова А.Е.	«Әлеуметтік желілерді информатика пәні бойынша оқыту құралы ретінде пайдалану»	845
213.	Балтабаев Н.П.	«Мектептерде сабақ кестесін автоматтандыруға арналған интеллектуалды жүйе құру»	851
214.	Балтабаев Н.П., Дәрменов Ә.М., Мұратова М.М.	«Жасанды интеллект негізінде жаратылыстану пәндерін оқытуды жетілдіру: BilimALL AI платформасының мүмкіндіктері»	854
215.	Баумуратова Х.Б.	«АКТ оқыту барысында бастауыш сынып оқушыларының цифрлық сауаттылықтарын қалыптастырудың әдістемесі»	856
216.	Баумуратова Ш.Б.	«Жасанды интеллект негізінде инклюзивті білім беруді жетілдіру»	859
217.	Ғазиз Ж.Е.	«Бастауыш мектепте ақпараттық-коммуникациялық технологияларды оқыту әдістемесі»	863
218.	Дәрменов Ә.М.	«Информатиканы қолжетімді ететін мобильді "BilimAll" қосымшасы»	866
219.	Дүйсегалиева Н.А.	«HIGH-TOUCH HIGH-TECH моделі арқылы болашақ информатика мұғалімдерін машиналық оқыту негізінде даярлаудың	870

	инновациялық тәсілдері туралы»	
220.	Еликбай А.Ж. «Ақпараттық дәуірде білім берудің жаңа кезеңі – Инфографика»	874
221.	Жаңабекқызы А. «EDCAFE AI көмегімен сабақты жоспарлау»	879
222.	Жумабекова У.Б., Сабырова М.Е., Сабыров Т.С. «Информатика пәнін жобалап оқыту технологиясы»	883
223.	Кендебай Н.А. «EDUVISION білім беру процесін қадағалайтын қосымша»	888
224.	Көшенова А. «Цифрлық сауаттылықтың мектеп курсы бойынша интеллектуалдық оқу басылымдарына арналған дидактикалық материалдар»	891
225.	Куанышева Д.Ж. «Инклюзивті білім беруде педагогтың ақпараттық-коммуникациялық технологияларды (АКТ) қолдану даярлығын жетілдіру»	893
226.	Мауленова М.А. «Үлкен деректерді өңдеуде машиналық оқытудың әдістері мен құралдары»	897
227.	Мылтыкбаева Ж.Т. «Жаратылыстану пәндерін STEM білім беру мен ROS операциялық жүйесі негізінде кешенді оқыту»	901
228.	Надирхан Г.Е. «Ауыл мектептерінде цифрлық оқытуды дамыту мүмкіндіктері»	903
229.	Орынбаев М.Ж. «Компьютерлік көру алгоритмдерін машиналық оқыту негіздері бойынша қолданудың оқу-әдістемелік негіздері»	907
230.	Сабитова А.Б., Ражапова А.Н. «Жасанды интеллект және білім: болашақ мұғалімдерге арналған жаңа мүмкіндіктер»	910
231.	Сағындықова А.С. «Болашақ информатика мұғалімдерін магистратураға даярлаудағы онлайн-курстардың рөлі»	915
232.	Сайлау Ж.Б. «Халықаралық зерттеуге оқушыларды АКТ арқылы дайындаудағы педагогтердің құзыреттілігін арттыру жолдары»	918
233.	Төрәлі Қ.Н. «Бастауыш сынып оқушыларының цифрлық сауаттылығын дамытудың ерекшеліктері»	923
234.	Турмаганбетова З.П., Алтыбаева А.Н. «Ерекше білімді қажет ететін оқушыларға мектеп информатика курсы оқытуды ұйымдастыру»	927
235.	Халхабай А. ««Алгоритмдеу және бағдарламалау» курсы бойынша мобильді қосымшаны оқу үдерісінде қолдану»	931
236.	Ысмайыл Н. «Мектеп информатика курсына жобалық оқыту әдісін енгізу»	936
237.	Ізбасарова М.Р. «Білім берудегі тестілеу жүйелері»	938

Подсекция 2.2

Интеллектуальные информационные системы

238.	Amantayeva Gulden Turarkyzy «Comparative analysis of models and methods in heart disease prediction problems»	944
------	---	-----

239.	Tanirbergenov Meirbek Sagyndykovich «Facial Recognition-Based Attendance Management»	947
240.	Toleubay Daniyar Manatuly «Cardiac disease prediction using machine learning algoritms»	952
241.	Yerezhepov Rakhat Aibulatovich «Detecting logical fallacies in web content with nlp-powered crawling»	957
242.	Ажикенов Арман Русланович, Абашев Арслан Азатабекович «Оптимизация дорожного трафика в Астане через симуляцию транспортных потоков»	962
243.	Аманжол Альфараби Маликович, Сабит Мадияр, Кушербаев Бекзат Алибекулы «Система визуализации и анализа данных о передвижении нефти на основе интерактивной карты»	968
244.	Аскапова Мадина Куанышбековна «Параллельді қазақ-түрік сөйлеу корпусы қалыптастырудың әдісі мен моделін құру»	972
245.	Бекқожин Дастан Ақанұлы «Терең оқыту негізінде қолжазба таңбаларын тану программалық құралын әзірлеу»	975
246.	Дакенов Алишер Мырзахметұлы «Анализ сигналов ЭЭГ нейросетевыми методами для ранней диагностики нейродегенеративных заболеваний»	978
247.	Доспол Нәзгүл Нурланқызы, Жеткенбай Лена «Балабақшадағы балалардың эмоциялық жағдайын бақылауға арналған эмоцияларды тану жүйесін әзірлеу»	987
248.	Ермекбай Айболат, Молдабек Елжан «Жасанды интеллект негізінде веб-қосымша әзірлеу»	992
249.	Жұмал Жания Ержанқызы, Абдурахман Жансая Берікжанқызы «Применение голосового ИИ-помощника в геймифицированной образовательной среде»	1001
250.	Каримов Руслан Жасинович «Эффективность существующих ИИ-решений в основных направлениях транспортной логистики»	1007
251.	Кубиева Сабина Талгатовна, Утепбергенова Зарина Арманкызы «Разработка iot системы по уходу за растениями на базе искусственного интеллекта»	1012
252.	Кудобаев Даниал Дулатович «Разработка информационной системы для автоматизации стоматологических услуг»	1017
253.	Мусина Данель Тлеухановна «Интеллектуальные инструменты автоматизированной диагностики надежности информационных систем»	1024
254.	Рогова Ксения Александровна, Қабдыбек Ризат Досмжанұлы, Джумадиева Тогжан Бекежановна «Мониторинг инженерных конструкций на основе искусственного интеллекта»	1030

255.	Сафонова Софья Александровна «Современные аспекты информационной безопасности в облачных вычислениях: модели, угрозы и методы защиты»	1034
256.	Смаилова Назгүл Батырбекқызы «Терең оқыту арқылы кітап ұсыныстарын әзірлеу: collaborative filtering, content-based және nlp әдістерінің комбинациясы»	1041
257.	Тажібай Аружан Айдосқызы, Кудубаева Сауле Альжановна «Көру қабілеті әлсіз адамдарға арналған ai дауыстық көмекші: нақты уақытта объектілерді анықтау және қашықтықты бағалау»	1046
258.	Тайжанов Азамат Жанкелдіұлы «Python тілінде фильмдердің интеллектуалды ұсыныс жүйесін әзірлеу»	1051
259.	Умирзахов Сундетали Кабылбекович «Сұраныстарды интеллектуалды талдау негізінде ұйымның сайты үшін чат-бот құру»	1055
260.	Шайхстан Марғұлан «ИОТ Сенсорлары негізінде ауа ластану деңгейін болжау»	1060

Подсекция 2.3

Современные тенденции в программной инженерии и управлении в условиях цифровой индустрии

261.	Bekenova A.B. «Development of a registration panel for users and doctors with integration into the database»	1077
262.	Bolat A.Zh. «Data analysis methods and decision making using big data and machine learning tools»	1081
263.	Алтайұлы А. «Visual studio интегралды ортасында «қойма қызметкерлеріне арналған» мәліметтер қорын жобалау»	1086
264.	Арап А.Қ. «Ақылды сурет салушы роботты әзірлеу»	1088
265.	Артыкбекқызы А. «Ақылды үйлердегі заттар интернеті(iot) мен робототехниканың өзара әрекеттесуі»	1091
266.	Ахметова А.Д. «Тоңазытқыштағы өнімдерді бақылауға және тағам әзірлеу ұсынысын беруге арналған программалық қосымша»	1096
267.	Дәрібай Д.Д. «Робототехниканы қолдану арқылы қойма логистикасындағы қолданыстағы басқару жүйелерін талдау»	1100
268.	Жамбулов С.Ж. «Білім алушыларды информатика және программалау олимпиадаларына дайындауда жасанды интеллекттің қолданысы»	1102
269.	Каиржан Р.С. «Development of system for recognition of emotional states of employees based on computer vision methods on Raspberry Pi»	1108
270.	Кайрекенова Н.Р. «Өнеркәсіптік роботты көру үшін машиналық оқытудың заманауи тәсілдері: әдістер, деректер жиынтығы және оптимизациялау»	1111

271.	Калижан А.К. «Разработка системы биометрической аутентификации с предотвращением deepfake атак»	1113
272.	Касылкасова К.Н. «Программное обеспечение smartmed для обработки медицинских данных и диагностики»	1118
273.	Қабдешев Ә.Е. «Жөтелді талдау негізінде денсаулықты диагностикалаудың интеллектуалды программасын әзірлеу»	1120
274.	Махаев Е.Е. «Разработка облачного приложения для автоматизации деятельности сети аптек»	1123
275.	Муратов М.М. «Эффективность единой информационной системы агропромышленного комплекса»	1126
276.	Нуржанова А.Б. «Современные методы классификации эмоций: анализ подходов и перспективы развития»	1130
277.	Нурпеисова З.Р. «Обзор и исследование методов искусственного интеллекта для анализа рынка недвижимости»	1134
278.	Рақымбек А.С. «Кітапқұмарларға арналған платформа: кітаптарды оқу және бөлісу үшін әлеуметтік желіні жобалау және іске асыру»	1138
279.	Сагидуллина Д.С. «Visual studio интегралды ортасында «қаржылық транзакцияларды қадағалау және талдауға арналған» мәліметтер қорын жобалау»	1144
280.	Төлеубай Д.М. «Yolov10 қолдану арқылы рентген суреттерінде сүйек сынуын анықтауды кешенді зерттеу»	1147
281.	Утегенова Д.Б. «Visual studio интегралды ортасында «фитнес орталық қызметкері үшін» мәліметтер қорын жобалау»	1152
282.	Шаймуратов А.Ж. «Проектирование аппаратно-программного комплекса для автоматизированного учета железнодорожного подвижного состава»	1154
Подсекция 2.4		
Информационная безопасность		
283.	Akniyet N. «Smart home automation and security system using arduino uno r4 and esp32 microcontrollers with telegram integration»	1158
284.	Askhatov A. «Analysis of social engineering methods and development of a defense strategy for corporate structures»	1165
285.	Bekturganov A.B. «Development of an early detection model for ddos attacks based on network traffic analysis»	1170
286.	Gabdullin A. «Analysis of modern wireless network security protocols and prospects for their development»	1174

287.	Garifullin A. «Modern information security management systems: construction and implementation in the digital era»	1179
288.	Igumenshev D.V. «Methods of embedding malicious code into pdf files»	1182
289.	Issabay T.B. «Utilizing sandboxes for cybersecurity training: a hands-on approach»	1187
290.	Kalybayev S. «Overview of modern authentication methods in telecommunication systems: from passwords to biometrics»	1191
291.	Kerim A. «Owasp top 10 and alternative methods of its compilation»	1194
292.	Yergazin A. «Analysis of a protection of hybrid intrusion detection and prevention system (idps) for low-latency 5g networks with adaptive learning using edge computing»	1199
293.	Yerzhanova Y.Y. «Key attacks in web forensics: xss, sql injection and rce»	1204
294.	Zhakay A. «Fundamentals of modern cryptography: from encryption to digital signatures»	1209
295.	Айдарова А.А. «Visualvm көмегімен cast-128 және kuznyechik блоктық шифрларының кілт генерациясын салыстыру және стандарттарға шолу»	1214
296.	Акимбекова Д.М., Каиржанова Д.Ж. «Жергілікті желінің қауіпсіздігін қамтамасыз ететін негізгі параметрлер»	1220
297.	Аскарлов А.Д. «Разработка и исследование эффективности метода и инструмента для выявления фейковых новостей в социальных сетях»	1224
298.	Ауесхан Н. «Аномалияларды анықтау әдістерін талдау»	1229
299.	Ерболатов А. «Анализ вредоносных программ с помощью ии и криптографическая защита»	1332
300.	Ерболатова А.Ж. «Neuvector және kubernetes: контейнерлік ортадағы қауіпсіздікті қамтамасыз ету тәсілдері»	1336
301.	Жанатаев М.К. «Стеганография на основе lsb: реализация сокрытия данных в медиафайлах»	1338
302.	Жарасхан Н.Ж., Қайупов Е.К. «Crystals-kyber алгоритмін ресурсы шектеулі құрылғыларға оңтайландыру»	1343
303.	Жолдасбаев М.Ә. «Заманауи операциялық жүйелердегі жады дампы кескінін алу құралдарын талдау және салыстыру»	1348
304.	Жолмұратұлы Б., Маратов Ә.Б., Ховдабай Н.А. «Екі факторлы	1353

	аутентификацияның қауіпсіздігі және оның қолданылуы»	
305.	Кадринов Д.М. «Автоматизация внедрения альтернативной soag платформы на основе средств со свободной лицензией»	1357
306.	Казбаганбетова М.А. «Wireshark бағдарламасын пайдаланып желілік трафикті талдау және ақпараттық қауіпсіздікті қамтамасыз ету»	1361
307.	Кәкімбек Ә.Қ., Серікбай А.Е., Наурызбаев Д.Е. «MITM шабуылы туралы»	1366
308.	Кеттеш Б.Н. «ELF талдауындағы capstone: сызықтық және рекурсивті дизассемблерлеу»	1370
309.	Көшкінбаева Ф.Қ. «Linux қорғаудың заманауи әдістеріне талдау.openvas және nmap көмегімен осалдықтарды анықтау»	1374
310.	Қадыр Н.Е. «Заманауи фишинг түрлері мен олардың ұйымдық ақпараттық жүйелерге ықпалы»	1379
311.	Қажкен Е.Е., Темиржан С.А. «Қауіпсіздік инциденттеріне қалай жауап беруге болады?»	1384
312.	Қартбай Е.Ғ., Тынарбай Н.И. «MITM шабуылы (адамның ортадағы шабуылы)»	1388
313.	Маратов Б.Ж. «Әлеуметтік инженерия қауіпсіздікке қатер ретінде: қызметкерлерді қорғау және оқыту әдістері»	1393
314.	Мағзумов А.М. «Websocket протоколындағы осалдықтарды талдау»	1397
315.	Майданов А.С. «Автоматизация процесса анализа оперативной памяти с использованием python»	1401
316.	Мақсат Ә., Нурсейтов С. «Блокчейн қажеттілік пе, әлде сән бе?»	1406
317.	Қ. Мырзағалиұлы. «Инциденттерді анықтауда желілік логтарды талдаудың маңызды рөлдері»	1409
318.	Нурбатуров С.К. «Интеграция honeypot в ит-инфраструктуру компании»	1412
319.	Нуриева Д.Р., Исайнова А.Н. «Анализ рисками безопасности данных в медицинских учреждениях»	1415
320.	Нұрлан А.Т. «Кескіндердегі статистикалық стегоанализ әдістері»	1420
321.	Оралбеков Е.А. «Ddos-шабуылдардың жаңа буыны»	1424

322.	Рамазанова Ж, Нұрлан А, Жайсанбаева А. «Бұлтты технологияларды пайдалану кезіндегі тәуекелдер мен қауіпсіздік шараларын зерттеу»	1430
323.	Сахатбекқызы Т., Бахтиярқызы Т.А. «IoT құрылғыларының желідегі қауіпсіздігін қалай қамтамасыз етуге болады: стратегиялар және packet tracer көмегімен модельдеу»	1434
324.	Серғазы М. «Повышение производительности разработчиков с помощью интегрированных искусственных интеллектов и соображения кибербезопасности»	1440
325.	Султанов А.М. «Стеганография в кибербезопасности казахстана»	1443
326.	Танатаров Е., Іргебай С., Султанов А. «WI-FI желісінде шақырылмаған қонақтарды автоматты түрде анықтау жүйесі»	1447
327.	Таубай М.Е. Рамагуллаев Ә.А. «Фишинг: желідегі beef әдісі арқылы алдау және одан сақтану»	1452

СЕКЦИЯ 3 ЕСТЕСТВЕННЫЕ НАУКИ

		ПОДСЕКЦИЯ 3.1 АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВРЕМЕННОЙ БИОЛОГИИ	
328.	Акимкара А.Б.	Гербарийдің ботаникалық зерттеулерде қолданылуы және гербарий қорындағы кеппе шөптің қалыптасу ерекшеліктері	1457
329.	Ақылбек А.	Астана қаласындағы ботаникалық бағының ландшафттағы <i>geranium sanguineum</i> биологиялық ерекшеліктеріне сипаттама беру	1459
330.	Әділхан Ж.	Мобильді байланыс пен қолданбалардың адамның мінез-құлқына әсерін анықтау	1463
331.	Базарбаева Қ.	Жасөспірімдерде девиантты мінез-құлықтың даму қаупі	1467
332.	Байдосова А.Б.	Методика использования игровых технологий на уроках биологии	1471
333.	Байдосова А.Б.	Актуальные проблемы современной биологии с использованием игровых технологий в образовании	1474
334.	Ғазизова Ә.	Сәулеленген егеуқұйрықтардың бүйректеріндегі морфофункционалдық өзгерістерді салыстырмалы бағалау	1477
335.	Еркін З.Б.	Биология сабақтарында оқушылардың сыни ойлау қабілетін жетілдіруде блум таксономиясын пайдалану	1482
336.	Жанабергенова	Кенеттен жүрек өлімі: генетикалық аспектілері	1486

ӘОЖ 81.93.29

ИНЦИДЕНТТЕРДІ АНЫҚТАУДА ЖЕЛІЛІК ЛОГТАРДЫ ТАЛДАУДЫҢ МАҢЫЗДЫ РӨЛДЕРІ

Қ. Мырзағалиұлы

7M06306 “Ақпараттық қауіпсіздік жүйелері” мамандығы бойынша магистрант, Л.Н. Гумилев атындағы ЕҰУ, Астана қ.

К.М.Сагиндыков

Ғылыми жетекшісі, т.ғ.к., доцент, Л.Н. Гумилев атындағы ЕҰУ, Астана қ.

Мақалада киберқауіпсіздік құралы ретінде желілік логтардың маңызы қарастырылады. Олардың мүмкіндіктері кибершабуыл іздерін анықтауда, трафикті талдауда және SIEM жүйелері мен корреляция әдістерін қолдану арқылы аномалияларды анықтауда қарастырылады. Жасанды интеллектті қоса алғанда, заманауи технологиялар арқылы қолданудың практикалық аспектілеріне, шектеулерге және тиімділікті арттыру жолдарына ерекше назар аударылады. Талдау негізінде өсіп келе жатқан қауіптер жағдайында цифрлық жүйелерді қорғау үшін желілік логтарды оңтайландыру бойынша ұсыныстар ұсынылады.

Түйін сөздер: желілік логтар, логтар корреляциясы, SIEM жүйесі, трафик, аномалия.

Цифрлық трансформация киберқауіпсіздік ландшафтын өзгертті, бұл желілерді негізгі шабуыл нысанына айналдырды. 2024 жылғы Verizon Data Breach Investigations Report мәліметтері бойынша, оқиғалардың 82% - ы желілік осалдықтарға байланысты, ал киберқылмыстың жаһандық шығыны жыл сайын 6 трлн доллардан асады (Morgan, 2024). Түйіндер арасындағы өзара әрекеттесуді тіркейтін желілік логтар қауіптерді бақылау, анықтау және тергеудің маңызды құралына айналды. Олар нақты уақыттағы талдау және оқиғаларды ретроспективті қалпына келтіру үшін деректерді ұсынады, бұл оларды кибершабуылдармен күресуде таптырмас етеді. Мақаланың мақсаты-желілік логтардың мүмкіндіктерін жан-жақты бағалау, оларды талдау әдістерін зерттеу, шектеулерді анықтау және технологиялар мен қауіптердің эволюциясы жағдайында олардың даму жолдарын ұсыну.

Желілік логтар – бұл желілік құрылғылар (маршрутизаторлар, брандмауэрлер, IDS/IPS) және трафик параметрлерін бекітетін бағдарламалық жасақтама: IP мекенжайлары, порттар, протоколдар, деректер көлемі және уақыт белгілері. Олар ішкі және сыртқы әрекеттерді бақылауға мүмкіндік беретін желілік байланыстарды қамту арқылы жүйелік ұялардан ерекшеленеді. Журналдар құрылымдалған болуы мүмкін (мысалы, JSON форматында) немесе құрылымдалмаған (мәтіндік файлдар), бұл олардың өңделуіне әсер етеді.

Splunk, QRadar немесе ArcSight сияқты SIEM жүйелерінде желілік логтар оқиғаларды корреляциялау және шабуылдар тізбегін құру үшін қолданылады. Олардың теориялық маңыздылығы белсенділіктің "сандық іздерін" қамтамасыз етуде жатыр, бірақ практикалық құндылығы жинау, сақтау және талдау сапасымен анықталады. Мысалы, syslog стандарты біртұтастықты қамтамасыз етеді, бірақ әрдайым күрделі тергеу үшін жеткілікті мәліметтерді қамтымайды.

Желілік логтар қауіптердің кең ауқымын анықтауда тиімді. DDoS шабуылдарында олар трафиктің аномалиясын түсіреді, бұл зиян көздерін бұғаттауға мүмкіндік береді. Фишинг жағдайында DNS сұрауларының журналдары зиянды домендерге жүгінуді, ал деректер бұзылған кезде — шығатын трафиктің күдікті көлемін анықтайды. Олар сондай-ақ заңды хаттамалар арқылы деректерді туннельдеу сияқты жасырын қауіптерді талдауға көмектеседі.

Нақты мысалдар олардың маңыздылығын көрсетеді. 2020 жылғы SolarWinds шабуылды логтар арқылы командалық серверлермен шифрланған қосылыстарды анықтады, бұл оқиғаға деген реакцияны тездетті. 2017 жылғы WannaCry SMB-ді брандмауэр логтарында пайдалану әрекеттерін көрсетті, ал 2021 жылы Colonial Pipeline-ге шабуыл деректерді шифрлау алдында логтар арқылы желіні алдын ала сканерлеуді анықтады. Cobalt Strike APT тобы жағдайында логтар сирек порттардың қолданылуын тіркеді, бұл мақсатты шабуылды көрсетті.

Желілік логтар цифрлық криминалистика талдауы үшін де маңызды. Оқиғадан кейін олар хронологияны қалпына келтіруге мүмкіндік береді: кіру нүктесінен (мысалы, фишингтік хат) зиянды кодты орындауға және деректерді сүзуге дейінгі аралық. Бұл оларды зиянды бағалауға және алдын-алу шараларын жасауға негіз етеді.

Желілік логтарды өңдеу олардың көлемі мен күрделілігіне байланысты заманауи тәсілдерді қажет етеді. Дәстүрлі қолмен талдау, автоматтандыруға жол берді. SVM (Support Vector Machines) және нейрондық желілер сияқты машиналық оқыту алгоритмдері ауытқуларды 92% дәлдікпен анықтайды (Lee et al., 2022). Мысалы, кластерлеу тән емес трафик үлгілерін бөліп көрсетуі мүмкін, ал регрессиялық талдау белсенділіктің өсуін болжауы мүмкін.

Корреляциялық талдау толық суретті құру үшін әртүрлі көздерден алынған журналдарды біріктіреді. Мысалы, ICMP сұрауларымен бірге сәтсіз аутентификация желіні барлауды көрсетуі мүмкін. Elasticsearch немесе Apache Kafka сияқты платформалар терабайт деректерін нақты уақытта өңдеуге мүмкіндік беретін масштабталуды қамтамасыз етеді. Бейнелеу (графиктер, жылу карталары) талдаушыларға нәтижелерді түсіндіруге көмектеседі, бірақ құрылымдалмаған журналдарды алдын-ала қалыпқа келтіруді қажет етеді.

Дәлдікті арттыру үшін гибриді әдістер қолданылады. Мысалы, қолтаңбаны талдау (белгілі қауіптерді іздеу) және мінез-құлық (ауытқуларды анықтау) тіркесімі белгілі және нөлдік күндік шабуылдарды анықтауға мүмкіндік береді. Дегенмен, модельдерді теңшеу үлкен көлемдегі деректер мен есептеу ресурстарын қажет етеді.

Желілік логтарда айтарлықтай шектеулер бар. Сапалығы құрылғылардың конфигурациясына байланысты — негізгі оқиғаларды жазбау олардың құндылығын төмендетеді. Трафикті шифрлау (HTTPS, TLS, VPN) хабар мазмұнын жасырады, бұл құпиялық мәселелерін тудыратын SSL инспекциясы сияқты құралдарды қажет етеді. Деректердің көлемі тағы бір проблема болып табылады: ірі желілер сақтау жүйелерін шамадан тыс жүктейтін күніне 10 ТБ лог шығарады (IBM Security, 2023).

Журналдар көбінесе контекстен айырылады. Мысалы, IP мекенжайына қосылу оның мақсатын түсіндірмейді, бұл жүйелік логтармен немесе threat intelligence деректерімен біріктіруді қажет етеді. Жалған позитивтер логтарды талдауды қиындатады — заңды трафикті қате түрде қауіп ретінде жіктеуге болады, әсіресе кибер-дүйсенбі сияқты ең жоғары белсенділік кезеңдерінде. Қосымша шектеу — бұл логтардың осалдығы. Шабуылдаушылар 2017 жылы Equifax-қа жасалған шабуылдағыдай жазбаларды жоя алады немесе бұрмалай алады, онда логтар ішінара жойылып, тергеуді қиындатады.

Зерттеулер осы шектеулерді жеңуге бағытталған. Lee et al. (2022) 95% дәлдікке жететін журналдарды талдау үшін терең оқыту моделін жасады. Kumar et al. (2023) 85% ықтималдықпен шабуылдарды болжайтын болжамды тәсілді ұсынды. Chen, L., et al. (2023) шифрды шешпестен қауіптерді анықтау үшін метадеректерді қолдана отырып, шифрланған трафикті өңдеуге бағытталған.

Коммерциялық секторда Palo Alto Networks журналдарды Cortex XDR-де мінез-құлық талдауымен біріктіреді, ал Cisco журналдарды қауіп деректерімен байыту шешімдерін әзірлейді. NIST (2023) интеграцияны жеңілдететін JSON-LD сияқты стандарттарды алға тартады. Зерттеулер сонымен қатар сот-медициналық тексерулерге қатысты логтарды жалған заттардан қорғау үшін блокчейнді қолдануды зерттейді.

Желілік логтарды талдауды енгізу салалар бойынша әр түрлі. Қаржы секторында (банктер, финтех) GDPR немесе PCI DSS сияқты реттеуші талаптарға байланысты жоғары өңдеу жылдамдығы қажет. Мысалы, JPMorgan Chase жауап беру уақытын 8 сағатқа дейін қысқартып, нақты уақыттағы логтарды талдау үшін QRadar пайдаланады (Gartner, 2023). Пациенттердің деректері HIPAA арқылы қорғалған денсаулық сақтауда логтарды шифрлауға және оларды ұзақ мерзімді сақтауға баса назар аударылады.

Шағын компаниялар көбінесе AWS CloudTrail сияқты бұлтты шешімдерді арзан шығындарға байланысты тандайды, ал ірі корпорациялар бақылау үшін жергілікті жүйелерді қалайды. SIEM енгізу құны шағын бизнес үшін 1 100 мыңнан ірі ұйымдар үшін 1.1 млн-ға дейін ауытқиды, жыл сайынғы қолдау шығындары осы соманың шамамен 15% құрайды (IBM Security, 2023). Қызметкерлерді оқыту негізгі фактор болып табылады: талдаушылар ережелерді орнату және деректерді түсіндіру дағдыларын меңгеруі керек.

Target case (2013) оқиғадан кейін логты талдауды жаңарту анықтау уақытын 72-ден 10 сағатқа дейін қалай қысқартқанын көрсетеді. Сонымен қатар, Uber-ге шабуыл (2016) кемшіліктерді анықтады: журнал мониторингінің болмауы шабуылдаушыларға бір жылға дейін деректердің бұзылуын жасыруға мүмкіндік берді.

Трафиктің көлемі үлкен телекоммуникацияда логтарды қысуға және таңдамалы талдауға баса назар аударылады. Verizon ауытқуларға назар аудара отырып, күніне 50 ТБ журналдарды өңдеу үшін Kafka-ны пайдаланады. Бөлшек саудада (мысалы, Walmart) басымдық транзакцияларды қорғау болып табылады, бұл логтардың POS жүйелерінің деректерімен корреляциясын қажет етеді. Мемлекеттік секторда (мысалы, DARPA) журналдар АРТ-мен күресу үшін threat hunting жүйелерімен біріктірілген.

Желілік ұялардың болашағы келесі буын технологиясымен байланысты. Жасанды интеллект тарихи деректерді талдау арқылы Darktrace сияқты қауіптерді болжайды. Кванттық есептеу өңдеуді жылдамдатады, бұл 5G және IoT үшін маңызды. STIX сияқты стандарттар ұйымдар арасында деректер алмасуды жеңілдетеді, ал блокчейн олардың тұтастығын қамтамасыз етеді.

Zero Trust тұжырымдамасы әрбір қосылымды тексеру құралы ретінде логтардың рөлін арттырады. Edge computing-ті дамыту IoT құрылғыларында орталықтандырылмаған логтарды жинауды қажет етеді, бұл оларды талдау үшін жаңа қиындықтар тудырады. Ақырында, AI негізіндегі автоматтандыру жылдамдық пен дәлдікті арттыру арқылы адам факторына тәуелділікті азайтады.

Қорытынды және ұсыныстар

Менің ойымша, желілік журналдар сандық жүйелерді киберқауіптерден қорғауға көмектесетін маңызды құрал болып табылады және мен өз жұмысымда олардың құндылығын көрсетуге тырыстым. Олар маған трафикті бақылауға, ауытқуларды табуға және оқиғалардың қалай болатынын түсінуге мүмкіндік береді, бұл шабуылдармен күресте шынымен құтқарады. Бірақ қиындықтардың бар екенінде айта өткен жөн — үлкен көлемдегі деректер, шифрлау және бәрін дұрыс орнату қажеттілігі. Біз SIEM жүйелері мен логтардың корреляциясын қолданудың, сондай — ақ жасанды интеллектті қосудың пайдасын көре аламыз — бұл талдауды дәлірек және жылдамырақ етеді. Менің мақаламда көрсетілгендей, егер сіз процестерді автоматтандырып, өз мамандарыңызды оқытсаңыз, желілік логтар көп пайда әкеледі. Мен олар одан әрі қажет болатынына сенімдімін, әсіресе егер олар жаңа технологиялар мен нақты міндеттерді ескере

отырып жасалса. Бұл жұмыс маған киберқауіпсіздікті қалай жақсартуға болатынын түсінуге көмектесті және менің қорытындыларым басқаларға пайдалы болады деп үміттенемін.

Ұсыныстар:

1. *Трафикті талдауды автоматтандыру.* Желілік логтардың үлкен көлемін өңдеу үшін Splunk немесе QRadar сияқты SIEM жүйелерін енгізіп, жасанды интеллектке негізделген аномалияны анықтау алгоритмдерін қосқан жөн. Бұл қауіптерді анықтауды тездетеді және талдаушыларға жүктемені азайтады.

2. *Логтар корреляциясын орнату.* Мен әртүрлі көздерден оқиғаларды байланыстыру үшін корреляция ережелерін орнатуды ұсынамын – мысалы, брандмауэр журналдары, серверлер және DNS. Бұл оқиғалардың толық бейнесін құруға және олардың себептерін тезірек табуға көмектеседі.

3. *Деректерді жинау сапасын жақсарту.* Журналдар трафиктің барлық негізгі параметрлерін — IP мекенжайларын, порттарды, уақыт белгілерін қамтуы үшін желілік құрылғыларды мұқият конфигурациялау қажет. Деректерді өткізіп жіберу олардың пайдасын азайтады, сондықтан мен конфигурацияларды үнемі тексеріп отыруға кеңес беремін.

4. *Мамандарды оқыту.* Мен қызметкерлерді желілік логтармен және SIEM жүйелерімен жұмыс істеуге үйрету маңызды деп санаймын. Аномалияларды қалай іздеу керектігін түсіну және нәтижелерді түсіндіру қауіп-қатерге жауап беру жылдамдығын арттырады.

Қолданылған әдебиеттер тізімі

1 Иванов А.В. Сетевые логи как инструмент обнаружения киберугроз: СибФУ //Красноярский университет. – 2022. – № 1. – С. 15–30. https://elib.sfu-kras.ru/bitstream/handle/2311/145678/ivanov_network_logs.pdf?sequence=1

2 Петров С.М. Корреляция логов в системах SIEM для анализа сетевого трафика. – 2023. https://earchive.tpu.ru/bitstream/11683/78945/1/TPU1489765_petrov.pdf

3 Сидоров Д.И., Козлов Р.А. Применение систем SIEM для обработки сетевых логов и выявления аномалий. – М.: ФГУП «Изд-во «Информатика и безопасность» МГУ им. М.В. Ломоносова, 2021. – 480 с.

4 Михайлов Е.А., Степанов П.В. Анализ трафика и обнаружение аномалий с использованием сетевых логов //Журнал кибербезопасности. – 2020. – № 2. – С. 35–50. <https://elibrary.ru/item.asp?id=42837412>

5 Коваленко О.Н. Методы корреляции логов для повышения эффективности систем SIEM //Труды СПИИРАН. – 2023. – № 5. – С. 62–78. https://spii.ras.ru/proceedings/2023/kovalenko_siem_logs.pdf

6 Lee J., Chen L. Deep Learning for Anomaly Detection in Network Logs //Journal of Cybersecurity. – 2022. – № 8(3). – С. 45–60. https://cyberjournal.org/2022/lee_chen_anomaly_detection.pdf

УДК 004.056

ИНТЕГРАЦИЯ HONEYROT В ИТ-ИНФРАСТРУКТУРУ КОМПАНИИ

Нурбатуrow Сырым Канатұлы
mr.nurbaturov1@gmail.com

Магистрант кафедры Информационной безопасности, Астана, Казахстан
Научный руководитель – Сантеева Сая Әділбайқызы, PhD, старший преподаватель