

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

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

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

**PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«ҒЫЛЫМ 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 «IoT 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. Раматуллаев 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

- **SMS-тен бөлек аутентификация әдістерін қосу** (мысалы, Email арқылы растау немесе аутентификатор қолданбаларын пайдалану).
- **UI/UX жақсарту**, пайдаланушылар үшін 2FA процесін жеңілдету.
- **Қауіпсіздікті одан әрі күшейту**, мысалы, логин әрекеттерін бақылау және күдікті әрекеттерді анықтау алгоритмдерін енгізу.

Жоғарыда айтылғандарды талдай отырып, екі факторлы аутентификацияны қолдану қажет деген қорытынды жасауға болады. Дегенмен, қолданылатын факторлар әртүрлі болуы керек екенін ескеру қажет, яғни сенімділік үшін әртүрлі растау әдістерін қолдану қажет. Біздің жағдайда сәйкестендіру тек SMS-код арқылы жүзеге асырылады, ол жүйенің қауіпсіздік деңгейіне белгілі бір шектеулер қояды.

SMS аутентификациясы жеке басын растау үшін ыңғайлы, бірақ ол хабарламаларды ұстау, фишингтік шабуылдар және SIM картасын ауыстыру сияқты бірқатар қауіптерге сезімтал. Мұндай тәуекелдерді азайту үшін кодты енгізу әрекеттерінің санын шектеуді, оның жарамдылық мерзімін қысқартуды және күдікті кіру әрекеттерін талдауды қоса алғанда, қосымша қауіпсіздік шараларын қолдану ұсынылады.

Кейбір осалдықтарға қарамастан, SMS аутентификациясы қарапайымдылығы мен қолжетімділігіне байланысты сәйкестендіруді тексерудің танымал және кеңінен қолданылатын әдісі болып қала береді. Дегенмен, қауіпсіздік деңгейін арттыру үшін биометриялық сәйкестендіру немесе аппараттық кілттер сияқты балама әдістерді енгізу мүмкіндігін қарастырған жөн.

Қолданылған әдебиеттер тізімі

1. Ruiz-Martínez, A., Sánchez-Martínez, D., Martínez-Montesinos, M., & F. Gómez-Skarmeta, A. (2007). A Survey of Electronic Signature Solutions in Mobile Devices. *Journal of Theoretical and Applied Electronic Commerce Research*, 2(3), 94–109. MDPI AG ”
2. Albeshier AS. Reviewing the Usability of Web Authentication Procedures: Comparing the Current Procedures of 20 Websites. *Sustainability*. 2023; 15(14):11043.
3. Risk Analysis Research on SMS Verification Code and Biometric Recognition Technology (Likun Yu (2024))
4. Django/Flask ресми құжаттамалары. (<https://flask.palletsprojects.com/en/stable/>)
5. Mobizon.kz API құжаттамасы. (<https://mobizon.kz/help/api-docs>)

УДК 004

АВТОМАТИЗАЦИЯ ВНЕДРЕНИЯ АЛЬТЕРНАТИВНОЙ SOAR ПЛАТФОРМЫ НА ОСНОВЕ СРЕДСТВ СО СВОБОДНОЙ ЛИЦЕНЗИЕЙ

Кадринов Даулет Маулетович

kadrinov23@mail.ru

Магистрант второго курса кафедры информационной безопасности, ену им. Л. Н. Гумилева,
Астана, Казахстан

научный руководитель – Оспанова А. Б.

Введение

Рост числа кибератак делает автоматизацию реагирования критически важной, но существующие SOAR-решения остаются дорогими и сложными для малого и среднего бизнеса. Угрозы затрагивают не только IT-сектор, но и другие сферы, включая госструктуры

и образование. Цель работы — разработка доступной SOAR-платформы с автоматическим развертыванием, что упростит её интеграцию и снизит затраты на внедрение.

Методы и технологии

Для эффективного управления инцидентами используется Elastic Stack (Elasticsearch, Logstash, Kibana) для сбора и анализа логов, выявления угроз и передачи алертов в TheHive. IRP-платформа TheHive автоматически создаёт кейсы, а Cortex анализирует артефакты (IP, хэши, URL). Python-скрипты обеспечивают автоматизацию реагирования: связывают сервисы, выполняют плейбуки, блокируют IP, изолируют хост и отправляют уведомления в Telegram. Система контейнеризована в Docker, а Docker Swarm управляет балансировкой. Развёртывание автоматизировано с помощью Terraform (создание VM) и Ansible (настройка сервисов). Такой подход обеспечивает масштабируемость, гибкость и доступность, делая платформу эффективной альтернативой коммерческим решениям.

Схема на рисунке 1 представляет работу альтернативной SOAR-платформы, объединяющей SIEM, IRP и автоматизированное реагирование на инциденты. Весь процесс начинается с того, что компьютеры и другие системы отправляют логи в SIEM, где Logstash нормализует данные и передает их в Elasticsearch для хранения и анализа, а Kibana используется для визуализации. Если в логах выявляется подозрительная активность, система генерирует алерты, которые затем поступают в специальные скрипты. Эти скрипты анализируют входящие события и передают обработанные алерты в IRP-систему TheHive, где создаются кейсы для расследования инцидентов. Если угроза подтверждается, система автоматически инициирует реагирование, выполняя блокировку IP-адресов атакующего или изоляцию скомпрометированного хоста. По результатам предпринимаемых действий формируется отчет, а для оперативного информирования администратора запускаются скрипты, которые отправляют уведомления, например, в Telegram. Вся эта архитектура обеспечивает автоматическое выявление, обработку и нейтрализацию угроз, минимизируя ручной труд и сокращая время реагирования на инциденты.

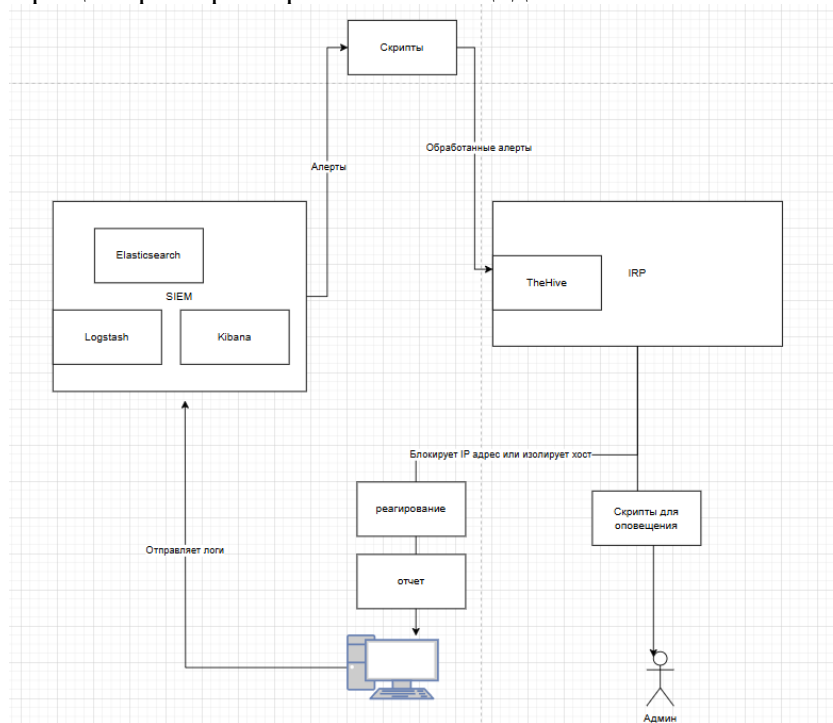


Рисунок 1. Схема инфраструктуры SOAR

Так же есть определенные шаблоны с помощью которых идет обработка инцидентов. Рисунок 2 отражает процесс реагирования на инцидент, связанный с Malware Alert из SIEM.

1. Malware Alert поступает в SIEM, анализируется факт запуска PowerShell или CMD.
 - Если запуск был, проверяется наличие исполняемых файлов с расширениями .exe, .bat, .dll.
 - Если файлы найдены, выполняется удаление вируса.
 - Если файлы не найдены, хост изолируется для предотвращения распространения угрозы.
2. Если запуска PowerShell/CMD не было, проверяется, был ли файл скачан из браузера.
 - Если да, анализируется загруженный файл. Если он вредоносный — выполняется удаление вируса.
 - Если файл не найден, хост изолируется как потенциально скомпрометированный.

Схема помогает быстро классифицировать угрозу и принять решение о дальнейших действиях.

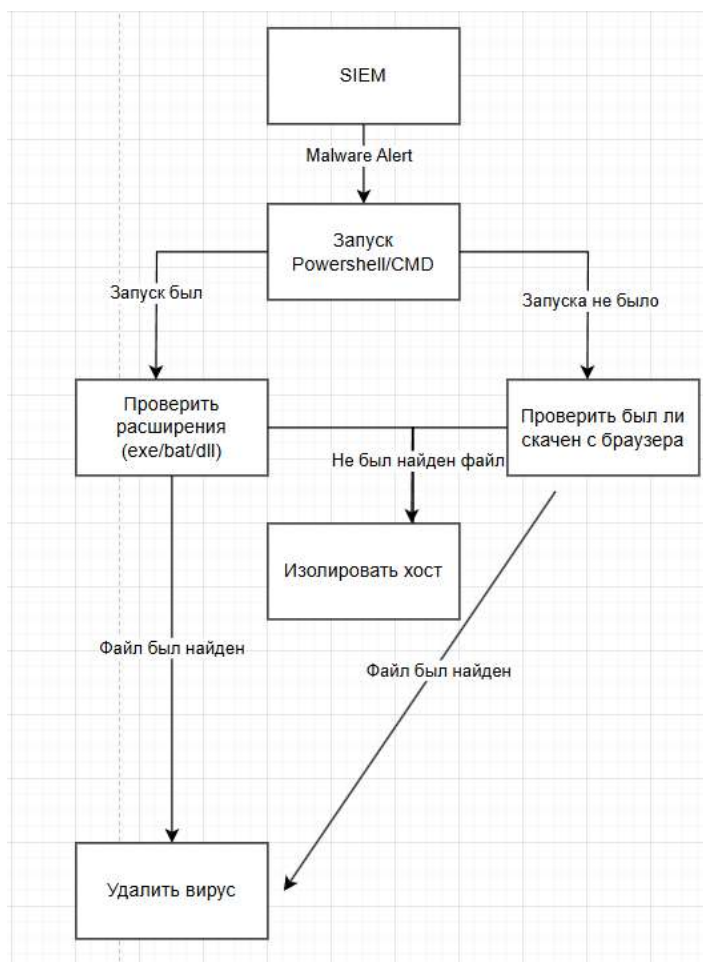


Рисунок 2. Схема работы автоматического реагирования

Код на рисунке 3 реализует автоматизированную обработку инцидентов, соответствующую ранее представленной схеме реагирования.

1. Проверка запуска PowerShell/CMD

- Запрос в Elasticsearch анализирует логи, выявляя запуск powershell.exe или cmd.exe.

- Соответствует этапу "Запуск PowerShell/CMD" в схеме.
- 2. **Проверка подозрительных расширений**
 - Анализируются файлы с расширениями .exe, .bat, .dll.
 - Отражает этап "Проверить расширения (exe/bat/dll)".
 - Если найден подозрительный файл, возможна его изоляция или удаление.

```

from elasticsearch import Elasticsearch
import requests

# Конфигурация
ELASTIC_HOST =
ELASTIC_INDEX = "logs*" # Индекс логов
TELEGRAM_BOT_TOKEN =
TELEGRAM_CHAT_ID =

# Подключение к Elasticsearch
es = Elasticsearch([ELASTIC_HOST])

def search_logs(query):
    """Поиск логов в Elasticsearch."""
    response = es.search(index=ELASTIC_INDEX, body=query, size=10)
    return response.get("hits", {}).get("hits", [])

def check_powershell_cmd():
    """Проверка запуска PowerShell/CMD."""
    query = {
        "query": {
            "bool": {
                "should": [
                    {"match": {"process.name": "powershell.exe"}},
                    {"match": {"process.name": "cmd.exe"}}
                ]
            }
        }
    }
    return search_logs(query)

def check_file_extension():
    """Проверка наличия подозрительных расширений файлов."""
    query = {
        "query": {
            "bool": {
                "should": [
                    {"match": {"file.extension": "exe"}},
                    {"match": {"file.extension": "bat"}},
                    {"match": {"file.extension": "dll"}}
                ]
            }
        }
    }
    return search_logs(query)

```

Рисунок 3. Скрипт

Разработанная SOAR-платформа превосходит коммерческие аналоги FortiSOAR, R-Vision и Splunk SOAR по ключевым параметрам которые отражены в таблице 1. Разработанная платформа быстрее, дешевле и гибче существующих решений, делая её оптимальным выбором. Таблица была основана на официальных данных от документаций продуктов

Таблица 1

Критерий	Проект SOAR	FortiSOAR	R-Vision	Splunk SOAR
Лицензия	Полностью открытая, без ограничений	Закрытая, привязка к Fortinet	Закрытая, привязка к экосистеме R-Vision	Закрытая, требует лицензии Splunk

Стоимость	Бесплатно, платишь только за ресурсы на которых будет работать	Дорого, подписка и поддержка	Дорого, скрытые платежи	Очень дорого, цена зависит от логов
Гибкость интеграций	Полностью кастомизируемая, любые API и сервисы	Ограничена продуктами Fortinet	Ограничена только R-Vision	Хорошая, но сложная в настройке
Развертывание	Автоматическое (Terraform + Ansible), готово за минуты	Долгая ручная настройка	Долгая настройка, нужны инженеры	Сложное, требует специалистов Splunk
Автоматизация	Полная, любые скрипты на Python	Ограниченная, только через Fortinet	Ограниченная, кастомизация сложная	Есть, но требует дорогостоящих специалистов

Заключение

Разработанная SOAR-платформа на основе open-source решений обеспечивает эффективное управление инцидентами, автоматизацию реагирования и интеграцию с SIEM. Благодаря контейнеризации и автоматизированному развертыванию система легко масштабируется и адаптируется под нужды организации, предлагая доступную альтернативу коммерческим продуктам.

Список использованных источников

1. Elastic. Deployment guide. – URL: <https://www.elastic.co/guide/en/enterprise-search/current/deployment.html> (дата обращения: 23.03.2025).
2. R-Vision. SOAR — Автоматизация реагирования на инциденты. – URL: <https://rvision.ru/products/soar> (дата обращения: 23.03.2025).
3. Splunk. Splunk Security Orchestration and Automation (SOAR). – URL: https://www.splunk.com/en_us/products/splunk-security-orchestration-and-automation.html (дата обращения: 23.03.2025).
4. Fortinet. FortiSOAR. – URL: <https://www.fortinet.com/products/fortisoar> (дата обращения: 23.03.2025).

УДК 004

WIRESHARK БАҒДАРЛАМАСЫН ПАЙДАЛАНЫП ЖЕЛЛІК ТРАФИКТІ ТАЛДАУ ЖӘНЕ АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ.

Казбаганбетова Мейрагуль Асылхановна

mira_85k@mail.ru

Қ.Жұбанов атындағы Ақтөбе өңірлік университеті, магистрант, Ақтөбе, Қазақстан
Ғылыми жетекшісі-Г.А.Шангытбаева

Аннотация. Қазіргі ақпараттық технологиялар дәуірінде желілік қауіпсіздік маңызды орын алады. Кибершабуылдар мен зиянды бағдарламалардан қорғану үшін желілік трафикті