

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

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

**Студенттер мен жас ғалымдардың
«GYLYM JÁNE BILIM - 2025»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ
XX Международной научной конференции
студентов и молодых ученых
«GYLYM JÁNE BILIM - 2025»**

**PROCEEDINGS
of the XX International Scientific Conference
for students and young scholars
«GYLYM JÁNE BILIM - 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. «Neuvecton 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

Ranking Factors	Exploitability, Prevalence, Impact	Frequency of occurrence, CVSS severity score
Update Frequency	Every 3 - 4 years	Annually
Latest Edition	2021 (Next update in 2025)	2024

Conclusion. Our article analyzed the Methodology of OWASP Top 10 and compared it to CWE Top 25. Their key differences were in data collection, where if OWASP Top 10 approached hybrid manner of statistical data and industry survey, CWE Top 25 purely relied on statistical data that was provided in NVD, CVE, and etc. Also another difference in methodology was in ranking factors, where OWASP Top 10 uses their own Risk Ranking Methodology that contains exploitability, prevalence, and impact, and CWE Top 25 uses frequency of occurrence, CVSS severity score.

Literature

1. Indusface. Understanding the OWASP Top 10 risk score [Electronic resource]. – Indusface, 2024. – URL: <https://www.indusface.com/learning/owasp-top-10-risk-score/>
2. OWASP Foundation. OWASP Risk Rating Methodology [Electronic resource]. – URL: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology
3. OWASP Foundation. OWASP Top 10:2021[Electronic resource]. – URL: <https://owasp.org/Top10/>
4. CWE. 2024 CWE Top 25 most dangerous software weaknesses [Electronic resource]. – URL: https://cwe.mitre.org/top25/archive/2024/2024_methodology.html
5. CWE. CWE Top 25 most dangerous software weaknesses [Electronic resource]. – URL: <https://cwe.mitre.org/top25/>
6. OWASP Foundation. The data [Electronic resource]. – URL: <https://www.owasptopen.org/thedata>

ANALYSIS OF A PROTECTION OF HYBRID INTRUSION DETECTION AND PREVENTION SYSTEM (IDPS) FOR LOW-LATENCY 5G NETWORKS WITH ADAPTIVE LEARNING USING EDGE COMPUTING

Yergazin Adil

ergazin.200332@gmail.com

Department of Information Security System, Faculty of Information Technologies, L.N.

Gumilyov Eurasian National University, Astana, Kazakhstan

Supervisor – Z. Tashenova

1. Introduction

The next generation of mobile networks is developing and evolving in the current era of digitalization, including 5G technology that is utilized in many spheres to meet customer needs with the possession of design priorities on efficiency, versatility, and scalability to match with characteristics based on connectivity and performance of the systems. 5G cellular networks should be efficient, and they differ in terms of requirements and features. In accordance with the emergence of 5G technologies, more improvements were utilized to maintain 5G networking, to reach clients needs, and to be efficient where distinct services vary on the options of requirements and features [28].

The novelty of this research lies in the development and evaluation of a Hybrid IDPS that integrates adaptive learning and edge computing. Adaptive learning reduces false positives and identifies new threats, while edge computing ensures low-latency responses and scalability for a high-density device environment. This dual approach offers an innovative framework to enhance the

security of 5G networks effectively.

The research aims to reveal the vulnerable 5G networks and the effectiveness of IDPS protection by reviewing its securing methods, additionally with the integration of adaptive learning. Adaptive learning methods are integrated into the system to reduce false positives and identify and prevent new cyber threats. The system guarantees real-time detection and response using advanced computing, offering efficient and scalable security solutions for many devices in the 5G environment, including IoT devices.

This research employs a theoretical and comparative analysis approach to investigate existing Intrusion Detection and Prevention Systems (IDPS) and their application within 5G networks. The methodology focuses on identifying vulnerabilities in network architectures such as Mobile Adhoc Networks (MANETs), Internet of Things (IoT), heterogeneous 5G systems, LTE-A, and Software-Defined Networking (SDN). It evaluates various IDPS techniques, including signature-based, anomaly-based, and hybrid methods, to understand their strengths and limitations in securing low-latency 5G environments. By integrating insights from this analysis, the study aims to analyze a hybrid IDPS with adaptive learning, leveraging edge computing for efficient threat detection and mitigation in 5G networks.

The research is guided by the following questions to explore the security challenges in 5G networks and the effectiveness of Intrusion Detection and Prevention Systems (IDPS):

- How effective are IDPS solutions in protecting 5G networks against diverse security threats?
- What characteristics define the most optimal IDPS for securing low-latency 5G networks
- Which 5G network components are most vulnerable to cyberattacks?

These questions aim to systematically analyze the vulnerabilities of 5G network components, evaluate existing IDPS techniques, and identify the critical features necessary for analyzing an adaptive hybrid IDPS tailored for the dynamic and low-latency nature of 5G networks.

2. Methodology

2.1 Analysis of IDPS methods for securing 5G networks

This methodology of the research handles the theoretical and comparative analysis of the existing 5G networks, their general workflow, security, and the existing IDPS to reveal its usage characteristics and security issues for developing the hybrid IDPS with adaptive learning by edge computing to secure the 5G networks. In the scope of 5G networks possessed networks vulnerabilities that might be detected and prevented by IDP systems, where it is segmented to signature-based detection, anomaly-based detection, and hybrid detection. They identify their strengths and limitations, particularly in low-latency scenarios. The 5G network vulnerabilities are numbered in MANETs (Mobile Adhoc Networks), IoT (Internet of Things), heterogeneous 5G and MCC (Mobile Cloud Computing), LTE-A systems for 5G network architectures, SDN (Software Defined Networking) [4], [15], [26], [20], [8], [18], [21], and various types of IDS/IPS system solutions are provided to them each individually with theoretically analysis and characteristics comparison analysis [4], [15], [26], [20], [8], [18], [21].

2.2 Theoretical and comparative analysis of existing 5G networks and IDPS

The dynamic and decentralized nature of MANETs makes the detection and prevention of masquerading attacks particularly complex [4]. MANETs are vulnerable to various cyber-attacks, such as black holes, gray holes, MITM (Man-In-The-Middle), and spoofing attacks, which destroy communication and compromise data integrity [4]. The IDS for MANET-cloud environments addresses challenges and ensures secure communication [4]. In the context of IDS for MANETs, the application of game theory is crucial with the help of assessing strategic decision-making in conflict scenarios, allowing the identification of optimal strategies for handling security threats [4]. The increasing prevalence of Internet of Things (IoT) devices has highlighted significant security

concerns, with many of these devices lacking sufficient protection, making them prime targets for malicious activities [15], [26], [20]. This growing number of vulnerable IoT devices opens the door to cyber-attacks, as attackers exploit their weak security measures to launch threats such as data breaches and unauthorized access, DDoS attacks [26], [15]. The IDPS systems are necessary for monitoring the behaviors of targets, accepted as security agents, to detect and prevent where they are activated and neighborhoods of targets [20]. The IDS system might efficiently detect and mitigate various attacks, additionally including DDoS attacks in 5G networks with the reduction of network availability influencings. [20], [15]. Security remains a significant concern in heterogeneous 5G networks due to the varied nature of RATs, each with unique vulnerabilities [8]. The interrelation among heterogeneous networks that might connect distributed services increases the risk of multiple intrusion appearances [8]. The security issues in MCC and heterogeneous 5G network utilization might be closed by intrusion detection techniques [8]. The specified approaches of IDS were signature-based, anomaly-based, and specification-based, where it requires the formation of a special demand with the behavior evaluation standards [8]. The LTE and LTE-A systems possessed vulnerabilities in accordance with interference mitigation, mode selection, device synchronization, security, and quality of service [18]. LTE and LTE-A systems are vulnerable to RF (Radio Frequency), including jamming, spoofing, and sniffing, and the exploration of the varieties of physical layer susceptibilities could rattle 5G network communication [18]. The IDS might detect anomaly behaviors in the 5G network [18]. If consider the workflow of IDS with an effective update, it includes two root segments, such as sample extraction from the dataset and selection of the common features from the data called DO-IDS [18]. The SDN contains the susceptibility in security based on the domain benefit as a double-edged sword that enables to simply manage the network [21]. The specific vulnerabilities of SDN depend on its being exploitable on account of the centralized construction reliance, ability to compromise the controller, and the development and deployment of the malware on the controller [21]. Each efficient IDS admits three methods, including a brute force method, a recovery approach, and an anticipatory approach with a wide exploration of packets in the IDS, like Snort, which is required to inspect wired network media at about 1 Gbps, with the beginning of packet dropping at 1.5 Gbps depending on the overhead [21]. In the Snort additions with FPGA and ASIC, the network speed at 4 and 7.2 Gbps acquires optimal packet drop percentage [21]. This methodology explores the vulnerabilities of 5G networks and systematically compares existing intrusion detection and prevention systems (IDPS), including their features such as signature-based, anomaly-based, and specific approaches as being hybrid, across various network architectures such as MANETs, IoT, heterogeneous 5G, LTE-A, and SDN, to develop a hybrid IDPS with adaptive learning using edge computing to secure 5G networks effectively.

2.3 Overview of solution tools

Unlike traditional static models, adaptive learning continuously updates its knowledge base to reflect new threats and network behaviors, making it particularly well-suited for the fast-paced nature of 5G environments [5].

In a 5G network, this is particularly important as the demand for real-time data processing grows, especially in applications such as smart cities, industrial automation, and healthcare, where delays can have serious consequences [7].

The combination of local processing power via edge computing with the adaptability of adaptive learning creates a powerful security framework that can address both known and unknown threats, making it a vital component of 5G security strategies [22], [8].

3. Results and Discussion

To keep 5G networks secure, it's essential to integrate hybrid Intrusion Detection and Prevention Systems (IDPS) with adaptive learning and edge computing. Different IDPS methods have their strengths and weaknesses—signature-based detection is great for known threats but ineffective against new ones, while anomaly-based detection can spot emerging attacks but often produces false

alarms. A hybrid solution utilizes the union of the two for more precise accuracy. Adaptive learning integration examines large volumes of network traffic and learns from emerging threats in real-time to increase security and is particularly labeled helpful for volatile environments such as IoT and mission-critical applications such as healthcare and autonomous vehicles. Furthermore, edge computing computes data nearer to the source, reduces the latency, conserves bandwidth, and because of that maintains security. The integration of these various technologies yields a flexible and scalable security framework capable of detecting and combating both known and unknown threats. Considering the vulnerability associated with 5G components such as MANETs, IoT, LTE-A, heterogeneous 5G, and SDN—each susceptible to various cyber threats—holistic security solutions are necessary; however, the integration of these solutions has its own challenges.

Hybrid Intrusion Detection and Prevention Systems (IDPS) combine signature-based and anomaly-based detection, offering robust protection against both known and unknown attacks. However, they can suffer from high false positives and increased processing overhead due to dynamic network topologies. Adaptive learning systems continuously adapt to changing network conditions, reducing false positives by learning from new attack behaviors, though they demand frequent updates and are vulnerable to adversarial attacks. Lastly, edge computing processes data locally, enhancing scalability and reducing latency, particularly for mobile and IoT devices, but it faces limitations in computational power and presents security risks due to its distributed nature.

4. Conclusion

This study successfully addressed the research questions by evaluating the effectiveness of IDPS solutions in safeguarding 5G networks, identifying the key characteristics of an optimal IDPS for low-latency environments, and pinpointing the most vulnerable components of 5G network infrastructures. The findings demonstrate that while existing IDPS techniques offer varying degrees of protection, their limited adaptability and high false positive rates pose significant challenges in dynamic 5G environments.

The proposed hybrid IDPS framework, integrating adaptive learning and edge computing, emerges as a viable solution to these challenges. Adaptive learning ensures continuous improvement by identifying and mitigating evolving threats, while edge computing enhances real-time detection and response capabilities. These features collectively address the latency-sensitive and high-density device requirements of 5G networks, making the proposed system highly scalable and efficient.

The research also identified critical vulnerabilities within 5G components such as MANETs, IoT devices, and SDN. These components are particularly susceptible to cyberattacks due to their decentralized architectures and resource constraints. By tailoring the hybrid IDPS to address these vulnerabilities, the study provides a robust framework for enhancing 5G network security.

In conclusion, this research contributes to the field of cybersecurity by providing a comprehensive analysis of IDPS effectiveness in 5G networks and proposing an innovative, adaptive solution. Future work could include practical implementation and testing of the hybrid IDPS to further validate its effectiveness in real-world scenarios.

Literature

1. A. Afaq, N. Haider, M. Z. Baig, K. S. Khan, M. Imran, and I. Razzak, "Machine learning for 5G security: Architecture, recent advances, and challenges," *Ad Hoc Networks*, vol. 123, p. 102667, Dec. 2021, doi: 10.1016/j.adhoc.2021.102667.
2. I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, and M. Ylianttila, "Security for 5G and Beyond," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 1–1, 2019, doi: 10.1109/comst.2019.2916180.
3. I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Overview of 5G Security Challenges and Solutions," *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36–43, Mar. 2018, doi: 10.1109/mcomstd.2018.1700063.

4. S. A. Alghamdi, "Novel trust-aware intrusion detection and prevention system for 5G MANET–Cloud," *International Journal of Information Security*, Sep. 2021, doi: 10.1007/s10207-020-00531-6.
5. A. Chiche and M. Meshesha, "Towards a Scalable and Adaptive Learning Approach for Network Intrusion Detection," *Journal of Computer Networks and Communications*, vol. 2021, pp. 1–9, Jan. 2021, doi: 10.1155/2021/8845540.
6. A. Dutta and E. Hammad, "5G Security Challenges and Opportunities: A System Approach," *IEEE Xplore*, Sep. 01, 2020. doi: 10.1109/5GWF49715.2020.9221122.
7. F. Fang and X. Wu, "A Win–Win Mode: The Complementary and Coexistence of 5G Networks and Edge Computing," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 3983–4003, Mar. 2021, doi: 10.1109/jiot.2020.3009821.
8. K. Gai, M. Qiu, L. Tao, and Y. Zhu, "Intrusion detection techniques for mobile cloud computing in heterogeneous 5G," *Security and Communication Networks*, vol. 9, no. 16, pp. 3049–3058, Feb. 2015, doi: 10.1002/sec.1224.
9. M. K. Hasan et al., "A Review on Security threats, vulnerabilities, and Counter Measures of 5G Enabled Internet-of-Medical-Things," *IET Communications*, vol. 16, no. 5, Nov. 2021, doi: 10.1049/cmu2.12301.
10. C. Hashemi-Pour, "What is the CIA Triad? Definition, Explanation and Examples," *TechTarget*, Dec. 2023. <https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA>
11. Md. A. Hasnat, S. T. A. Rumeen, Md. A. Razzaque, and Md. Mamun-Or-Rashid, "Security Study of 5G Heterogeneous Network: Current Solutions, Limitations & Future Direction," *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)*, Feb. 2019, doi: 10.1109/ecace.2019.8679326.
12. A. Imanbayev et al., "Research of Machine Learning Algorithms for the Development of Intrusion Detection Systems in 5G Mobile Networks and Beyond," *Sensors*, vol. 22, no. 24, p. 9957, Dec. 2022, doi: 10.3390/s22249957.
13. M. A. Javed and S. Khan Niazi, "5G Security Artifacts (DoS / DDoS and Authentication)," *IEEE Xplore*, Mar. 01, 2019. doi: 10.1109/COMTECH.2019.8737800.
14. C. Jiang, H. Xu, C. Huang, and Q. Huang, "An Adaptive Information Security System for 5G-Enabled Smart Grid Based on Artificial Neural Network and Case-Based Learning Algorithms," *Frontiers in Computational Neuroscience*, vol. 16, Apr. 2022, doi: 10.3389/fncom.2022.872978.
15. Umar Danjuma Maiwada et al., "Enhancing DDoS Detection in 5G Systems through Advanced Intrusion Detection Techniques," *Zhongguo Kuangye Daxue Xuebao*, vol. 29, no. 3, pp. 130–140, 2024, Accessed: Mar. 14, 2025. [Online]. Available: <https://zkdx.ch/journal/zkdx/article/view/74>
16. S. Park, D. Kim, Y. Park, H. Cho, D. Kim, and S. Kwon, "5G Security Threat Assessment in Real Networks," *Sensors*, vol. 21, no. 16, p. 5524, Aug. 2021, doi: 10.3390/s21165524.
17. H. M. Tran, Ca Van Phan, and Q.-T. Vien, "An Overview of 5G Technologies," Jun. 2018, doi: 10.1007/978-981-13-0396-8_4.
18. A. Rahman et al., "Network Anomaly Detection in 5G Networks," *Mathematical Modelling of Engineering Problems*, vol. 9, no. 2, pp. 397–404, Apr. 2022, doi: 10.18280/mmep.090213.
19. "Attacks on 5G Infrastructure From Users' Devices," *Trend Micro*, Sep. 20, 2023. https://www.trendmicro.com/en_us/research/23/i/attacks-on-5g-infrastructure-from-users-devices.html
20. H. Sedjelmaci, "Cooperative attacks detection based on artificial intelligence system for 5G networks," *Computers & Electrical Engineering*, vol. 91, p. 107045, May 2021, doi: 10.1016/j.compeleceng.2021.107045.

21. S. S. Shah and S. P. Bendale, "An Intuitive Study: Intrusion Detection Systems and Anomalies, How AI can be used as a tool to enable the majority, in 5G era," *ICCUBEA Int. Conf.*, Sep. 2019, doi: 10.1109/iccubea47591.2019.9128786.
22. A. Singh, K. Chatterjee, and S. C. Satapathy, "An edge based hybrid intrusion detection framework for mobile edge computing," *Complex & Intelligent Systems*, Aug. 2021, doi: 10.1007/s40747-021-00498-4.
23. S. Sullivan, A. Brighente, S. A. P. Kumar, and M. Conti, "5G Security Challenges and Solutions: A Review by OSI Layers," *IEEE Access*, vol. 9, pp. 116294–116314, 2021, doi: 10.1109/access.2021.3105396.
24. B. A. Tama and S. Lim, "Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation," *Computer Science Review*, vol. 39, p. 100357, Feb. 2021, doi: 10.1016/j.cosrev.2020.100357.
25. R. Ullah, M. A. U. Rehman, M. A. Naeem, B.-S. Kim, and S. Mastorakis, "ICN with edge for 5G: Exploiting in-network caching in ICN-based edge computing for 5G networks," *Future Generation Computer Systems*, vol. 111, pp. 159–174, Oct. 2020, doi: 10.1016/j.future.2020.04.033.
26. N. Yadav, S. Pande, A. Khamparia, and D. Gupta, "Intrusion Detection System on IoT with 5G Network Using Deep Learning," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–13, Mar. 2022, doi: 10.1155/2022/9304689.
27. X. Yan, Y. Xu, X. Xing, B. Cui, Z. Guo, and T. Guo, "Trustworthy Network Anomaly Detection Based on an Adaptive Learning Rate and Momentum in IIoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6182–6192, Sep. 2020, doi: 10.1109/tii.2020.2975227.
28. H. Yu, H. Lee, and H. Jeon, "What is 5G? Emerging 5G Mobile Services and Network Requirements," *Sustainability*, vol. 9, no. 10, p. 1848, Oct. 2017, doi: 10.3390/su9101848.

UDC 004.056

KEY ATTACKS IN WEB FORENSICS: XSS, SQL INJECTION AND RCE

Yerzhanova Yerke Yerzhankyzy

ymerzhanova@mail.ru

Master's student at the Faculty of Information Technology
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
Scientific supervisor – S.A. Santeyeva

Information security is one of the critical subjects that requires in-depth analysis by every state. Vulnerabilities in web applications are continuously being identified, necessitating their timely detection and mitigation. Organizations must consistently conduct comprehensive testing of their applications to ensure resilience against potential threats. Web forensics is a specialized domain within web forensics that focuses on investigating incidents related to web applications, websites, and online activities. Its primary objective is identifying, analyzing, and reconstructing digital evidence following cyberattacks and security breaches.

The key areas of focus in web forensics include:

- Analysis of web server logs;
- Investigation of compromised web applications;
- Forensic analysis of browsers and user data;
- De-anonymization of attackers;
- Forensic examination of cloud-based web services [1].