

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 «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

СОВРЕМЕННЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОБЛАЧНЫХ ВЫЧИСЛЕНИЯХ: МОДЕЛИ, УГРОЗЫ И МЕТОДЫ ЗАЩИТЫ

Сафонова Софья Александровна

safonova_sa@enu.kz

Студентка факультета Информационных технологий, ЕНУ им. Л.Н.Гумилева, Астана,
Казахстан

Научный руководитель – Ахаева Ж. Б.

Аннотация: В данной статье будут рассмотрены самые распространенные модели облачных технологий и проведен собирательный обзор по научным статьям и литературным источникам на основные проблемы и инструменты решения. Внимание уделено самым распространенным категориям угроз: проблемы мониторинга, контроль трафика и совместимости, безопасность виртуализации, настройка пользовательского доступа и кибератаки, а также перечислены распространенные инструменты для их нейтрализации.

Ключевые слова: облачные вычисления, информационная безопасность, защита данных, управление доступом

Введение. Облачные вычисления представляют собой современную модель предоставления вычислительных услуг через интернет, включая серверы, хранилища, базы данных и программное обеспечение. Согласно отчету Gartner [1], к 2028 году облачные технологии станут необходимостью для бизнеса. Сами облачные сервисы обеспечиваются провайдером, в связи с чем возрастает проблема безопасности для потребителя, в зависимости от облагаемой ими ответственности, которая может варьироваться от модели к модели. Выдвинем гипотезу, что угрозы классифицируются по типам, а следовательно, к ним можно комплектно применять способы эффективной защиты. Целью данной работы является проведение комплексного анализа угроз, связанных с использованием облачных технологий. Необходимо определить основных категории угроз и предложить инструменты для их ликвидации, изучить отчеты международных организаций и просмотреть научные статьи, систематизировать угрозы и определить их в категории.

Концепция облачных вычислений не является новой и может рассматриваться как развитие существующих сетевых технологий, в частности Интернета. Джон Вакка (John R. Vacca) выделяет основную идею облачных вычисления — это передача управления вычислительными ресурсами сторонним специализированным провайдерам, которые могут обеспечивать их эффективное использование, предлагая высокое качество обслуживания при снижении затрат [2].

Мазер Т., Кумарасвами С., Латиф Ш. рассматривают классификационную модель «SPI», представляющая собой подход к описанию основных типов облачных сервисов, включая три ключевые модели обслуживания: SaaS, PaaS и IaaS [3]. На рисунке 1 представлена детальная схема взаимодействия между различными моделями обслуживания и развертывания сервисов.

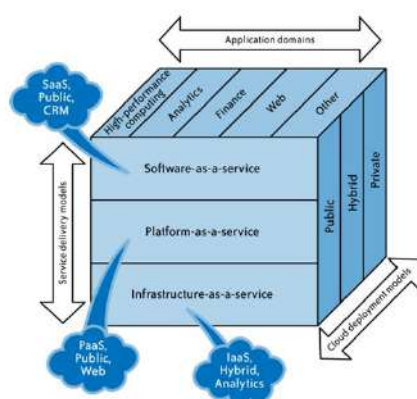


Рисунок 1. Модель «SPI». Отображает виды моделей обслуживания, развертывания и их применение.

Модели обслуживания

Модель обслуживания облачных услуг — это стандартизированный набор ИТ-ресурсов и сервисов, структурированных провайдером для предоставления клиентам. Национальный институт стандартов и технологий США, выделяет следующие модели:

1. SaaS (Software as a Service) – программное обеспечение как услуга.

SaaS функционирует по принципу веб-сервисов, предоставляя клиентам доступ к программному обеспечению через облачную инфраструктуру поставщика. Пользователи получают доступ к приложениям посредством стандартных веб-интерфейсов с различных устройств.

2. PaaS (Platform as a Service) – платформа как услуга.

PaaS представляет собой облачную платформу, предоставляющую клиентам профессиональную среду для разработки и развертывания приложений в изолированном пространстве провайдера. Данная модель оптимизирована для управления базами данных и разработки программного обеспечения.

3. IaaS (Infrastructure as a Service) – инфраструктура как услуга.

IaaS представляет собой модель облачных вычислений, предоставляющая клиентам возможность развертывания всей необходимой вычислительной инфраструктуры в облаке, включая операционные системы. Данное решение обеспечивает полнофункциональную виртуальную среду, аналогичную традиционной физической инфраструктуре [4].

Ответственность за безопасность со стороны клиента и поставщика

Безопасность облачных сервисов функционирует в рамках модели совместной ответственности. Данная модель предусматривает следующее распределение обязанностей:

- Облачный провайдер обеспечивает безопасность инфраструктуры облака, включая физические центры обработки данных, сетевые компоненты и базовую облачную архитектуру.
- Организация-клиент отвечает за безопасность своих ресурсов в облаке, в том числе за защиту размещенных приложений, систем и данных.

Cloud Security Alliance (CSA) отмечает, что в модели SaaS основная ответственность за безопасность лежит на поставщике, так как пользователь ограничен в управлении приложением и отвечает лишь за права доступа. В модели PaaS провайдер защищает платформу, а клиент — собственные решения и настройки безопасности. В IaaS клиенту передается наибольший объем ответственности, включая защиту всех развернутых компонентов, в то время как провайдер обеспечивает безопасность базовой инфраструктуры [5]. Такое распределение обязанностей помогает точнее определить угрозы и подобрать меры защиты в зависимости от типа облачной модели - от SaaS к IaaS возрастает ответственность пользователя, однако физическая безопасность, безопасность сервисов и доступность всей инфраструктуры — это постоянная ответственность специалистов облака. Это разделение помогает ясно определить угрозы и выбрать соответствующие меры защиты в зависимости от модели облачного сервиса.

Климачев С. А. утверждает, что «в модели SaaS внимания заслуживают вопросы, касающиеся безопасности данных, приложений и развертывания, в PaaS – уязвимости хоста и ресурсов» [6]. Никифорова А. А. также разделяет зоны ответственности между в разных моделях, то есть в модели IaaS поставщик отвечает за вычислительные, сетевые ресурсы и хранилище данных, тогда как клиент — за приложения, ПО и ОС. В PaaS поставщик управляет инфраструктурой и частью ПО, оставляя клиенту безопасность данных и приложений. В SaaS ответственность за санкционированный доступ полностью лежит на поставщике [7].

Риски, связанные с облачной безопасностью

Данные, хранящиеся в облаке, являются важнейшим компонентом облачных вычислений, однако клиенты часто не рискуют передавать и взаимодействовать с данными из-за опасений по поводу конфиденциальности, потери и отсутствия полного контроля. После размещения данных в облаке пользователи не знают ни о местонахождении данных, ни о мерах безопасности, ни о том, как они обрабатываются. К основным проблемам безопасности

относятся проблемы мониторинга, контроль трафика, безопасность виртуализации, работа с аутентификацией и кибератаками, как показано в таблице 1.

Проблемы мониторинга и реагирования. В своих работах Гребенник О. Г. [8] и Гладкий М.В. [9] утверждают, что «при использовании облачных вычислений периметр сети размывается или исчезает». Объясняется это тем, что в облаке используются многочисленные компоненты — виртуальные машины, API, облачные хранилища, сети и сервисы третьих сторон — что увеличивает число потенциальных точек входа для атакующих. Сам периметр сети или поверхность атаки — это все точки входа и уязвимости, которые злоумышленник может использовать для проникновения в сеть или систему [10]. С. А. Климачев говорит о высоком шансе «аномалий» из-за сложности структуры облачной инфраструктуры и отсутствие методической базы для корректной оценки эффективности систем мониторинга, что усложняет определение корректного решения способа защиты [6]. У Шатурного М.В. защита периметра входит в «Безопасность инфраструктуры», где безопасность лежит полностью под ответственность провайдера [11]. Согласно Forrester, преобладающее большинство организаций (62%) применяют комбинированный подход, задействуя либо несколько публичных облаков (мультиоблачная архитектура), либо интегрируя публичные облака с локальной инфраструктурой (гибридная архитектура), что усложняет мониторинг, так как каждая платформа имеет свой набор инструментов наблюдения [12].

Контроль трафика и совместимости приложений. Application Programming Interfaces (APIs) обеспечивают взаимодействие между программными приложениями, при этом как упоминает Беспалова Н. В., «являются слабыми точками системы», так как могут предоставить несанкционированный доступ к системе и пользовательским данным [13]. Гребенник О.Г. [8] относит это к типу «функциональные атаки на элементы облака», обусловленный многослойностью облака, а Шатурный М.В. [11] определяет защиту API, как «безопасность на уровне управления», ведь позволяют интегрировать несколько приложений, с разными условиями аутентификации. Никифорова А.А [7]. и Гладкий М.В. [9] рассматривают совместимость с базами данных и большими данными, доступ к которым должен был ограничен узкому кругу лиц и требовать проверку веб-сетевого трафика, иначе высока вероятность перехвата пакетов или легкого проникновения в систему через слабо защищенный интерфейс, а Митрошина Е.В. [14] отмечает SOAP, REST и HTTP протоколы, где слабая защита приводит к «перенаправлению операций» или краже личных данных. Сложная интеграция API и разнообразие протоколов требуют усиленной аутентификации, контроля трафика и ограниченного доступа к критически важным ресурсам.

Безопасность инфраструктуры и виртуализации. Современные облачные технологии обеспечивают динамическое масштабирование ресурсов в соответствии с операционными требованиями организации. Учитывая простоту создания виртуальных машин и контейнеров, возникает риск их неконтролируемого распространения. Гребенник О.Г. [11] и Гладкий М.В. [9] рассматривают их как «атаки на системы управления» и «атаки на гипервизор» - захват ресурсов виртуальных машин. Шатурный М.В. [11] отмечает, что безопасность виртуализации можно разделить на защиту гипервизора и средств управления безопасностью виртуальных машин, обусловленных виртуальной инфраструктурой. Это выражается в появлении машин «невидимок» способным перехватывать трафик и управлять другими машинами, саботируя работу облака или загрузку вирусов, через загрузку образа, как приводит Митрошина Е. В. [14] Васильев В. Н. [15] отмечает также возможное слежение за пользователем со стороны хоста или виртуальной машины, в целом их изменчивость влияет на целостность всей системы безопасности. Неактивные виртуальные машины и контейнеры не только компрометируют безопасность инфраструктуры, но и приводят к нерациональному увеличению расходов на облачные сервисы.

Некорректная настройка пользовательского доступа и аутентификации. Инфраструктура облачных сервисов обеспечивает оптимизированный удаленный доступ посредством интернет-соединения, что существенно повышает эффективность использования корпоративных ресурсов независимо от географического положения пользователя. Беспалова Н. В. [13] утверждает, что «причиной утечки информации нередко является проблема

некачественной настройки механизмов аутентификации» из-за высокого риска компрометации через фишинг с целью кражи объектов интеллектуальности собственности внутри компании. Важно, что нарушители могут быть, как и внутренними, так и внешними, объясняя низкий уровень квалификации сотрудников и несоответствие их пользовательских прав к должностным полномочиям. Васильев В. Н. [15], Гладкий М.В. [9], Гребенник О. Г. [8] выделяют необходимость согласованной защищённости данных, которую могут предоставить только ограничения по группам пользователей и ранжировка данных по уровню важности. Коробенкова Д. А. [16] и Митрошина Е. В. [14] также рассматривает проблему утечки, утверждая, что причинной этому является «недостаток осведомленности» со стороны пользователя – слабые учетные данные или неполная проверка подлинности пользователя. К примеру, согласно отчету групп реагирования на инциденты Google Cloud, за первый квартал 2023, около 55% всех компрометаций облачных систем произошли в результате слабых паролей или их полного отсутствия [17].

Кибератаки и вредоносное ПО. Коробенкова Д. А. [16], Гребенник О. Г. [8], Гладкий М. В. [9] и Беспалова Н. В. [13] определяют DDoS как основной тип кибератаки на облачные ресурсы. В случае DDoS-атак злоумышленники предпринимают попытки дестабилизировать систему посредством генерации избыточного количества запросов к вычислительным ресурсам, что может привести к существенному снижению производительности или полному прекращению работы системы. В 2024 Microsoft столкнулась с крупным сбоем, вызванным атакой DDoS, которая затронула пользователи по всему миру, сделав недоступными ключевые сервисы Microsoft 365 [18]. Фишинговые атаки часто рассматриваются как способ первоначального проникновения и часто сопряжены с низким уровнем осведомленности пользователя. В рамках фишинговых атак злоумышленники осуществляют рассылку электронных сообщений, имитирующих письма от доверенных источников, с целью получения несанкционированного доступа к конфиденциальным данным. Беспалова Н. В. отмечает, что атака может не только выкрасть учетные записи, но и привести к «внедрению эксплойта» - вредоносных программ отсроченного действия [13]. Согласно последнему отчету IBM X-Force о киберугрозах в облачной среде, фишинг является основным способом начального доступа для атак на облачные системы. Этот метод, используемый хакерскими группами для кражи учетных данных и получения доступа к сетям, составил треть всех облачных инцидентов, на которые IBM X-Force реагировала за последние два года [19]. В спектре угроз также выделяются инъекционные атаки. Инъекционная атака — это несанкционированное вмешательство в работу уязвимых серверов, позволяющее злоумышленникам получить доступ к данным, компрометировать учетные записи и распространять вредоносное ПО. О таких атаках упоминают Митрошина Е. В. [14], Гладкий М. В. [9], Гребенник О. Г. [11], Беспалова Н. В. [13]. В мае 2023 года была выявлена критическая уязвимость в MOVEit Transfer. Хакерская группа Cl0p эксплуатировала SQL-инъекцию для кражи данных крупных компаний и госучреждений, включая Shell, Deutsche Bank, PwC, Департамент энергетики США, BBC и British Airways. По состоянию на июль 2023 года атака затронула около 400 организаций и более 20 млн человек, а в ноябре 2024 года стало известно об утечке данных сотрудников Amazon [20].

Таблица 1. Перечень угроз в облачной инфраструктуре

Область угрозы	Описание угроз
Проблемы мониторинга и реагирования	Отсутствие комплексного решения [6] Размытие периметра сети [8], [9], [11] Трудность оценки эффективности защиты [6]
Контроль трафика и совместимости приложений	Отсутствие фильтрации трафика [11], [7] Утечка информации [8], [9], [11], [13], [14], [15], [16] Отсутствие шифрования [7], [9] [11], [13] Недостаточный контроль над IP [11], [13], [14] Отсутствие защиты шлюзов API [9], [11], [13], [14]
Безопасность инфраструктуры и виртуализации	Уязвимости гипервизора [8], [9], [11], [15] Вредоносные VM [9], [8], [14], [15] Атаки при переносе VM [9], [14], [15] Слежение со стороны хоста [15]

	Захват хост машины [9], [14], [15]
Некорректная настройка пользовательского доступа и аутентификации	Кража/компрометация учетных записей [6], [8], [13], [14], [16] Слабые пароли и недостаточная проверка авторизации [11], [14] Отсутствие политик доступа [7], [9], [11], [15]
Кибератаки и вредоносное ПО	Фишинг [13], [16] Трояны [14], [16] DoS/DDoS [8], [9], [13], [14], [16] SQL-инъекции [8], [9], [13], [14] Спуфинг [14]

Способы защиты облака

На основе анализа можно выделить четыре ключевых набора инструментов для обеспечения безопасности облачной инфраструктуры. Эти методы включают системы управления доступом и идентификацией, защиты данных от потерь, мониторинга безопасности и управления событиями, а также шифрования данных.

1. Identity and Access Management (IAM) — это система управления цифровыми идентификациями и правами доступа пользователей к ресурсам организации.

Согласно Шатурному М.В. «управление контролем доступа требует взаимодействия провайдера и клиента облачных услуг по вопросам распределения обязанностей в обеспечении его функционирования» [11]. Сюда же входит работа с многофакторной аутентификацию (MFA), согласно Митрошиной Е. В. [14], Гребеннику О. Г. [8] и Васильеву В. Н. [15], а также политика нулевого доверия (Zero Trust), обеспечивающей безопасность даже в случае компрометации учетных данных, по мнению Беспаловой Н. В. [13].

2. Data Loss Prevention (DLP) – ПО для обнаружения утечек и их предотвращения, благодаря блокированию чувствительной информации во время использования (in use), передачи (in motion) и хранения (at rest).

К DLP относят стандартные меры безопасности, такие как брандмауэры, предотвращает доступ посторонних во внутреннюю сеть, системы обнаружения вторжений (IDS) для выявляет попытки проникновения посторонних и антивирусное ПО, защищают от внешних и внутренних атак. Гладкий М.В. выделяет «средства контроля целостности», способные проводить контроль свойств и метаданные файлов, проверяя их на компрометацию [9]. Google утверждает, что Система предотвращения потери данных (DLP) обеспечивает комплексный контроль над информационными активами, включая их автоматическое обнаружение, классификацию и защиту [21].

3. Security Information and Event Management (SIEM) — это система управления информационной безопасностью и событиями, которая анализирует логи, отслеживает инциденты и выявляет угрозы в IT-инфраструктуре организации.

Беспалова Н. В. [13] относит данный функционал к категории «Мониторинг рисков безопасности инфраструктуры», а Шатурный М.В. [11] к - «реагированию на инциденты». В функционал SIEM входят автоматизированный мониторинг безопасности, корреляция событий для выявления сложных атак, анализ логов в реальном времени, обнаружение уязвимостей, предупреждение сбоев, а также контроль ключевых параметров производительности сети [22].

4. Public Key Infrastructure (PKI) - шифрование данных для хранения и передачи. Шифрование данных – основополагающий механизм защиты облачной инфраструктуры. Согласно Kaspersky бывает:

- Комплексное шифрование коммуникаций в облачной среде.
- Усиленное шифрование конфиденциальных данных, включая аутентификационную информацию.
- Сквозное шифрование для всего массива загружаемой информации [23].

Кеерг утверждает, что особую актуальность защита данных приобретает в процессе их перемещения между различными хранилищами или при передаче из облака в локальную инфраструктуру [24]. Гребенник О.Г. отмечает шифрование, как «один из эффективных способов защиты данных», так как они отвечают, как за сохранность данных, так и защиту при

передаче, используя AES, TLS, IPsec [11]. Аналогично, Беспалова Н. В. [13] указывает, что облачные системы имеют встроенные системы шифрования данных, упрощая шифрование на всех этапах - пользовательской, при передаче и в процессе хранения в базе. Гладкий М. В. рассматривает так же «самозащищенные данные», требующие от среды удовлетворения определённого набора правил для доступа к информации, обеспечивающие максимальный уровень защиты критически важной информации, поскольку доступ к ним возможен исключительно при наличии соответствующего ключа шифрования [9].

Заключение

По мере увеличения числа организаций, переходящих на облачные технологии, возрастает и актуальность вопросов информационной безопасности. Проведённый анализ позволил выявить ключевые угрозы, с которыми сталкиваются пользователи облачных сервисов: сложности мониторинга, в результате расширенного периметра атак, слабые точки системы через интерфейсы приложений, поддержка сохранности инфраструктуры и инструментов виртуализации, слабая настройка аутентификации и некорректное распределение ролей в соответствии с должностными полномочиями и внешние атаки.

Учитывая это, эффективная защита облака требует комплексного подхода, основанного на применении современных инструментов и практик. В частности, важно внедрять системы управления доступом (IAM), обеспечивающие разграничение прав пользователей и поддержку многофакторной аутентификации. Для предотвращения утечек данных рекомендуется использовать решения класса DLP, позволяющие контролировать движение и хранение информации на всех этапах её жизненного цикла. Не менее значимым элементом защиты является внедрение систем мониторинга и реагирования на инциденты (SIEM), обеспечивающих своевременное обнаружение угроз и анализ событий безопасности. Дополнительно, использование инфраструктуры открытых ключей (PKI) позволяет организовать надёжное шифрование данных как при передаче, так и при хранении, что особенно важно в условиях распределённых вычислений. В совокупности данные меры значительно повышают уровень защищённости облачных систем и позволяют минимизировать риски, связанные с киберугрозами и утратой конфиденциальной информации. Применение данных методов защиты необходимо вне зависимости от модели обслуживания и развертывания облачной инфраструктуры. Однако степень ответственности за обеспечение безопасности варьируется в зависимости от выбранной модели: она может лежать как на облачном провайдере, так и на клиенте.

Список использованных источников

1. Gartner Says Cloud Will Become a Business Necessity by 2028 // Gartner URL: <https://www.gartner.com/en/newsroom/press-releases/2023-11-29-gartner-says-cloud-will-become-a-business-necessity-by-2028> (дата обращения: 06.03.2025).
2. Vacca J. R. Cloud Computing Security: Foundations and Challenges. - 1st edition - CRC Press, 2016. - 520 p.
3. Mather T., Kumaraswamy S., Latif S. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. - 1st edition - O'Reilly Media, 2009. - 334 p.
4. Mell P. M., Grance T. SP 800-145. The NIST Definition of Cloud Computing // Technical Report. - Gaithersburg: National Institute of Standards and Technology, 2011
5. CSA Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. – 4th Edition - Cloud Security Alliance, 2017
6. Климачев С.А. К вопросу безопасности облачных вычислений // Инновационная наука. - 2016. - №10. - С. 65–67.
7. Никифорова А. А. Информационная безопасность и облачные вычисления // E-Scio. - 2021. - №11. - С. 22–28.
8. Гребенник О. Г., Иваницкий А. В., Николаенко М. А. Анализ безопасности облачных вычислений // Теория и практика современной науки. - 2015. - №6. - С. 279–281.
9. Гладкий М. В. Безопасность приложений на платформах облачных вычислений // Труды БГТУ. - 2015. - №6. - С. 204–207.

10. What is an attack surface? // Cloudflare URL: <https://www.cloudflare.com/learning/security/what-is-an-attack-surface/> (дата обращения: 14.03.2025).
11. Шатурный М.В. Особенности обеспечения безопасности облачных систем // Инженерный вестник Дона. - 2024. - №7
12. Baum R., Blackborow J., Lloyd J. Cloud Maturity Drives Business Success. - Forrester Research, 2024. - 30 p.
13. Беспалова Н. В. Методы и системы защиты информации, информационная безопасность // Computational Nanotechnology. - 2024. - №5. - С. 124–132.
14. Митрошина Е. В. Исследование угроз безопасности облачных вычислений // E-Scio. - 2017. - №. 1 (4). - С. 96–99
15. Васильев В. Н. Безопасность в облачных вычислениях // Теория и практика современной науки. - 2017. - №3. - С. 158–166.
16. Коробенкова Д. А. Информационная безопасность в эпоху цифровых технологий: вызовы и решения // Вестник науки. - 2025. - №3. - С. 41–44.
17. Office of the CISO Threat Horizons. August 2023 Threat Horizons Report. - Google Cloud, 2023. - 31 p.
18. Microsoft And AWS Outages: A Wake-Up Call for Cloud Dependency // Forbes URL: <https://www.forbes.com/sites/emilsayegh/2024/07/31/microsoft-and-aws-outages-a-wake-up-call-for-cloud-dependency/> (дата обращения: 15.03.2025).
19. Zeizel A., Caridi C., McMillen D. X-Force Cloud Threat Landscape Report 2024. - IBM, 2024. - 25 p.
20. MOVEit Data Leak Exposes Employee Data of Amazon, HSBC & More – What You Need to Know // SOCRadar Cyber Intelligence Inc. URL: <https://socradar.io/moveit-data-leak-exposes-employee-data-of-amazon-hsbc-more-what-you-need-to-know/> (дата обращения: 15.03.2025).
21. What is cloud security? // Cloud Google URL: <https://cloud.google.com/learn/what-is-cloud-security> (дата обращения: 06.03.2025).
22. Безопасность облачных вычислений // Хабр URL: <https://habr.com/ru/companies/ussc/articles/860484/> (дата обращения: 07.03.2025).
23. Что такое безопасность облака? // Kaspersky URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-cloud-security> (дата обращения: 06.03.2025).
24. Что такое безопасность облачных вычислений? // Keeper URL: https://www.keepersecurity.com/ru_RU/resources/glossary/what-is-cloud-computing-security (дата обращения: 25.03.2025).