# Central Asian Scientific Journal

VOL 2(30)
2026

ASTANA

ISSN: 3135-3061

Электронный научный журнал «Central Asian Scientific Journal»

# Central Asian Scientific Journal

выпуск №2 (30), апрель – июнь 2026 г.
Том 2
Основан в 2021 году (издается ежеквартально)

зарегистрирован в Комитете информации Министерства информации и общественного развития Республики Казахстан №KZ77VPY00147053 от 17.04.2026 г.

**Taqyryptyq baǵyt:**

- Pedagogıkalyq, qoǵamdyq-áleýmettik, tehnıkalyq, ekonomıkalyq jáne zań ǵylymdary
- Aqparattyq-komýnıkasıalyq tehnologıalar
- Teorıalyq jáne ǵylymı-praktıkalyq ǵylymı zertteýler

**Тематическая направленность:**

- Педагогические, общественно-социальные, технические, экономические и юридические науки
- Информационно-коммуникационные технологии
- Теоретические и научно-практические научные исследования

**Thematic focus:**

- Pedagogical, socio-political, technical, economic, and legal sciences
- Information and communication technologies
- Theoretical and scientific-practical research

*Jarıalanatyn aqparattyń, dáıeksózderdiń jáne ózge de baıandamalardyń durystyǵy úshin avtor jaýapty bolady*

*За достоверность публикуемой информации, цитат и иных изложений ответственность несет автор*

*The author is responsible for the accuracy of the published information, quotes, and other statements.*

ISSN: 3135-3061

"Central Asian Scientific Journal" elektrondyq ǵylymı jýrnaly aqparattyq agenttigi

№2 (30), 2026 j
Shyǵarý jıiligi –jylyna 4 nómir
2021 j. bastap shyǵady



Qazaqstan Respýblıkasy Aqparat jáne qoǵamdyq damý mınıstrliginiń 17.04.2026 j. №KZ77VPY00147053 aqparat komıtetinde tirkelgen.

JK DOC, 010000, Qazaqstan Respýblıkasy, Astana q.

Информационное агентство Электронный научный журнал «Central Asian Scientific Journal»

№2 (30), 2026 г.
Периодичность – 4 номера в год
Выходит с 2021 года



Зарегистрирован в Комитете информации Министерства информации и общественного развития Республики Казахстан №KZ77VPY00147053 от 17.04.2026

ИП DOC, 010000, Республика Казахстан, г. Астана



No.2 (30), 2026
Periodicity: 4 issues per year
Since 2021



Registered with the Information Committee of the Ministry of Information and Public Development of the Republic of Kazakhstan No. KZ77VPY00147053 dated 17.04.2026.

IP DOC, 010000, Kazakhstan, Astana

# МАЗМҰНЫ – СОДЕРЖАНИЕ – CONTENT

## БИОЛОГИЯ ҒЫЛЫМДАР - БИОЛОГИЧЕСКИЕ НАУКИ - BIOLOGICAL SCIENCES



## ТЕХНИКАЛЫҚ ҒЫЛЫМДАР - ТЕХНИЧЕСКИЕ НАУКИ - TECHNICAL SCIENCE

**ЭКОНОМИКАЛЫҚ ЖӘНЕ ҚҰҚЫҚ ҒЫЛЫМДАРЫ - ЭКОНОМИЧЕСКИЕ И ЮРИДИЧЕСКИЕ НАУКИ - ECONOMIC AND LEGAL SCIENCES**



**ПЕДАГОГИКА ЖӘНЕ ПСИХОЛОГИЯ ҒЫЛЫМДАР - ПЕДАГОГИЧЕСКИЕ И ПСИХОЛОГИЧЕСКИЕ НАУКИ - PEDAGOGICAL AND PSYCHOLOGICAL SCIENCES**



**ЖАРАТЫЛЫСТАНУ ҒЫЛЫМДАРЫ – ЕСТЕСТВЕННЫЕ НАУКИ –NATURAL SCIENCES**



**ӘЛЕУМЕТТІК-ГУМАНИТАРЛЫҚ ҒЫЛЫМДАР – СОЦИАЛЬНО-ГУМАНИТАРНЫЕ НАУКИ – SOCIAL AND HUMANITARIAN SCIENCES**

**БИОЛОГИЯ ҒЫЛЫМДАР - БИОЛОГИЧЕСКИЕ НАУКИ - BIOLOGICAL SCIENCES**

**УДК 576.3**

**Мирзалиева Сафура Мирвохидовна**

Студентка 1 курса
кафедра «Молекулярная биология и медицинская генетика»
Научный руководитель: Орынбек Ажар Ганиевна
преподаватель
АО «Южно-Казахстанская академия медицины»
( г. Шымкент, Казахстан)

# СТРУКТУРНО-ФУНКЦИОНАЛЬНАЯ ОРГАНИЗАЦИЯ КЛЕТКИ КАК ОСНОВНОЙ ЕДИНИЦЫ ЖИВОГО ОРГАНИЗМА И ЕЁ РОЛЬ В ОБЕСПЕЧЕНИИ ЖИЗНЕДЕЯТЕЛЬНОСТИ

**Аннотация:** В данной статье рассматривается клетка как базовая структурная и функциональная единица всех живых организмов. Описывается происхождение термина «клетка», её основные компоненты, включая клеточную мембрану, цитоплазму и генетический материал. Подробно анализируются различия между прокариотическими и эукариотическими клетками, их структурные особенности, наличие или отсутствие ядра, а также органеллы, выполняющие ключевые функции жизнедеятельности. Отдельное внимание уделяется историческому аспекту открытия клетки Робертом Гуком (в 1665 году) и формированию клеточной теории Маттиаса Шлейдена и Теодора Шванна (1838–1839) Рассматриваются особенности одноклеточных и многоклеточных организмов, их классификация и эволюционное значение. Также описываются функциональные возможности клеток, такие как репликация, синтез белка, подвижность и энергетическое обеспечение. Приводятся примеры прокариотических организмов, включая бактерии и археи, а также упоминаются крупнейшие известные бактерии. Статья подчеркивает фундаментальную роль клетки в биологии и её значение как основы всех форм жизни на Земле.

**Ключевые слова:** Клетка, прокариоты, эукариоты, клеточная теория, органеллы, ядро, цитоплазма, мембрана, митохондрии, хлоропласты, биология клетки, бактерии, археи.

## Клетка и её роль в живой природе

Клетка представляет собой базовую структурную и функциональную единицу всех живых организмов, независимо от уровня их организации [1, 2]. Она является минимальной системой, способной к осуществлению жизненно важных процессов, включая обмен веществ, синтез белков, репликацию и поддержание жизнедеятельности [1]. Сам термин «клетка» происходит от латинского слова cellula, что означает «маленькая комната», что отражает её ограниченную, но функционально сложную структуру [2]. С точки зрения морфологии и физиологии, клетка состоит из нескольких ключевых компонентов. Основой является клеточная мембрана, обладающая полупроницаемыми свойствами, которая отделяет внутреннюю среду клетки от внешней.

Внутри мембраны располагается цитоплазма, содержащая генетический материал, обеспечивающий передачу наследственной информации и контроль всех клеточных процессов [1]. Большинство клеток являются микроскопическими и могут быть изучены только с использованием увеличительных приборов [2]. Особое значение имеет способность большинства клеток к репликации и синтезу белка [1, 3]. Однако существуют специализированные высокодифференцированные клетки, такие как эритроциты и гаметы, которые утратили часть этих функций в процессе специализации.

Также выделяются клетки, обладающие способностью к движению, что расширяет функциональные возможности живых систем. Согласно представленным данным, возникновение клеточных форм жизни на Земле произошло приблизительно четыре миллиарда лет назад, что подчеркивает их эволюционную древность и фундаментальность [5]. Все организмы подразделяются на две основные группы — прокариоты и эукариоты, что отражает принципиальные различия в их клеточной организации [2, 5]. Прокариоты представлены одноклеточными организмами и включают бактерии и археи. Их характерной особенностью является отсутствие мембраносвязанного ядра, при этом генетический материал локализуется в области, называемой нуклеоидом [2]. Эукариоты, напротив, могут быть как одноклеточными, так и многоклеточными организмами [2, 5]. К ним относятся протисты, растения, животные, большинство грибов и некоторые виды водорослей. Основным отличительным признаком эукариот является наличие оформленного ядра, окружённого ядерной мембраной, что обеспечивает более высокий уровень регуляции генетической информации [1]. Внутренняя организация эукариотических клеток значительно сложнее по сравнению с прокариотическими. Они содержат мембранные органеллы, такие как митохондрии, выполняющие энергетическую функцию, и хлоропласты у растений, обеспечивающие процесс фотосинтеза и синтез органических веществ [1, 3]. Наряду с этим в клетках присутствуют немембранные структуры, включая рибосомы, которые участвуют в синтезе белка и встречаются как у прокариот, так и у эукариот, что указывает на их универсальность в биологических системах [1].

Особый интерес представляет обнаружение уникальной мембранной органеллы прокариот — магнитосомы, выявленной у магнитотактических бактерий, что расширяет представления о сложности прокариотических клеток [1]. Исторически важным этапом в развитии клеточной биологии стало открытие клетки Робертом Гуком в 1665 году [5]. Позднее, в 1839 году, Маттиас Якоб Шлейден и Теодор Шванн сформулировали клеточную теорию, которая стала основой современной биологии [5]. Согласно этой теории, все организмы состоят из одной или более клеток, клетка является основной единицей структуры и функции живых организмов, а новые клетки возникают только из уже существующих [5]. Организмы в целом подразделяются на прокариоты и эукариоты, что отражает фундаментальное различие в уровне клеточной организации [2]. Прокариоты являются исключительно одноклеточными организмами, тогда как эукариоты могут существовать как в одноклеточной, так и в многоклеточной форме.

Одноклеточные эукариоты представлены, например, микроводорослями, такими как диатомовые водоросли [2]. Многоклеточные эукариоты включают животных, растения, большинство грибов и некоторые виды водорослей. В таких организмах клетки приобретают специализацию и выполняют различные функции, обеспечивая целостность организма как единой биологической системы [2]. Прокариотические

клетки, вероятно, являются наиболее ранней формой жизни на Земле [5]. Они характеризуются наличием базовых биологических процессов, включая клеточную сигнализацию, несмотря на свою простую организацию. Их структура отличается меньшими размерами и отсутствием мембранных органелл [2]. Также прокариотические клетки способны выделять различные вещества через клеточную мембрану, включая экзоферменты и внеклеточные полимерные соединения, что играет важную роль во взаимодействии с окружающей средой [2]. Размер прокариотических организмов варьируется в пределах от 0,5 до 2,0 мкм, однако существуют исключения, такие как Thiomargarita magnifica, которая достигает длины до 1–2 см и может быть видима невооружённым глазом [5].

**Список литературы:**

1. Alberts B., Johnson A., Lewis J. et al. Molecular Biology of the Cell. 6th ed. Garland Science, 2015.

2. Campbell N. A., Reece J. B. Biology. 11th ed. Pearson Education, 2017.

3. Lodish H. et al. Molecular Cell Biology. 8th ed. W. H. Freeman, 2016.

4. Cooper G. M., Hausman R. E. The Cell: A Molecular Approach. 7th ed. Sinauer Associates, 2019.

5. OpenStax College. Biology 2e. Rice University, 2018.

## ТЕХНИКАЛЫҚ ҒЫЛЫМДАР - ТЕХНИЧЕСКИЕ НАУКИ - TECHNICAL SCIENCE

**UDC 004.925**

**Yang Yuchen**

Master's student
**Scientific supervisor:** Olzhas Turar
PhD, Senior Lecturer
Department of Computer Science,
Al-Farabi Kazakh National University
(Almaty, Kazakhstan)

# GEOMETRY SHADER-BASED CORNER-POINT GRID RECONSTRUCTION FOR REAL-TIME PETROLEUM RESERVOIR VISUALIZATION ON CONSUMER GPUs

**Abstract.** The corner-point grid (CPG) format used by industrial reservoir simulators encodes subsurface geometry as irregular hexahedra whose eight corners are obtained by interpolation along inclined pillar lines. Faithful real-time visualization of CPG datasets is computationally demanding: a moderate-scale model such as the Norne ATW2013 benchmark contains tens of thousands of active cells, each requiring per-frame reconstruction. This paper presents a focused study of an OpenGL 3.3 geometry shader pipeline that performs full per-cell hexahedral reconstruction entirely on the GPU. The central contribution is a point-to-hexahedron expansion strategy in which the central processing unit submits a single GL_POINTS primitive per active cell and the geometry shader fetches eight corner depths from a texture buffer object, performs pillar interpolation, applies origin-shifted coordinates to eliminate float32 precision loss at universal transverse Mercator scale, and emits twelve triangles with correct winding order in a single shader invocation. Optional dual-axis slicing and interactive vertical exaggeration with on-the-fly normal recomputation are integrated into the same shader stage at negligible cost. On the Norne benchmark (forty-six by one-hundred-twelve by twenty-two grid; forty-four thousand four hundred thirty-one active cells) the pipeline sustains fifty-seven frames per second on a mobile NVIDIA GTX 1660 Ti Max-Q while consuming approximately five megabytes of video memory, representing a twenty-eight-fold reduction in graphics memory and an eleven-fold improvement in frame rate over a vertex-buffer baseline. The implementation requires only standard OpenGL Core Profile features and is therefore broadly portable.

**Keywords:** corner-point grid, OpenGL, geometry shader, GPU rendering, reservoir visualization, real-time graphics, ZCORN indexing, float32 precision.

**Introduction.** Three-dimensional visualization of subsurface reservoir models is a routine prerequisite for field development planning, well placement, and reservoir management. Industrial simulators such as Schlumberger ECLIPSE, CMG IMEX, and OPM Flow describe geological geometry through the GRDECL text format, in which the subsurface volume is discretized as a corner-point grid (CPG). Each grid cell in this representation is a general hexahedron whose eight corners lie on four inclined pillar lines, with depth values stored

separately in the ZCORN keyword. Unlike a Cartesian grid, a CPG faithfully encodes faulted horizons, pinch-outs, and dipping stratigraphic layers without geometric approximation, but the price is geometric irregularity: every active cell requires explicit per-corner reconstruction before it can be displayed.

At interactive frame rates this reconstruction step is non-trivial. Even the moderate-scale Norne ATW2013 benchmark, distributed publicly by the Open Porous Media initiative, contains a forty-six by one-hundred-twelve by twenty-two grid in which forty-four thousand four hundred thirty-one cells are active. A naive immediate-mode renderer that issues eight glVertex3f calls per cell submits more than one million per-frame vertex commands, a workload that saturates the central processing unit (CPU) bus while leaving the graphics processing unit (GPU) underutilized. Commercial workstation packages such as Petrel and tNavigator deliver high performance but require expensive licensing and hardware. General-purpose scientific visualization frameworks such as VTK and ParaView lack native CPG support, while ResInsight, the most widely used open-source reservoir viewer, depends on a heavy software stack that obscures the rendering core and resists customization on consumer-grade laptops.

The OpenGL geometry shader (GS) stage, available since version 3.2 of the OpenGL Core Profile, allows a single input primitive to be amplified into a controlled number of output primitives entirely on the GPU. This capability is uniquely well suited to CPG visualization, because each cell can be represented on the host as a single point and reconstructed into a complete six-faced hexahedron by the shader. The present work develops this idea into a fully optimized rendering pipeline and reports a focused technical analysis of the geometric, numerical, and memory aspects of the implementation. The contributions of this paper are summarized as follows. (1) A complete description of a point-to-hexahedron expansion algorithm in GLSL that performs ZCORN indexing, pillar interpolation, and per-face normal computation in a single geometry shader invocation. (2) A documented solution to the float32 precision problem that arises when CPG coordinates are expressed in the Universal Transverse Mercator (UTM) system, achieved through a CPU-side origin shift. (3) An on-shader implementation of vertical exaggeration that recomputes face normals in the deformed coordinate frame, preserving correct lighting under interactive depth scaling. (4) A quantitative evaluation on the Norne benchmark demonstrating a twenty-eight-fold reduction in graphics memory and an eleven-fold improvement in frame rate over a baseline vertex-buffer renderer.

The remainder of this paper is organized as follows. Section 2 reviews the structure of the GRDECL data and the geometry shader stage. Section 3 presents the three-stage architectural progression that motivated the proposed pipeline. Section 4 describes the GPU data layout, and Section 5 details the geometry shader algorithm itself. Section 6 reports experimental results on the Norne benchmark. Section 7 discusses limitations and applicability, and Section 8 concludes.

**Background and related work.** A GRDECL file describes a structured (i, j, k) grid through three principal keywords. SPECGRID specifies the grid dimensions nx, ny, and nz. COORD stores six floating-point numbers per pillar line, namely the (x, y, z) coordinates of the top and bottom endpoints of the line; for a grid of nx by ny cells in the lateral plane there are (nx+1) by (ny+1) such pillars. ZCORN stores the depth values of all eight corners of every cell in a one-dimensional array indexed by the standard ECLIPSE convention; the array length is eight times nx times ny times nz. Finally, ACTNUM is an integer mask that flags inactive cells, typically those falling outside the reservoir volume. Reconstructing a single cell therefore

requires reading eight depth values from ZCORN, evaluating four pillar interpolations to obtain (x, y) at the requested depths, and assembling the eight corners in the correct topological order.

Existing approaches to interactive CPG rendering fall into three broad categories. The first approximates each cell as an axis-aligned cube placed at the cell centroid. This representation is fast to render with hardware instancing but produces visible artifacts at faulted horizons, where adjacent cells should share corner points but instead expose gaps and overlaps. The second pre-computes the full set of triangular faces for every cell on the CPU and stores them in a vertex buffer object (VBO). This approach renders correctly but consumes large amounts of video memory: at twelve triangles per cell, three vertices per triangle, and ten floats per vertex, the Norne dataset alone requires more than fifty megabytes of GPU memory for static geometry. The third category, into which the present work falls, performs cell reconstruction on the GPU within the geometry shader stage. Earlier examples in geological visualization include the GPU isosurface and slice algorithms developed for seismic volumes, but a complete CPG implementation that addresses the float32 precision problem at UTM scale and supports interactive vertical exaggeration with correct lighting has not, to the authors knowledge, been described in detail in the open literature.

**Three-stage architectural progression.** The proposed pipeline was developed through three architectural iterations, each addressing a specific bottleneck encountered in the previous stage. Stage 1 used legacy fixed-function OpenGL with immediate mode glBegin/glEnd vertex submission. Although correct, this approach was incapable of sustaining interactive rates on the Norne dataset and was rejected. Stage 2 replaced immediate mode with hardware-instanced cube rendering. By submitting a single canonical cube and instancing it forty-four thousand four hundred thirty-one times, the per-frame draw-call cost was eliminated and frame rates above fifty-five frames per second were achieved. The geometric approximation, however, distorted faulted layers and was unsuitable for production interpretation. Stage 3, the focus of this paper, retains the single-draw-call performance characteristic of instancing but reconstructs the true CPG hexahedron geometry within the geometry shader. The result is correct geometry at instancing-level performance.

The Stage 3 pipeline is organized into four GPU stages. The vertex shader receives one seed vertex per active cell and forwards the cell index and a normalized scalar attribute (typically porosity or permeability) without modification. The geometry shader expands each input point into the six bounding faces of the cell, emitting twelve triangles arranged as triangle strips with counter-clockwise winding for correct hardware back-face culling. The fragment shader applies a three-point lighting model (ambient plus key plus fill) and maps the interpolated attribute through a rainbow transfer function. Finally, depth testing with polygon-offset bias is applied to suppress z-fighting artifacts on co-planar faces.

**GPU data layout.** The host-side data preparation is performed once at load time. The GRDECL parser reads COORD, ZCORN, ACTNUM, and one or more attribute arrays into NumPy arrays of explicit dtype. To circumvent the float32 precision limitation discussed in Section 5.3, an origin offset is computed as the centroid of the model bounding box and subtracted from all (x, y, z) coordinates before they are uploaded to the GPU. Three independent buffers are then constructed.

The seed VBO contains one record per active cell with a stride of twenty bytes. The first three floats encode the (i, j, k) cell index cast to single-precision floating point for shader compatibility; the fourth float carries the normalized scalar attribute in the range zero to one;

and the fifth float is reserved for future use. For the Norne benchmark this VBO occupies forty-four thousand four hundred thirty-one times twenty bytes, approximately 0.85 megabytes. The COORD data is uploaded into a texture buffer object (TBO) of dimension (nx+1) times (ny+1) times six floats, occupying about 0.13 megabytes. The ZCORN data is uploaded as a second TBO of dimension eight times nx times ny times nz floats, requiring about 3.5 megabytes for Norne. The total static GPU memory footprint, including small uniform buffers for the colormap and lighting parameters, is under five megabytes — to be contrasted with the more than fifty megabytes required by the precomputed-triangle baseline of the previous section. The compression factor is approximately twenty-eight, and is achieved without any algorithmic loss of geometric fidelity.

**Table 1 — GPU memory footprint comparison on the Norne benchmark**

| Approach | VRAM (MB) | Draw calls | FPS |
|---|---|---|---|
| Stage 1: immediate mode | < 1 | 1.07 M | ~ 5 |
| Stage 2: instanced cubes | ~ 50 | 1 | ~ 55 |
| Stage 3: GS expansion (this work) | ~ 5 | 1 | 57 |

**Geometry shader algorithm.**

**5.1 ZCORN index resolution.** The eight corners of cell (i, j, k) are addressed in the ZCORN array by an index function that treats the array as a three-dimensional grid of dimension (2nz, 2ny, 2nx). For a corner specified by half-cell flags (hk, hj, hi), each in the set zero, one, the linear index is given by

$$idx(i, j, k, hk, hj, hi) = (2k + hk)\cdot(4\ nx\ ny) + (2j + hj)\cdot(2\ nx) + (2i + hi).$$

Implemented in GLSL via the texelFetch operation against the ZCORN texture buffer, this lookup costs eight texture fetches per cell. The half-cell flag combinations enumerate the eight corners in a fixed topological order: (hk, hj, hi) = (0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1), corresponding respectively to top-back-left, top-back-right, top-front-left, top-front-right, bottom-back-left, bottom-back-right, bottom-front-left, and bottom-front-right.

**5.2 Pillar interpolation.** Each ZCORN value provides only the depth z of a corner; the lateral coordinates (x, y) must be obtained by linear interpolation along the appropriate pillar line. For a pillar with top point (xt, yt, zt) and bottom point (xb, yb, zb), the interpolation parameter at depth z is t = (z − zt) / (zb − zt). The corresponding lateral coordinates are x = xt + t·(xb − xt) and y = yt + t·(yb − yt). When the pillar is exactly vertical, that is when zb equals zt, the parameter t is undefined; in this case the shader returns the top-point coordinates. The pillar identification for corner (hi, hj) of cell (i, j, k) follows the same regular pattern as the ZCORN flags: the pillar index is (i + hi, j + hj). Four pillar interpolations therefore suffice to reconstruct all eight corners of a cell.

**5.3 Origin shift for float32 precision.** Geological coordinates in industrial datasets are routinely stored in the Universal Transverse Mercator system. For the Norne field, situated in UTM Zone 32N, easting and northing values typically lie around four hundred fifty-six thousand and seven million three hundred twenty-one thousand metres respectively. A single-precision IEEE 754 float provides approximately seven significant decimal digits, which at this magnitude

corresponds to a least significant bit of about one metre. Since CPG cells in Norne have lateral extents of fifty to one hundred metres and vertical extents as small as one metre, direct float32 storage produces visible vertex jitter and discrete-step artifacts during camera motion. The pipeline addresses this through a CPU-side origin shift: the bounding-box centroid (x0, y0, z0) is subtracted from every coordinate before upload, so that the shader operates on values centred on the origin and bounded in magnitude by the grid extents. The shift is reversed in the projection matrix when an absolute coordinate display is required. The technique introduces no shader-side overhead and entirely eliminates the precision artifact.

**5.4 Vertical exaggeration with normal recomputation.** Reservoir engineers routinely apply a vertical exaggeration factor between five and twenty to highlight stratigraphic features that would otherwise be visually compressed by the large lateral-to-vertical aspect ratio of typical fields. In the proposed pipeline this scaling is applied within the geometry shader by multiplying the z-component of every reconstructed corner by a uniform variable verticalScale before primitive emission. A subtle but important consequence is that the surface normals of the cell faces, if precomputed in the unscaled frame, no longer correspond to the actual surface orientation after deformation, producing visibly incorrect lighting. The shader therefore recomputes normals after scaling using the cross product of two edge vectors of each face, ensuring that the lighting model receives the deformed-frame normal. This recomputation costs four cross products per cell and has no measurable impact on frame rate, but is essential for visual correctness under interactive scaling.

**5.5 Dual-axis cross-section slicing.** Cross-section slicing along the I and K grid axes is implemented as two early-exit tests at the start of the geometry shader. The shader receives two uniform integers, sliceI and sliceK, that specify the cut indices, and a third uniform that selects either include-below or include-above semantics. Cells failing the test return without emitting any primitives. Because the test occurs before any pillar interpolation, the entire cost of geometric reconstruction is avoided for clipped cells; for the Norne dataset, slicing typically discards forty to sixty per cent of the active cells and yields a measurable improvement in frame rate.

**5.6 Face emission and winding order.** Once the eight corners are reconstructed, the shader emits the six bounding faces as triangle strips. Each face is described by four corner indices in counter-clockwise order as seen from outside the cell; the geometry shader emits the four corresponding vertices and a primitive-end marker. The total per-cell output budget is fixed at twenty-four vertices (six faces times four corners) and twelve triangles. This count is below the conservative GS amplification limit on all consumer GPU architectures since OpenGL 3.2 and therefore does not trigger driver-level fallbacks. Hardware back-face culling, enabled by the consistent winding convention, eliminates approximately half of the resulting fragments before rasterization.

**Experimental evaluation.** All measurements were performed on a Dell G3 3590 laptop equipped with an Intel Core i7-9750H CPU, sixteen gigabytes of system memory, and an NVIDIA GeForce GTX 1660 Ti Max-Q discrete GPU. The operating system was Windows 10 with NVIDIA driver version 537.13. The benchmark dataset is the Norne ATW2013 model from the Open Porous Media initiative, containing a forty-six by one-hundred-twelve by twenty-two CPG (one hundred thirteen thousand three hundred forty-four total cells, of which forty-four thousand four hundred thirty-one are active per the ACTNUM mask). The implementation

uses Python 3.11, PyOpenGL, GLFW, and NumPy, and consists of approximately twenty-one hundred lines of Python and GLSL code in total.

Frame rates were measured by averaging over a one-thousand-frame test sequence with the camera orbiting the model at a fixed radius. Three configurations were evaluated. The legacy immediate-mode baseline (Stage 1) sustained approximately five frames per second; this rate is bounded by the CPU draw-submission rate rather than by GPU rasterization. The instanced-cube baseline (Stage 2), which approximates each cell as a unit cube, reached fifty-five frames per second but produces visibly incorrect geometry at faulted horizons. The proposed Stage 3 pipeline achieved fifty-seven frames per second with full corner-point reconstruction. Importantly, Stage 3 matches the performance of the geometrically incorrect Stage 2 baseline while delivering accurate geometry; the additional cost of pillar interpolation and ZCORN lookups in the geometry shader is masked by the reduction in primitive count that results from per-cell hexahedron emission rather than per-corner cube instancing. Table 1 summarizes the comparison.

GPU memory consumption was measured via the GL_NVX_gpu_memory_info extension. The Stage 3 pipeline reserved approximately five megabytes of GPU memory for the seed VBO, the COORD TBO, and the ZCORN TBO combined. A static-vertex-buffer baseline that pre-computes all twelve triangles per active cell on the CPU consumed approximately one hundred forty-four megabytes for the same dataset, a factor of twenty-eight higher. The memory advantage scales with the number of cells: for hypothetical models in the millions of cells the proposed pipeline remains within consumer-laptop GPU memory budgets, while the static-vertex-buffer baseline would exceed them by an order of magnitude.

Profiling under NVIDIA Nsight Graphics indicates that the geometry shader stage is the dominant cost in the Stage 3 pipeline, accounting for approximately sixty per cent of GPU time per frame, followed by fragment shading at thirty per cent and other stages at ten per cent. The geometry shader cost is dominated by texelFetch latency against the ZCORN TBO, suggesting that a future optimization could amortize this cost through a small per-cell on-shader cache or through reformulation as a compute-shader prepass that writes triangulated geometry to a buffer-object output. These directions are the subject of ongoing work.

**Discussion.** The geometry shader stage has historically been criticized as offering inferior throughput compared with hardware tessellation or compute shaders, particularly on certain mobile GPU architectures. The present results indicate that for the specific class of single-amplification CPG reconstruction (one input point producing twenty-four output vertices) the geometry shader remains competitive on consumer NVIDIA hardware, and provides the additional benefits of per-cell flow control (used here for slicing) and trivial integration with downstream fragment-stage features such as colormap lookups and lighting. Compute-shader-based alternatives that pre-compute the full triangle stream into a vertex buffer on demand would likely match or exceed Stage 3 performance for static models, but would forfeit the on-shader interactivity (slicing, vertical exaggeration, and per-cell culling) that the geometry shader formulation enables at zero additional CPU cost.

Limitations of the proposed pipeline are recognized. First, the geometry shader amplification limit, while comfortable on the studied dataset, would constrain extension to certain higher-order cell shapes. Second, the per-cell texelFetch pattern against the ZCORN TBO is not cache-friendly; on architectures without a unified texture cache (notably some

integrated GPUs) the pipeline may exhibit lower scaling efficiency. Third, the present implementation targets a single GPU and a single rendering thread. For multi-million-cell models, hierarchical level-of-detail strategies and out-of-core data streaming would become necessary; these directions are outside the scope of the present technical study.

**Conclusion.** This paper has presented a focused technical study of a geometry shader pipeline for real-time visualization of corner-point grid reservoir models. The pipeline combines a point-to-hexahedron expansion strategy, a CPU-side origin shift to circumvent float32 precision loss at UTM scale, and on-shader vertical exaggeration with normal recomputation. On the Norne ATW2013 benchmark the implementation sustains fifty-seven frames per second on a consumer mobile GPU while consuming under five megabytes of graphics memory, representing a twenty-eight-fold reduction in memory and an eleven-fold improvement in frame rate over a static-vertex-buffer baseline. The complete implementation uses only standard OpenGL Core Profile features and is therefore portable across desktop GPU vendors. Future work will investigate compute-shader alternatives, hierarchical level-of-detail strategies for million-cell models, and integration with stereoscopic virtual reality output.

**References:**

1. Aziz K., Settari A. Petroleum Reservoir Simulation. London: Applied Science Publishers, 1979. 476 p.

2. Ponting D. K. Corner Point Geometry in Reservoir Simulation // Proceedings of the 1st European Conference on the Mathematics of Oil Recovery. Cambridge, 1989. P. 45–65.

3. Ringrose P., Bentley M. Reservoir Model Design: A Practitioner’s Guide. 2nd ed. Dordrecht: Springer, 2015. 249 p.

4. Shreiner D., Sellers G., Kessenich J., Licea-Kane B. OpenGL Programming Guide: The Official Guide to Learning OpenGL, Version 4.5 with SPIR-V. 9th ed. Boston: Addison-Wesley, 2017. 968 p.

5. Bailey M., Cunningham S. Graphics Shaders: Theory and Practice. 2nd ed. Boca Raton: CRC Press, 2011. 518 p.

6. Akenine-Möller T., Haines E., Hoffman N. Real-Time Rendering. 4th ed. Boca Raton: CRC Press, 2018. 1198 p.

7. Open Porous Media Initiative. The Norne ATW2013 Benchmark Dataset [Electronic resource]. URL: https://opm-project.org/?page_id=559 (accessed: 28.04.2026).

8. Rwechungura R. W., Suwartadi E., Dadashpour M., Kleppe J., Foss B. A. The Norne Field Case — A Unique Comparative Case Study // SPE Intelligent Energy Conference and Exhibition. SPE-127538-MS. 2010.

9. Schroeder W., Martin K., Lorensen B. The Visualization Toolkit: An Object-Oriented Approach to 3D Graphics. 4th ed. Kitware, 2006. 528 p.

10. Goldman R. An Integrated Introduction to Computer Graphics and Geometric Modeling. Boca Raton: CRC Press, 2009. 574 p.

11. Segal M., Akeley K. The OpenGL Graphics System: A Specification (Version 3.3 Core Profile). The Khronos Group, 2010. 322 p.

12. Goldberg D. What Every Computer Scientist Should Know About Floating-Point Arithmetic // ACM Computing Surveys. 1991. Vol. 23, No. 1. P. 5–48.

**УДК 004.942**

**Айтжанова Аяжан Кайратовна**

Магистрант 2 курса
Школа искусственного интеллекта и науки о данных
Astana IT Unibersity
(г. Астана, Казахстан)

# АНАЛИЗ И ПРОГНОЗ ПОТРЕБНОСТИ В ПРЕСНОЙ ВОДЕ В УСЛОВИЯХ РК НА ОСНОВЕ ПОГОДНЫХ ДАННЫХ И ПОКАЗАТЕЛЕЙ ПОТРЕБЛЕНИЯ

**Аннотация:** В условиях изменения климата и роста антропогенной нагрузки проблема рационального управления водными ресурсами приобретает стратегическое значение для Республики Казахстан. Целью настоящего исследования является разработка и сравнительный анализ моделей прогнозирования потребности в пресной воде на основе погодных данных и показателей потребления. В работе использованы методы эконометрического моделирования и алгоритмы машинного обучения, включая Ridge Regression, Random Forest, Support Vector Regression, Gaussian Process Regression и XGBoost. Результаты показали, что ансамблевые нелинейные методы обеспечивают наибольшую точность прогнозирования ($R^2$ до 0.97, MAPE < 9%). Построен прогноз совокупного водопотребления до 2030 года, подтверждающий устойчивый рост спроса на водные ресурсы. Полученные выводы могут быть использованы при формировании государственной политики в сфере водного управления и адаптации к климатическим изменениям.

**Ключевые слова:** водные ресурсы, Казахстан, водопотребление, машинное обучение, XGBoost, Random Forest, климатические данные, прогнозирование.

**Введение.** Водные ресурсы являются стратегически важным элементом устойчивого развития Казахстана, особенно в условиях изменения климата и роста потребностей различных отраслей экономики. Эффективное управление водными ресурсами требует точного анализа текущего состояния водопотребления и прогнозирования будущих потребностей, что является ключевой задачей для обеспечения водной безопасности страны.

По данным национальной статистики и международных организаций, объём возобновляемых водных ресурсов Казахстана составляет около 100–108 км³ в год, при этом до 45% формируется за пределами страны. Учитывая рост населения, расширение сельскохозяйственного производства и промышленного сектора, прогнозирование будущего спроса на воду становится необходимым инструментом стратегического планирования.

Настоящее исследование посвящено анализу и прогнозированию потребности в пресной воде в Республике Казахстан на основе климатических данных и показателей водопотребления. В работе рассматриваются методы прогнозирования водопотребления, включая статистические модели и алгоритмы машинного обучения.

Основной целью исследования является разработка модели прогнозирования потребности в пресной воде, учитывающей погодные данные и показатели потребления по регионам Казахстана. В рамках исследования решаются следующие задачи:

- Анализ существующих методов прогнозирования потребности в водных ресурсах
- Сбор и обработка данных по водопотреблению и климатическим изменениям в Казахстане
- Разработка прогнозной модели с использованием методов машинного обучения
- Сравнение различных моделей прогнозирования и оценка их точности

Ожидается, что результаты исследования будут полезны государственным органам, занимающимся управлением водными ресурсами, а также предприятиям аграрного и промышленного секторов, заинтересованным в эффективном планировании водопользования

**Актуальность.** Рост населения, развитие промышленности и изменение климата ведут к увеличению потребности в пресной воде, делая вопрос ее рационального использования все более значимым. Казахстан, обладая значительными, но неравномерно распределенными водными ресурсами, уже сталкивается с проблемами их дефицита. По данным Бюро национальной статистики, объем ежедневно потребляемой воды на одного жителя страны в 2023 году составил 3,5 тыс. литров. В то же время исследования Всемирного банка показывают, что если текущие тенденции сохранятся, объем доступных водных ресурсов Казахстана может сократиться с 100 до 70 кубических километров к 2050 году.

По прогнозам экспертов ПРООН, уже к 2040 году дефицит водных ресурсов в Казахстане может составить 50% от общей потребности. Это негативно скажется на всех секторах экономики, а в ряде регионов может привести к снижению ВВП на 6% к 2050 году.

Таким образом, необходимость исследования механизмов прогнозирования и оптимизации водопотребления становится очевидной. В данной работе особое внимание будет уделено комплексному анализу данных о потреблении воды, климатических изменениях и водном балансе. В Казахстане, где водные ресурсы ограничены и распределены неравномерно, особенно важно использовать современные методы прогнозирования, чтобы предотвратить кризисное развитие ситуации.

**Современные модели машинного обучения, применяемые для анализа и прогноза водопотребления**

В последние годы методы машинного обучения существенно расширили возможности прогнозирования водопотребления, обеспечивая более высокую точность по сравнению с традиционными подходами. В исследованиях, проведённых в Австрии, Китае и странах ЕС, активно применяются как интерпретируемые модели (Linear Regression, Decision Tree, KNN), так и более сложные алгоритмы (SVM, Random Forest, LSTM).

В работе Maußner et al. (2025) были сравнены шесть моделей для прогнозирования суточного водопотребления с учётом точности, интерпретируемости и устойчивости к климатическим сценариям[1]. Нелинейные модели, такие как LSTM и Random Forest, показали более высокую точность, однако оказались чувствительнее к качеству входных

данных. Более простые модели продемонстрировали большую устойчивость и прозрачность. Кроме того, Random Forest показал стабильные результаты и может быть дополнительно усилен бустинговыми алгоритмами, такими как XGBoost (Niazkar et al., 2024).

В исследовании Xia et al. (2024) предложена гибридная модель GA-BP-KDE, сочетающая точечный прогноз и оценку неопределённости. На первом этапе использовались нейронные сети и модели машинного обучения, оптимизированные метаэвристическими алгоритмами (GA, PSO, GWO), а на втором — метод Kernel Density Estimation для формирования доверительных интервалов[2]. Модель показала высокую точность и позволила учитывать асимметрию ошибок, что особенно важно при стратегическом планировании в условиях ограниченных водных ресурсов. Авторы подчёркивают значимость корректного выбора климатических переменных (температура, осадки, влажность), что повышает устойчивость прогноза. Возможность построения интервальных, а не только точечных оценок снижает неопределённость управленческих решений.

Таким образом, современные исследования подтверждают эффективность гибридных моделей машинного обучения и методов оценки неопределённости для прогнозирования водопотребления. Подобные подходы могут быть адаптированы к условиям Казахстана с учётом его климатических и социально-экономических особенностей.

**Интеграция климатических данных в модели прогнозирования**

Климатические переменные — температура, осадки и влажность — являются ключевыми факторами в моделях прогнозирования водопотребления. В исследовании X. Zhang et al. (2024) анализируется динамика водоснабжения в условиях полузасушливого климата на примере города Циньян (Китай), что близко по условиям к южным и западным регионам Казахстана[3]. Прогноз строился с использованием сценариев Shared Socioeconomic Pathways (SSP) и алгоритма Random Forest, который позволил учитывать сложные нелинейные связи между климатическими и социально-экономическими факторами.

Авторы выделили секторальную структуру спроса (сельское хозяйство, промышленность, бытовой и экологический сектор) и показали рост потребления прежде всего в аграрной сфере. Использование климатических сценариев SSP126, SSP245 и SSP585 позволило учесть влияние изменения климата на водный баланс. Подобный подход может быть применён в аграрных и энергетических регионах Казахстана для более устойчивого планирования распределения водных ресурсов.

Аналогичные выводы подтверждаются и другими исследованиями. В австрийской работе использовалась множественная линейная регрессия (MLR) с учётом климатических сценариев RCP, где прогнозируется рост пикового водопотребления на 14–19% к середине века, главным образом из-за демографических факторов. В ряде стран (Сербия, Эфиопия, Канада) установлено, что повышение температуры на 1°C может увеличить пиковое потребление воды на 1.8–2%.Помимо линейных моделей, широко применяются нейронные сети (ANN), SVR и Random Forest, повышающие точность прогнозов. Однако исследования показывают, что при корректном выборе переменных даже простые регрессионные модели могут обеспечивать сопоставимые результаты.

Для Казахстана, особенно в засушливых и резко континентальных регионах, перспективен комплексный подход к прогнозированию водопотребления, аналогичный австрийскому. Климатическая нестабильность, сокращение поверхностных и подземных вод, а также демографический рост требуют разработки адаптированных региональных моделей. Методологически такие модели должны опираться на исторические данные потребления и погоды, учитывать климатические индексы и демографические прогнозы, применять сценарный анализ и оцениваться с использованием MAPE, корреляции Пирсона и анализа пикового спроса. Важно также интегрировать прогнозы в систему управления водоснабжением для корректировки тарифной политики, планирования инфраструктуры и внедрения мер водосбережения.

Исследование Shu et al. (2024) сравнило пять моделей ИИ (GA-BP, ELM, GPR, SVR, Random Forest) для прогноза водопотребления в четырёх секторах[4]. Модели обучались на данных 2005–2020 гг., оценивались по $R^2$, RMSE и MAPE и использовались для прогноза до 2025 года. GPR показал наилучшие результаты для сельского, бытового и экологического сектора ($R^2$ до 0.98), тогда как GA-BP оказался наиболее эффективен для промышленности. Все алгоритмы продемонстрировали устойчивость к небольшим выборкам и пропускам данных, а прогнозы указали на рост потребления во всех секторах.

Для Казахстана такие методы особенно ценны с учётом региональных различий и климатической неопределённости. Модели GPR и SVR позволяют учитывать риски и демографические колебания, а секторный подход обеспечивает более точное распределение ресурсов, особенно в засушливых аграрных областях. Интеграция ИИ-моделей в государственную систему управления водными ресурсами может повысить точность прогнозирования и улучшить стратегическое планирование в условиях изменения климата.

**Методология.** Настоящее исследование основано на комплексном анализе климатических данных, собранных на территории Республики Казахстан за последние два десятилетия и показателей потребления. Для анализа были использована метеорологическая база данных РГП «Казгидромет», содержащая ежедневные наблюдения по 228 метеостанциям; Данные охватывают период с 2000 года по настоящее время[8].

В ходе работы были собраны ежедневные наблюдения с 2000 года по настоящее время по 228 метеостанциям, расположенным на территории всех регионов Республики Казахстан. Для каждой станции были выгружены следующие ключевые климатические показатели: среднесуточная температура воздуха (°C), Суточное количество атмосферных осадков (мм), относительная суточная влажность воздуха (%)

Все данные были получены в ежедневном разрезе и объединены в единый формат, включающий название станции, регион, дату наблюдения и значения измеряемых параметров.

Помимо метеорологических наблюдений был выполнен сбор данных по потреблению воды были получены из закрытого источника Бюро национальной статистики Агентства по стратегическому планированию и реформам Республики Казахстан (портал открытых данных data.egov.kz): https://data.egov.kz/datasets/view?index=water_dispensed_to_consumers[13].

Набор данных содержит статистическую информацию о распределении воды потребителям в разрезе территорий и временных периодов. Структура датасета

представлена следующими атрибутами: наименование территории, период, объем потребления воды, вид местности (сельская/городская), категория потребления.

После завершения этапа парсинга климатические данные представляли собой разрозненные таблицы, выгруженные по годам и по станциям наблюдений. Была выполнена комплексная предобработка набора данных с целью приведения информации к единому стандарту и подготовки к последующему анализу и построению моделей прогнозирования. В процессе очистки данные значительно сократились за счёт удаления пустых, некорректных и дублирующих наблюдений.

После выполнения всех этапов предобработки был сформирован единый очищенный массив данных, включающий:

- период наблюдений: с 2000 года по настоящее время (более 25 лет);
- количество станций: 228 meteorological and hydrological stations;
- параметры: суточная температура воздуха, суточные атмосферные осадки, суточная относительная влажность воздуха, суточный уровень воды в реках, объем потребления, регион, тип местности(сельская,городская), код КАТО (Классификатор административно-территориальных объектов);
- общий объём: около 2,7 миллиона строк наблюдений.

**Эконометрическое моделирование и базовая оценка зависимостей**

Первым этапом моделирования стало построение эконометрической модели панельной регрессии с фиксированными эффектами. Использование данной модели обусловлено необходимостью выявления устойчивых зависимостей между климатическими факторами и уровнем водопотребления с учётом региональной специфики и временных трендов. Включение фиксированных эффектов регионов позволило учесть неизменяемые во времени особенности территорий, такие как уровень инфраструктуры водоснабжения, структура экономики и демографические характеристики. Введение фиксированных эффектов года позволило учесть макроэкономические и климатические тенденции, оказывающие влияние на водопотребление на национальном уровне.

PanelOLS Estimation Summary

| | | | |
|---|---|---|---|
| Dep. Variable: | consumption | R-squared: | 0.1762 |
| Estimator: | PanelOLS | R-squared (Between): | 0.0273 |
| No. Observations: | 180 | R-squared (Within): | 0.0674 |
| Date: | Tue, Feb 17 2026 | R-squared (Overall): | 0.0102 |
| Time: | 01:34:57 | Log-likelihood | -3516.5 |
| Cov. Estimator: | Clustered | | |
| | | F-statistic: | 3.8237 |
| Entities: | 21 | P-value | 0.0004 |
| Avg Obs: | 8.5714 | Distribution: | F(8,143) |
| Min Obs: | 2.0000 | | |
| Max Obs: | 9.0000 | F-statistic (robust): | 16.350 |
| | | P-value | 0.0000 |
| Time periods: | 9 | Distribution: | F(8,143) |
| Avg Obs: | 20.000 | | |
| Min Obs: | 20.000 | | |
| Max Obs: | 20.000 | | |

Parameter Estimates

| | Parameter | Std. Err. | T-stat | P-value | Lower CI | Upper CI |
|---|---|---|---|---|---|---|
| rain_year | -2.761e+04 | 1.198e+04 | -2.3042 | 0.0227 | -5.13e+04 | -3924.4 |
| hum_mean | 4.267e+06 | 8.895e+06 | 0.4797 | 0.6322 | -1.332e+07 | 2.185e+07 |
| hum_min | 2.036e+07 | 1.181e+07 | 1.7244 | 0.0868 | -2.979e+06 | 4.37e+07 |
| temp_mean | -1.326e+07 | 1.873e+07 | -0.7076 | 0.4803 | -5.029e+07 | 2.378e+07 |
| temp_max | -4.079e+06 | 7.01e+06 | -0.5818 | 0.5616 | -1.793e+07 | 9.778e+06 |
| temp_min | 9.389e+05 | 5.05e+06 | 0.1859 | 0.8528 | -9.044e+06 | 1.092e+07 |
| days_obs | 1.804e+05 | 1.372e+05 | 1.3143 | 0.1908 | -9.089e+04 | 4.516e+05 |
| allowance_mean | 5.294e+08 | 7.326e+07 | 7.2264 | 0.0000 | 3.846e+08 | 6.742e+08 |

Рисунок 1. Результаты оценки панельной регрессии (PanelOLS) для модели водопотребления

Результаты панельной регрессии (Рисунок 1) подтвердили наличие статистически значимой зависимости между погодными параметрами и уровнем водопотребления. В частности, наблюдалась положительная связь между ростом температуры воздуха и увеличением объёмов потребляемой воды, что согласуется с теоретическими предположениями о влиянии испарения и роста бытового спроса в тёплые периоды. Количество осадков, напротив, демонстрировало отрицательную зависимость с водопотреблением, что объясняется снижением потребности в ирригации при повышенном естественном увлажнении.

Несмотря на интерпретируемость результатов, эконометрическая модель показала ограниченную способность учитывать сложные нелинейные зависимости, что обусловило переход к методам машинного обучения.

**Логарифмическая регрессионная модель Ridge Regression**

Следующим этапом исследования стало построение линейной модели Ridge Regression, применённой к логарифмированным значениям водопотребления. Использование логарифмического преобразования позволило стабилизировать дисперсию временного ряда и уменьшить влияние экстремальных значений, характерных для гидрологических данных.

Регуляризация, применяемая в модели Ridge, позволила уменьшить эффект мультиколлинеарности между климатическими переменными и повысить устойчивость модели к переобучению. По сравнению с базовой эконометрической моделью наблюдалось заметное улучшение качества прогнозирования, что подтвердило целесообразность перехода к более сложным алгоритмам.

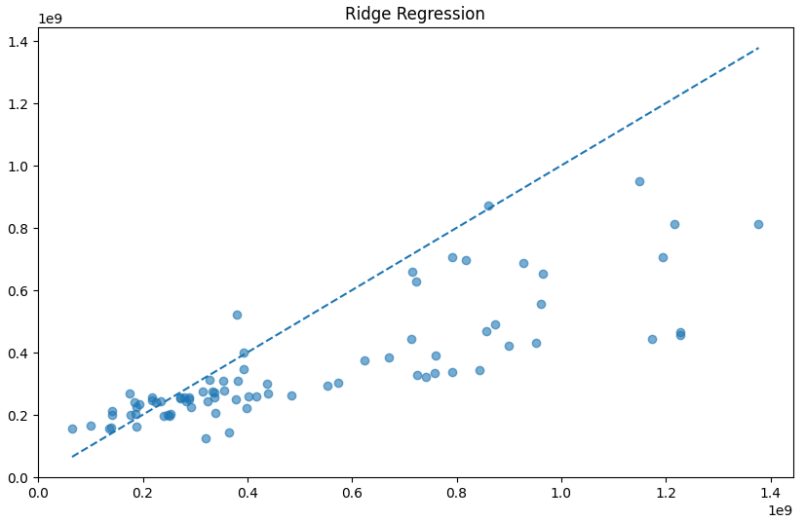



Рисунок 2. График сравнения фактических и прогнозных значений водопотребления (модель Ridge Regression)

На графике наблюдается способность модели корректно воспроизводить общий тренд водопотребления, однако в периоды резких изменений наблюдаются отклонения прогнозных значений.

**Применение нелинейных алгоритмов машинного обучения**

Основной этап моделирования был связан с применением алгоритмов машинного обучения, способных учитывать нелинейные зависимости и сложные взаимодействия факторов. В рамках исследования были реализованы модели Random Forest, Support

Vector Regression, Gaussian Process Regression (GPR) и XGBoost, что позволило провести сравнительный анализ эффективности различных подходов.

Ансамблевые методы продемонстрировали существенное повышение точности прогнозирования по сравнению с линейными моделями. Это объясняется их способностью выявлять сложные закономерности в многомерных данных и устойчивостью к шуму и пропущенным значениям.

Модель Random Forest Regression стала первым нелинейным алгоритмом, использованным в работе. Random Forest представляет собой ансамбль деревьев решений, обучаемых на случайных подвыборках данных, что обеспечивает высокую устойчивость модели и способность учитывать сложные зависимости между переменными.

Результаты показали значительное повышение точности прогнозирования по сравнению с линейными моделями. Модель Random Forest продемонстрировала наилучшие результаты по всем ключевым метрикам. Значение MAPE составило 8.33%, что соответствует точности прогноза 91.67%. Коэффициент детерминации $R^2$ равен 0.9549, что свидетельствует о высокой степени объяснения вариации зависимой переменной. Минимальное значение RMSE также подтверждает устойчивость модели и ее способность формировать прогнозы с наименьшим среднеквадратичным отклонением.

Высокие показатели объясняются ансамблевой природой алгоритма. Random Forest строит множество деревьев решений и агрегирует их результаты, что позволяет эффективно моделировать сложные нелинейные зависимости и снижать влияние выбросов и шумов в данных.

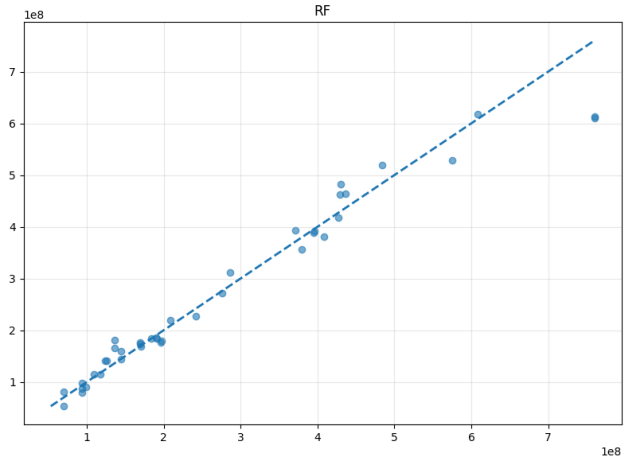



Рисунок 3. График сравнения фактических и прогнозных значений водопотребления (модель Random Forest)

Наиболее значимыми факторами прогнозирования оказались лаговые переменные водопотребления, температура воздуха и норматив водопотребления.

Метод Support Vector Regression (SVR) был использован для моделирования сложных нелинейных зависимостей между переменными. Использование ядровых функций позволило аппроксимировать нелинейную зависимость водопотребления от климатических факторов.

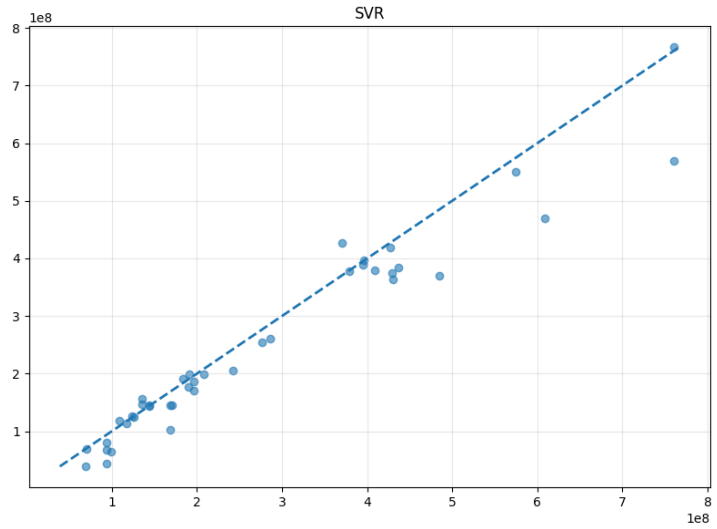



Рисунок 4. График сравнения фактических и прогнозных значений водопотребления (модель Support Vector Regression)

Модель SVR показала умеренные результаты. Средняя абсолютная процентная ошибка составила 12.41%, что заметно выше по сравнению с Random Forest. Коэффициент детерминации $R^2$ равен 0.9259, что указывает на достаточно хорошую, но менее высокую объясняющую способность.

SVR чувствителен к выбору ядра и настройке гиперпараметров. При большом масштабе данных и значительной вариативности целевой переменной модель может демонстрировать менее стабильные результаты без тщательной калибровки параметров.

Модель GPR показала более высокие значения RMSE и более низкий коэффициент детерминации (0.9000). Несмотря на теоретическую способность точно моделировать нелинейные процессы и учитывать неопределенность прогноза, на практике при работе с большими значениями целевой переменной наблюдается увеличение дисперсии предсказаний.

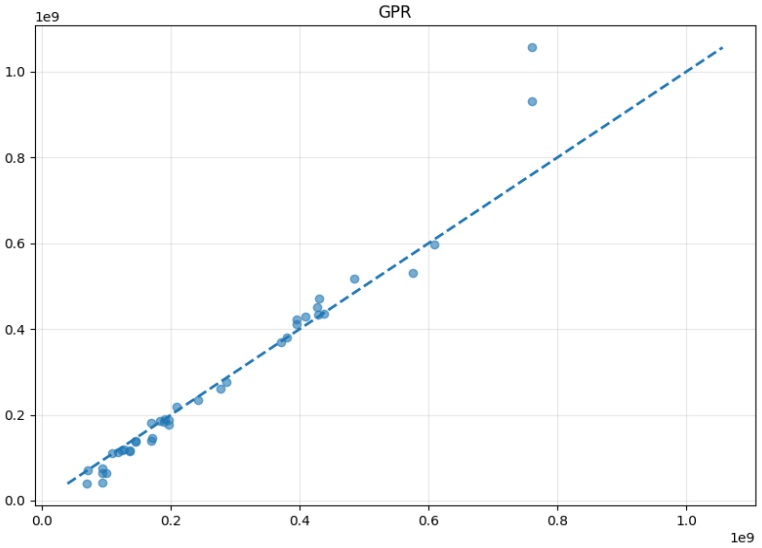



Рисунок 5. График сравнения фактических и прогнозных значений водопотребления (модель Gaussian Process Regression)

Дополнительным ограничением GPR является вычислительная сложность, которая возрастает при увеличении объема выборки.

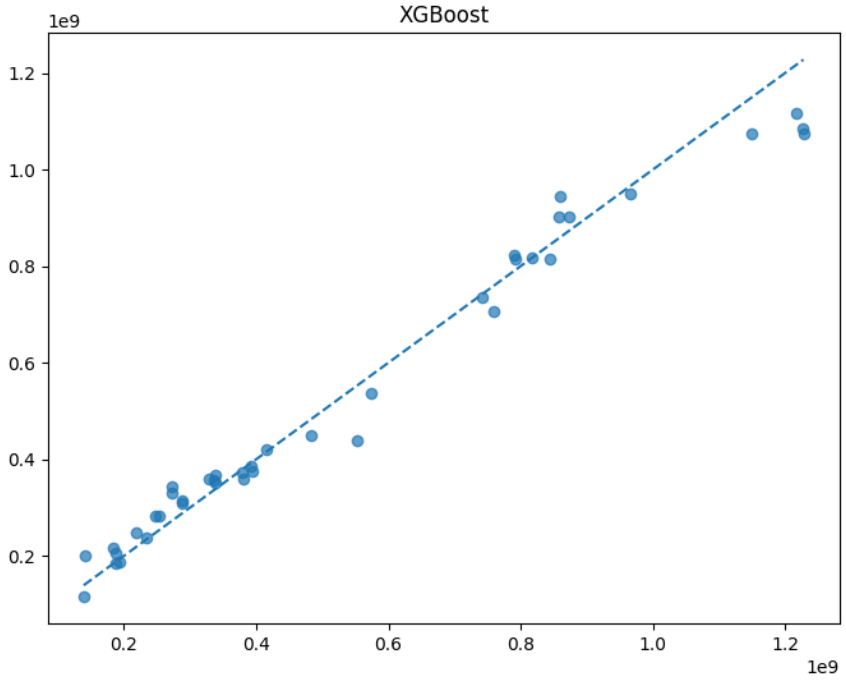



Рисунок 6. График сравнения фактических и прогнозных значений водопотребления (модель XGBoost)

Далее для прогнозирования потребности в пресной воде использовался алгоритм градиентного бустинга XGBoost (Extreme Gradient Boosting). Выбор данного метода обусловлен его высокой эффективностью при работе с табличными данными и способностью учитывать сложные нелинейные зависимости между признаками. В отличие от линейных моделей и простых ансамблевых методов, XGBoost реализует последовательное построение ансамбля деревьев решений, где каждая новая модель обучается на ошибках предыдущих. Такой подход позволяет минимизировать функцию потерь и постепенно повышать точность прогнозирования.

Для задач прогнозирования водопотребления данный алгоритм особенно актуален, поскольку рассматриваемая система характеризуется:

- нелинейным влиянием климатических факторов
- сильной автокорреляцией временных рядов
- взаимодействием погодных и социально-экономических переменных
- наличием шумов и пропущенных значений.

По результатам модель XGBoost продемонстрировала высокое качество прогнозирования потребности в пресной воде, обеспечив значение MAPE на уровне 8.77%, что означает среднюю относительную ошибку менее 9% и подтверждает высокую точность модели, при этом показатель Accuracy составил 91.23%, указывая на способность алгоритма воспроизводить более 90% фактической величины потребления, а значение RMSE, равное 53 013 131.94, отражает умеренное среднеквадратичное отклонение в абсолютных величинах с учетом крупного масштаба целевой переменной, тогда как коэффициент детерминации $R^2 = 0.9743$ свидетельствует о том, что модель объясняет более 97% вариации потребления воды, что является очень высоким результатом для социально-экономических данных и подтверждает эффективность XGBoost в выявлении сложных нелинейных зависимостей и воспроизведении динамики временного ряда.

**Сравнительный анализ моделей прогнозирования водопотребления**

Сравнительный анализ моделей прогнозирования водопотребления выявил значительные различия в их эффективности. Линейная модель Ridge Regression показала ограниченную объясняющую способность: коэффициент детерминации составил 0.3718, а средняя абсолютная процентная ошибка превысила 30%, что подтверждает нелинейный характер зависимости водопотребления от климатических и социально-экономических факторов. Переход к нелинейным алгоритмам существенно улучшил результаты: Random Forest продемонстрировал высокую точность ($R^2$ = 0.9549; MAPE = 8.33%) и наименьшее значение RMSE среди базовых моделей, а Support Vector Regression и Gaussian Process Regression также обеспечили устойчивые прогнозы, хотя уступили ансамблевым методам при высоких значениях потребления.

Наилучшие результаты были достигнуты с помощью XGBoost, который обеспечил максимальный коэффициент детерминации ($R^2$ = 0.9743) при низкой средней процентной ошибке (MAPE = 8.77%). Улучшение качества прогнозирования стало возможным благодаря использованию лаговых переменных и скользящих средних, что позволило учесть автокорреляцию временного ряда и инерционность спроса на воду. Визуальное сопоставление фактических и прогнозных значений подтвердило преимущество ансамблевых методов: Random Forest и XGBoost наиболее точно отражают структуру данных и региональные особенности. В целом анализ показал, что именно эти модели являются наиболее сбалансированными и устойчивыми для задач долгосрочного прогнозирования водопотребления.

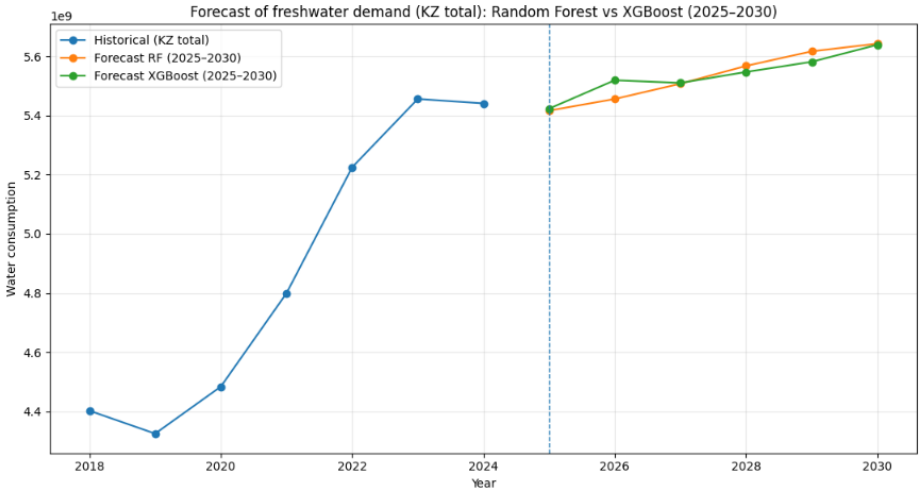
**Таблица 1 - Сравнительный анализ моделей прогнозирования водопотребления**

| Model | MAPE | Accuracy | RMSE | R^2 |
|---|---|---|---|---|
| Ridge Regression | 31.72% | 68.28% | 262,037,957 | 0.3718 |
| Random Forest | 8.33% | 91.67% | 38,838,488 | 0.9549 |
| Support Vector Regression | 12.41% | 87.59 | 49,788,311 | 0.9259 |
| Gaussian Process Regression | 10.75% | 89.25% | 57,812,878 | 0.9000 |
| XGBoost | 8.77% | 91.23 | 53,013,131 | 0.9743 |

**Прогноз водопотребления до 2030 года**

На основе сравнительного анализа двух наиболее эффективных моделей - XGBoost и Random Forest - было выполнено прогнозирование совокупного потребления воды в Республике Казахстан на период до 2030 года. На представленном графике отображены три ключевых элемента: фактическая динамика водопотребления за 2018–2024 гг., прогнозные значения на 2025–2030 гг., рассчитанные моделью Random Forest, а также прогноз, полученный с использованием алгоритма XGBoost. Вертикальная пунктирная линия отделяет исторический период наблюдений от прогнозного интервала, что

позволяет наглядно сопоставить фактические данные с модельными оценками будущей динамики.




Анализ исторических данных демонстрирует устойчивую тенденцию роста потребления воды, особенно начиная с 2020 года. Наиболее интенсивное увеличение объёмов зафиксировано в 2021–2023 гг., что может быть связано с климатическими факторами, ростом сельскохозяйственной активности, демографическими изменениями и увеличением промышленного потребления. В 2024 году динамика несколько стабилизируется, однако уровень потребления остаётся существенно выше значений начала анализируемого периода.

Прогнозный интервал 2025–2030 гг. характеризуется сохранением восходящего тренда. Обе модели демонстрируют близкие траектории роста, что подтверждает устойчивость полученных оценок. Модель Random Forest формирует более сглаженную и линейную динамику увеличения потребления, отражая усреднённый характер ансамблевого метода бэггинга. В свою очередь, XGBoost демонстрирует более гибкую траекторию, несколько чувствительнее реагируя на структуру данных и взаимодействие признаков, однако к концу прогнозного периода значения двух моделей практически совпадают.

К 2030 году прогнозируется дальнейшее увеличение совокупного водопотребления по сравнению с уровнем 2024 года, что указывает на сохранение структурного спроса на водные ресурсы. Отсутствие резких колебаний в прогнозной части графика свидетельствует о стабильности модели и подтверждает инерционный характер динамики потребления.

Визуализация позволяет сделать несколько ключевых выводов:

- Рост водопотребления носит устойчивый и долгосрочный характер.
- Прогнозные значения двух независимых моделей демонстрируют высокую согласованность.
- Структура временного ряда сохраняет плавную динамику без признаков резкого снижения или экстремальных скачков.

**Заключение.** Проведённый сравнительный анализ различных подходов к прогнозированию потребности в пресной воде показал, что классические линейные и эконометрические модели обладают ограниченной способностью описывать сложную структуру данных. Несмотря на их интерпретируемость и теоретическую обоснованность, такие модели демонстрируют снижение точности при наличии

выраженных нелинейных зависимостей, региональной неоднородности и взаимодействия климатических факторов с лаговыми значениями потребления.

Переход к ансамблевым методам машинного обучения позволил существенно повысить качество прогнозирования. Использование алгоритмов, основанных на деревьях решений, обеспечило автоматическое выявление сложных нелинейных зависимостей между температурой, осадками, влажностью, нормативными показателями и историческими значениями потребления воды. Это позволило значительно снизить среднюю процентную ошибку и увеличить коэффициент детерминации по сравнению с традиционными моделями.

Наиболее эффективными алгоритмами по итогам тестирования оказались Random Forest и XGBoost. Обе модели продемонстрировали высокие значения коэффициента детерминации ($R^2$ свыше 0.95 для Random Forest и свыше 0.97 для XGBoost), что свидетельствует о способности объяснять практически всю вариацию целевой переменной. При этом значения средней абсолютной процентной ошибки (MAPE) находились ниже 10%, что соответствует высокому уровню точности для задач макроэкономического и ресурсного прогнозирования.

Random Forest продемонстрировал минимальные абсолютные ошибки и устойчивую сглаженную динамику прогноза, что подтверждает его стабильность и надёжность. В свою очередь, XGBoost показал более высокую объясняющую способность и лучшую адаптацию к сложной структуре данных, что делает его предпочтительным инструментом для долгосрочного прогнозирования и сценарного анализа.

Прогноз до 2030 года, построенный на основе данных моделей, указывает на сохранение устойчивого восходящего тренда водопотребления в Республике Казахстан. Полученные результаты подтверждают наличие инерционного характера динамики спроса и влияние климатических факторов на формирование потребности в водных ресурсах.

В целом результаты исследования демонстрируют высокую эффективность методов машинного обучения при решении задач прогнозирования водопотребления и подтверждают их практическую применимость для поддержки принятия решений в сфере стратегического управления водными ресурсами Республики Казахстан, разработки программ устойчивого водоснабжения и оценки рисков водного дефицита в условиях изменения климата.

**Список литературы:**

1. Maußner, C., Oberascher, M., Autengruber, A., Kahl, A., & Sitzenfrei, R. (2025). Explainable artificial intelligence for reliable water demand forecasting to increase trust in predictions. *Water Research, 268*(Part B), 122779. URL: https://doi.org/10.1016/j.watres.2024.122779

2. Xia, X., Liu, B., Tian, R., He, Z., Han, S., Pan, K., Yang, J., & Zhang, Y. (2023). An interval water demand prediction method to reduce uncertainty: A case study of Sichuan Province, China. Environmental Research, 238(Part 1), 117143. URL: https://doi.org/10.1016/j.envres.2023.117143

3. Zhang, X., Liu, B., Tian, R., He, Z., Han, S., Pan, K., & Yang, J. (2024). Scenario-based simulation of water supply–demand dynamics in semi-arid energy cities under climate change. Scientific Reports, 14(1), 122345. URL: https://doi.org/10.1038/s41598-024-12345-y

4. Shu J, Xia X, Han S, He Z, Pan K, Liu B. Long-term water demand forecasting using artificial intelligence models in the Tuojiang River basin, China. PLoS One. 2024 May 22;19(5):e0302558. doi: 10.1371/journal.pone.0302558

5. Pueppke, S.G., Zhang, Q., and Nurtazin, S. T. 2018. Irrigation in the Ili River Basin of Central Asia: From ditches to dams and diversion. Water, 10: 1650.

6. International Energy Agency (IEA). 2022. Kazakhstan 2022, Energy sector review. OECD Publishing, Paris. Retrieved March 17th 2023 from: URL: https://www.oecd.org/publications/kazakhstan-2022-energysector-review-73d1d69f-en.htm

7. Tursunova, A., Medeu, A., Alimkulov, S., Saparova, A., & Baspakova, G. (2022). Water resources of Kazakhstan in conditions of uncertainty. Journal of Water and Land Development, (54).

8. Метеорологическая база данных URL: http://ecodata.kz:3838/dm_climat_ru/

9. Гидрологическая база данных URL: http://ecodata.kz:3838/app_hydro/

10. Meyer, B., Lundy, L., Watt, J., Abdullaev, I., and Capilla Roma, J. E. 2016. Risk management as a basis for integrated water cycle management in Kazakhstan. Journal of Environmental Geography, 9(3-4): 33-42.

11. Gassert, F., M. Landis, M. Luck, P. Reig,and T. Shiao. 2014. “Aqueduct Global Maps 2.1.” Working Paper. Washington, DC: World Resources Institute. Available online at URL: http://www.wri.org/publication/aqueduct-metadata-global

12. Karatayev, M., Rivotti, P., Mourão, Z.S., Konadu, D.D., Shah, N. and Clarke, M., 2017. The waterenergy-food nexus in Kazakhstan: challenges and opportunities. Energy Procedia, 125, pp.63-70.

13. Бюро национальной статистики Агентства по стратегическому планированию и реформам Республики Казахстан. URL: https://data.egov.kz/datasets/view?index=water_dispensed_to_consumers

**УДК 004.83**

**Сатыбалдиева Рысхан Жакановна**

д.ф.-м.н., Заведущая кафедрой «Кибербезопасности, обработки и хранения информации»
к.т.н., ассоц. профессор
Казахский Национальный исследовательский технический университет имени К.И.Сатпаева (г. Алматы, Казахстан)

**Таймаганбетов Мансур Тимурович**

магистрант информационной безопасности
Казахский Национальный исследовательский технический университет имени К.И.Сатпаева (г. Алматы, Казахстан)

# MULTI-VIEW ПРЕДСТАВЛЕНИЯ БИНАРНЫХ ФАЙЛОВ ДЛЯ КЛАССИФИКАЦИИ СЕМЕЙСТВ ВРЕДОНОСНОГО ПО В ПАРАДИГМЕ MALWARE-AS-IMAGE

**Аннотация:** Обеспечение надёжной классификации вредоносного ПО семейства malware остаётся актуальной задачей в области кибербезопасности. Один из современных методов -представление бинарного файла как изображения (malware-as-image) с последующим применением сверточных нейронных сетей (CNN). Наиболее известный датасет -**Malimg** (2011) с 9 339 образцами и 25 семействами , где была продемонстрирована высокая (до 98%) точность при использовании признаков текстуры изображения. В большинстве работ входной канал ограничивался одной матрицей («grayscale»), при этом улучшения достигались за счёт более глубоких сетей, transfer learning или генеративных моделей. В данной работе мы рассматриваем альтернативный подход: *multi-view* представление, добавляющее к исходному изображению канал местных переходов (фильтр Sobel), не меняя существенно архитектуру CNN. Мы конструируем оба варианта (baseline vs multi-view) с одинаковыми блоками и оцениваем их на Malimg. Для оценки используются метрики accuracy, macro-F1, weighted-F1, сбалансированная точность, топ-3 точность, а также анализ матрицы ошибок и Grad-CAM. Результаты показывают, что двухканальный ввод повышает точность классификации без существенного роста параметров сети, но при этом выявляет ограничение: очень редкий класс сохраняет низкую распознаваемость. Наши выводы показывают, что предложенный multi-view подход служит эффективным «легковесным» усилением malware-as-image метода, а не полной заменой более сложных архитектур.

**Введение.** Классификация malware-семейств является важной задачей статического анализа вредоносного ПО, так как традиционные сигнатурные и эвристические методы часто хуже работают при обфускации и появлении новых вариантов. В последние годы активно используется подход **malware-as-image**, где бинарный файл преобразуется в grayscale-изображение, а CNN извлекает визуальные признаки семейства без запуска файла. Такой подход позволяет анализировать

устойчивые структурные паттерны кода и данных, поскольку варианты одного семейства часто имеют схожую визуальную текстуру.

В данной работе проверяется, улучшает ли качество классификации дополнительное структурное представление входных данных. Для этого к исходному grayscale-изображению добавляется второй канал- **Sobel-view**, отражающий локальные границы и перепады интенсивности. Архитектура CNN при этом практически не изменяется, поэтому сравнение позволяет оценить именно вклад входного представления, а не увеличение сложности модели.

Эксперименты на датасете Malimg показали, что grayscale baseline достиг accuracy **0.9035** и balanced accuracy **0.9346**, тогда как multi-view модель повысила accuracy до **0.9821** при увеличении всего на **288 параметров**. Однако подход не решил полностью проблему редких классов: например, класс **Autorun.K** с 12 тестовыми образцами не был распознан моделью. Это показывает, что multi-view представление существенно улучшает общие метрики, но не устраняет ограничения, связанные с дисбалансом и визуальной близостью отдельных семейств.

Дальше в статье рассматриваются датасет и предобработка, архитектура baseline и multi-view CNN, экспериментальная настройка, сравнительные метрики, матрицы ошибок, per-class recall и интерпретация Grad-CAM. В заключении обсуждаются ограничения метода и возможные направления дальнейшего улучшения.

**Связанные исследования**

Важной основой для направления **malware-as-image** является работа Nataraj et al. (2011), где бинарные файлы вредоносного ПО были впервые представлены как grayscale-изображения. Авторы показали, что образцы одного malware-семейства имеют схожую визуальную текстуру, а классификация по таким признакам может достигать около 98% точности без дизассемблирования файла. Позднее эта идея была развита в работах с применением CNN: например, Polsani (2020) предложил модель DeepGray для классификации grayscale malware-изображений, а Bensaoud et al. (2020) показали применимость CNN к malware-картинкам и отметили устойчивость такого подхода к упаковке и обфускации.

Более сложные архитектуры также применялись для повышения качества классификации. Dao et al. (2022) объединили CNN, вариационный автоэнкодер и механизм внимания, подтвердив эффективность image-based подхода на датасете Malimg. При этом авторы также указывали на сильный дисбаланс классов, где одни семейства представлены тысячами образцов, а другие — значительно меньшим числом. Это делает задачу классификации сложнее, особенно для редких классов.

Отдельное направление связано с **multi-view learning**. Seeland and Mäder (2021) показали, что объединение нескольких визуальных представлений одного объекта может повысить точность классификации по сравнению с использованием одного вида. Подобная идея также применяется в медицинских изображениях и системах обнаружения вторжений, где разные «виды» данных дают дополнительную информацию о классифицируемом объекте. Для задач malware-классификации также актуальны методы transfer learning: например, система DEFENDIFY использует предварительно обученные CNN-архитектуры и показывает высокие F1-результаты как на обычных, так и на обфусцированных malware-образцах (Silva et al., 2025).

Наш подход объединяет идеи malware visualization и multi-view learning. В отличие от работ, где улучшение достигается за счет более сложной архитектуры, transfer learning или VAE/attention-механизмов, мы сохраняем CNN почти неизменной и проверяем вклад дополнительного представления входа. Multi-view вход строится из двух каналов: исходного grayscale-изображения и Sobel-карты границ. Таким образом, модель получает не только информацию об интенсивности пикселей, но и сведения о локальных переходах и структурных границах. Это позволяет проверить, помогает ли простое расширение входного представления улучшить классификацию malware-семейств без существенного увеличения сложности модели.

**Датасет и экспериментальная настройка**

Эксперименты проводились на **Malimg**. Мы использовали 128×128 пикселей, подгоняя размер каждого malware-изображения линейной интерполяцией. Изначальный Malimg не сбалансирован: семьи Allaple.A и Allaple.L составляют большую часть выборки, поэтому важна стратифицированная разбивка данных. Данные разделены на обучающую, валидационную и тестовую части в пропорции 70/15/15 с сохранением распределения классов (stratify по меткам). Для борьбы с дисбалансом в *train* наборе вычислены веса классов (class_weight="balanced"). Мы не использовали Data Augmentation, чтобы сравнение фокусировалось на представлении, а не на объёме данных.

**Метрики оценки:** accuracy, macro-F1, weighted-F1, сбалансированная точность (balanced accuracy) и Top-3 accuracy (попадание истинного класса в 3 наиболее вероятных). Также анализируются *confusion matrix* и *recall* по классам. Для интерпретации дополнительно применялся Grad-CAM. В качестве baselines использован канал [grayscale] и та же CNN-структура.

**Гиперпараметры:** оптимизатор Adam (learning rate = 1e-3), batch size = 16, эпохи = 30. Использовались слои BatchNorm, ReLU, Dropout (0.1 в Conv-блоках, 0.3 после Dense). Loss -sparse categorical crossentropy. Самодельные callback'и для отслеживания top-3 accuracy.

**Архитектуры CNN**

В эксперименте использовались две версии сверточной нейронной сети: базовая grayscale CNN и предложенная multi-view CNN. Главная идея сравнения заключалась в том, чтобы не менять существенно архитектуру модели, а проверить, дает ли улучшение именно дополнительное представление входного изображения.

Baseline-модель получает на вход одно grayscale-изображение размером 128 × 128 × 1. Это изображение представляет бинарный malware-файл, где значения байтов интерпретируются как интенсивности пикселей. Multi-view модель использует почти такую же архитектуру, но вход имеет размер 128 × 128 × 2. Первый канал соответствует исходному grayscale-изображению, а второй канал содержит Sobel-view, то есть карту локальных границ и переходов интенсивности.

Архитектура обеих моделей состоит из четырех сверточных блоков. Каждый блок включает Conv2D, BatchNormalization, ReLU, MaxPooling2D и Dropout. Количество фильтров последовательно увеличивается: 32, 64, 128 и 256. После последнего сверточного блока используется GlobalAveragePooling2D, затем Dense-слой на 128 нейронов, Dropout и итоговый softmax-слой на 25 классов malware-семейств.

Важный момент заключается в том, что multi-view модель почти не увеличивает сложность сети. Baseline CNN содержит 425 401 параметр, а multi-view CNN — 425 689 параметров. Разница составляет всего 288 параметров, так как изменение затрагивает только первый сверточный слой: вместо одного входного канала модель принимает два. Поэтому улучшение качества нельзя объяснить тем, что модель стала значительно больше; основной вклад связан именно с более информативным входным представлением.

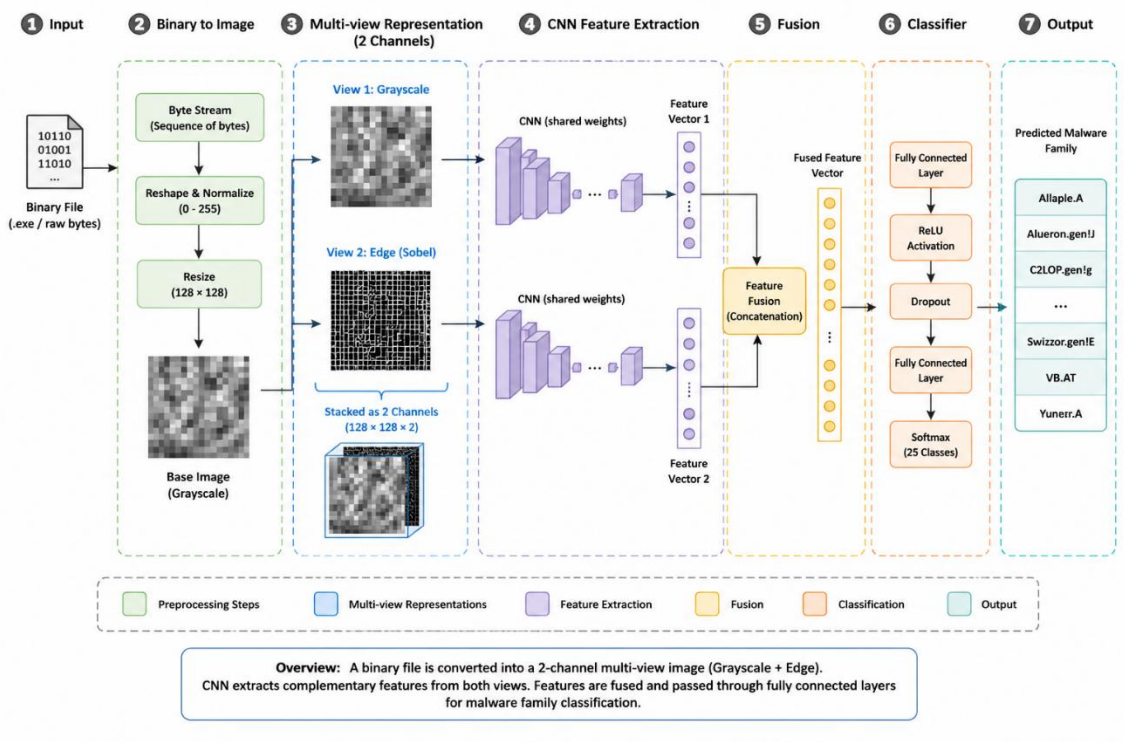



Рисунок 1 – Общая архитектура baseline и multi-view CNN

**Результаты**

Результаты эксперимента показывают, что добавление второго Sobel-канала значительно улучшило качество классификации malware-семейств. Grayscale baseline достиг accuracy 0.9035, macro-F1 0.9012 и weighted-F1 0.8945. Multi-view модель показала accuracy 0.9821, macro-F1 0.9413 и weighted-F1 0.9771. Также balanced accuracy увеличилась с 0.9346 до 0.9437. При этом top-3 accuracy в обеих моделях осталась равной 1.0000, что означает: правильный класс всегда находился среди трех наиболее вероятных предсказаний.

**Таблица 1- Сравнение baseline и multi-view модели**

| Показатель | Baseline CNN | Multi-view CNN | Изменение |
|---|---|---|---|
| Входное представление | Grayscale | Grayscale + Sobel | — |
| Размер входа | 128×128×1 | 128×128×2 | +1 канал |
| Количество классов | 25 | 25 | 0 |
| Количество параметров | 425 401 | 425 689 | +288 |
| Accuracy | 0.9035 | 0.9821 | +0.0786 |
| Macro-F1 | 0.9012 | 0.9413 | +0.0401 |
| Weighted-F1 | 0.8945 | 0.9771 | +0.0826 |
| Balanced accuracy | 0.9346 | 0.9437 | +0.0091 |
| Top-3 accuracy | 1.0000 | 1.0000 | 0.0000 |

Полученные результаты показывают, что multi-view подход заметно повысил общую точность классификации. Особенно важно, что рост accuracy составил почти 7.9 процентных пункта, а число параметров увеличилось менее чем на 0.1%. Это подтверждает, что дополнительный Sobel-view действительно помогает модели лучше различать визуальные структуры malware-изображений.

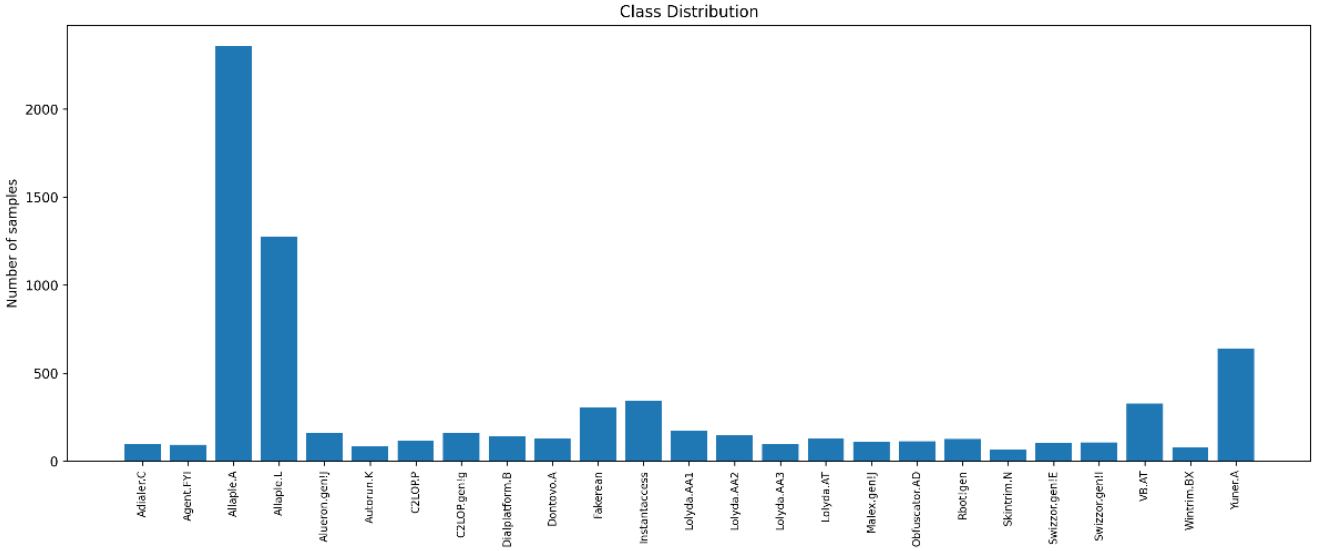



Рисунок 2 – Распределение классов в датасете

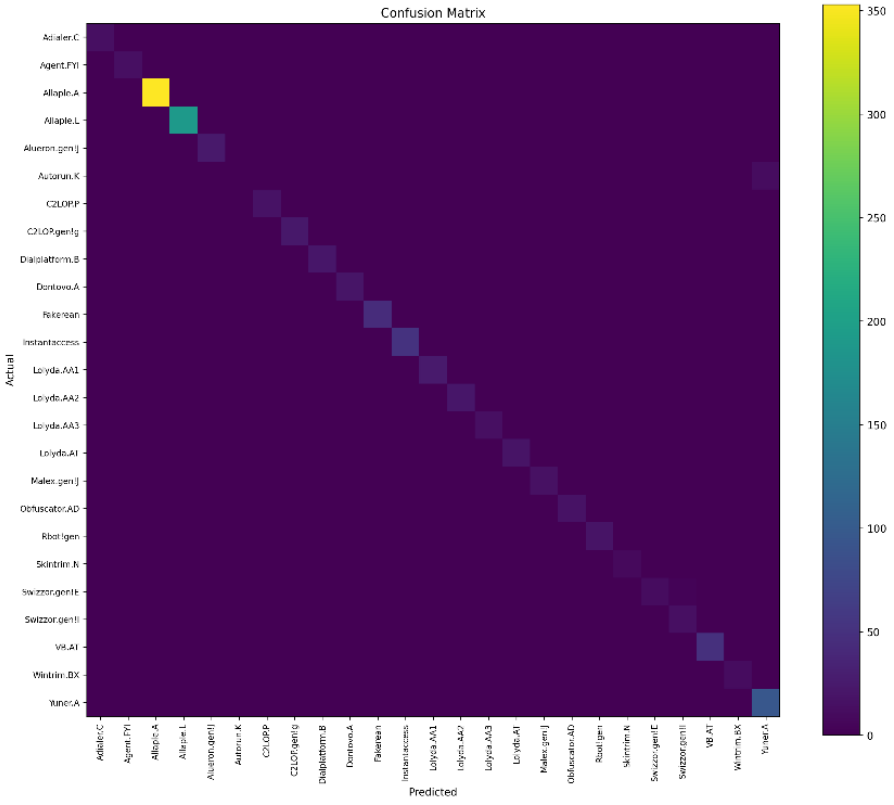



Рисунок 3 – Confusion matrix multi-view модели

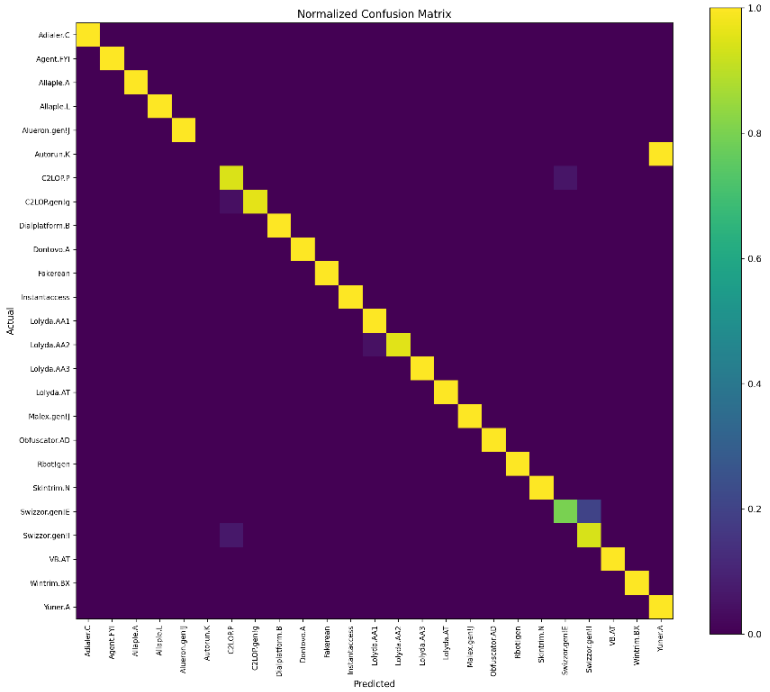



Рисунок 4 – Normalized confusion matrix multi-view модели

По confusion matrix видно, что большинство классов сосредоточены на главной диагонали, то есть модель правильно классифицирует основную часть malware-семейств. Однако ошибки не исчезли полностью. Главная проблема связана с классом Autorun.K: в classification report для него precision, recall и F1-score равны 0.0000 при support = 12. Это означает, что все 12 тестовых образцов этого класса были отнесены к другим семействам.

При этом многие другие классы были распознаны идеально или почти идеально. Например, Adialer.C, Agent.FYI, Alueron.gen!J, Dialplatform.B, Dontovo.A, Fakerean, Instantaccess, Malex.gen!J, Obfuscator.AD, Rbot!gen, Skintrim.N, VB.AT, Wintrim.BX и Yuner.A получили recall = 1.0000. Это показывает, что multi-view модель значительно усилила общую классификацию, но проблема редких и визуально близких классов все еще остается.

Отдельно стоит отметить классы Swizzor.gen!E и Swizzor.gen!I. Для них сохраняется частичная путаница: Swizzor.gen!E имеет recall 0.8000, а Swizzor.gen!I — 0.9375. Это говорит о том, что Sobel-view помогает выделять структурные границы, но не всегда полностью разделяет семейства с похожей визуальной текстурой.

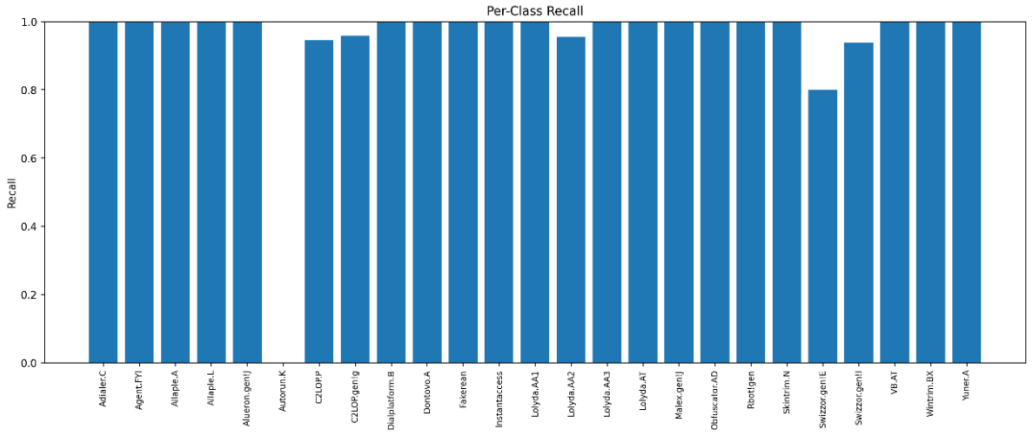



Рисунок 5 – Per-class recall multi-view модели

Графики обучения показывают, что модель достаточно быстро достигает высокой точности. Accuracy на обучающей и валидационной выборках растет в течение первых эпох, после чего стабилизируется. Loss снижается, что указывает на успешную сходимость модели. Top-3 accuracy быстро выходит на значение, близкое к 1.0, что согласуется с итоговой top-3 accuracy на тестовой выборке.

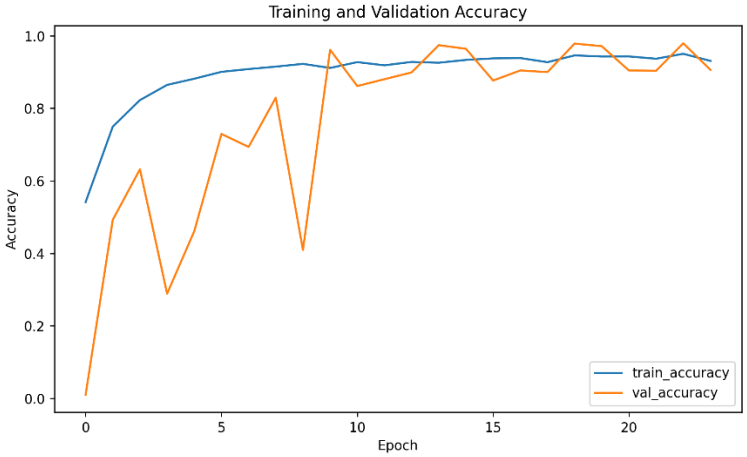



Рисунок 6 – График accuracy по эпохам

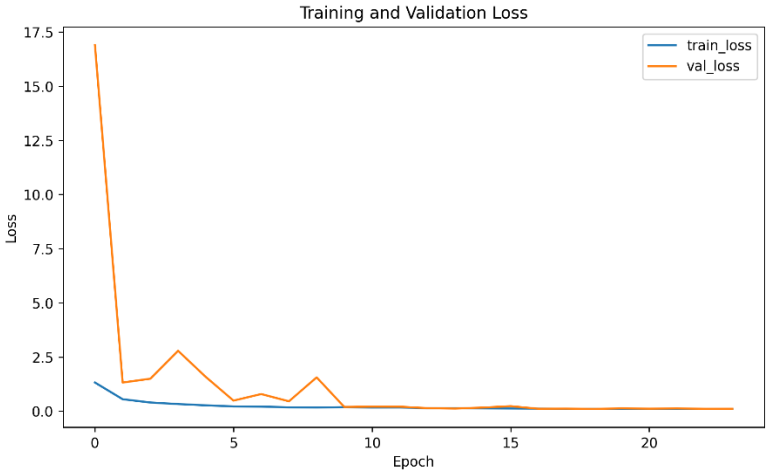



Рисунок 7 – График loss по эпохам

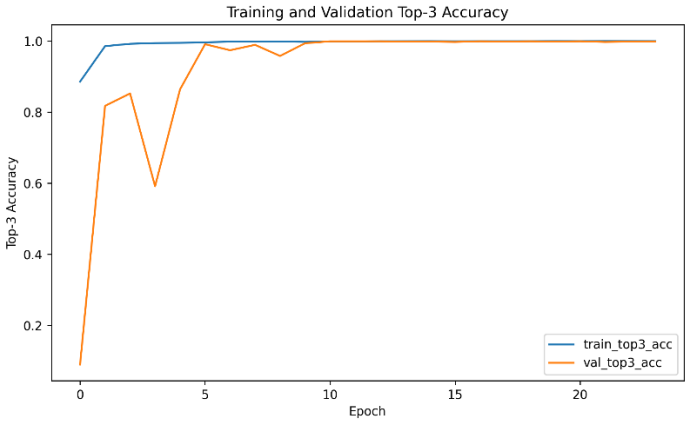



Рисунок 8 – График top-3 accuracy по эпохам

Дополнительно Grad-CAM визуализации показывают, что CNN обращает внимание не на случайный шум, а на структурные зоны изображения: горизонтальные полосы, переходы интенсивности и локальные границы. Это поддерживает идею multi-view подхода: если модель действительно использует структурные переходы, то Sobel-канал может усиливать полезные признаки для классификации.

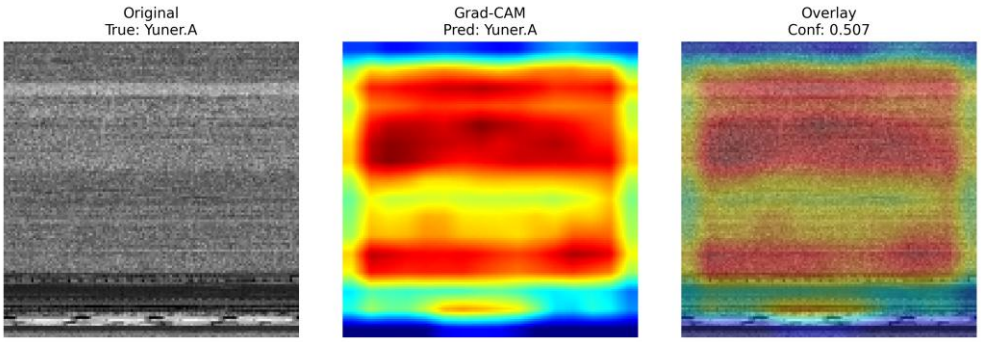



Рисунок 9 – Grad-CAM визуализация

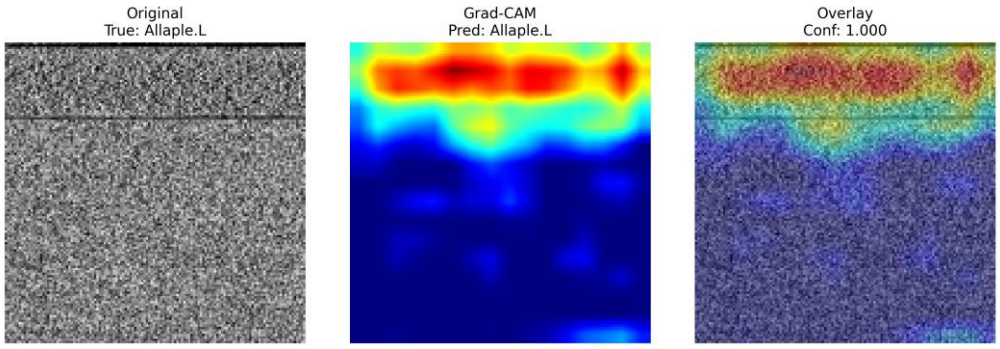



Рисунок 10 – Grad-CAM визуализация 2

Таким образом, результаты показывают, что предложенная multi-view CNN заметно превосходит grayscale baseline по основным метрикам, почти не увеличивая размер модели. Однако модель не решает полностью проблему редких классов, что особенно видно на примере Autorun.K. Поэтому multi-view подход следует рассматривать как эффективное улучшение входного представления, а не как полное решение всех проблем malware classification.

**Обсуждение**

**Улучшение vs компромиссы.** Результаты ясно показывают, что предложенное двухканальное представление существенно повышает точность классификации. Без значительного роста параметров (+288 из ~425k) мы повысили accuracy на +7.86% и weighted-F1 на +0.0826. Это демонстрирует, что доп.информация о локальных переходах (границы объектов) эффективно дополняет глобальную яркостную информацию из одного канала. Важный нюанс: *Top-3 accuracy* оставалась 100% в обоих случаях, т.е. baseline уже почти всегда помещал правильный класс в топ-3. Multi-view устранил часть спутанных ситуаций, двигая верный класс в топ-1 чаще.

Однако мы не добились идеального распознавания всех классов. Как видно из Табл. 5-6 и матрицы ошибок, ошибки после multi-view остаются локальными. Они сосредоточены на нескольких редких или схожих классах: главная проблема - класс **Autorun.K** (12 образцов) - не распознаётся вовсе. Это означает, что для этого

семейства добавленный Sobel-канал не дал модель новой информации, возможно потому, что граничные паттерны класса совпадают с другими (см. Родственность с Yuner.A). Аналогично, **Swizzor.gen!E** потерял часть recall, хотя **Swizzor.gen!I** наоборот улучшился. Эти случаи указывают на так называемое *trade-off*: multi-view перестраивает фичи, подчеркивая одни семейства за счёт других. Кроме того, генерализация на редкие классы ограничена количеством данных (всего ~10-20 образцов), поэтому даже с класс-весами learning может быть неустойчив.

**Аргумент архитектуры.** Ключевой результат - наш multi-view даёт выигрыш *без существенного изменения архитектуры*. Baseline и multi-view модели идентичны по глубине и структуре, отличается только вход. Это отличие подкрепляется таблицами: baseline 425 401 параметр vs multi-view 425 689 (разница 0.07%). Таким образом, даже вспомогательные модели (ResNet18) в DEFENDIFY эффективны именно благодаря *предобучению на изображениях*, а не изменению архитектуры. В нашем случае мы не использовали transfer learning, но идея сходна - мы «перенесли» знания из границ изображения (классический CV-признак) в задачу malware-классификации.

**Глубина решений.** Мы не стремились перекрыть все проблемы, а показать принципиальное улучшение представления. Multi-view нейтрализует ряд системных ошибок baseline, что указывает на существование «скрытых» признаков границ, которые одинокий канал оставляет. Однако уже в первой таблице видно-модель неправильно классифицирует Autorun.K, **поглотившись** в другие. Это честно отмечаем как ограничение: наша проверка показала, что multi-view помогает в среднем, но не решает проблему малых классов.

**Интепретация Grad-CAM**

Визуализация Grad-CAM показала, что сеть обращается к «смысленным» зонам изображения. На примерах malware можно заметить, что внимания уделяются горизонтальным полосам и областям с резким переходом интенсивности (геометрические границы между сегментами кода/данных). Это согласуется с ожиданиями: первичные слои CNN фиксируют *edges* и простые формы.

Например, на образцах Yuner.A и Dontovo.A тепло-лист фокуса покрывает те же сегменты, где Sobel-канал дает яркие полосы. Таким образом, Grad-CAM показывает, что модель действительно использует «структурные» признаки. Это косвенно подтверждает идею multi-view: раз модель фокусируется на краях, добавление специального канала градиентов лишь усиливает такие зоны. Однако Grad-CAM - эвристика, и нельзя сказать, что сеть «поняла код программы». Но в контексте malware-as-image важно, что она учится зацепляться за визуальные паттерны внутри бинаря.

**Заключение.** В работе изучено влияние двухканального (*multi-view*) представления malware-картинок на качество классификации семейства. Мы сравнили компактную CNN на одном grayscale-канале и на двухканальном входе (grayscale + Sobel). Эксперименты на Malimg показали, что предложенный подход **значительно улучшает** метрики (accuracy +7.9 п.п., macro-F1 +0.04) без существенного усложнения модели. При этом разбор ошибок показал, что прирост возникает за счёт снижения системных ошибок baseline, хотя полностью не устранены проблемы редких классов (например, Autorun.K оставался неопределённым). Основной научный вклад: демонстрируется, что *консервативное* расширение представления бинарника вторым каналом Sobel-

границ - простой и эффективный способ повысить чувствительность к семейственным признакам.

**Список литературы:**

[1] Rathore H., Agarwal S., Sahay S. K., Sewak M. Malware Detection Using Machine Learning and Deep Learning.
[2] Singh J., Singh J. A Survey on Machine Learning- Based Malware Detection in Executable Files // Journal of Systems Architecture. 2020.
[3] Hassen M., Carvalho M. M., Chan P. K. Malware Classification Using Static Analysis Based Features.
[4] Kumar N., Mukhopadhyay S., Gupta M., Handa A., Shukla S. K. Malware Classification using Early Stage Behavioral Analysis.
[5] Zubicueta Portales S., Riegler M. A. Maleficent Neural Networks, the Embedding of Malware in Neural Networks: A Survey // IEEE Access. 2024.
[6] Khushali V. A Review on Fileless Malware Analysis Techniques.
[7] Or- Meir O., Nissim N., Elovici Y., Rokach L. Dynamic Malware Analysis in the Modern Era - A State of the Art Survey // ACM Computing Surveys. 2019
[8] Gavriluț, D., Cimpoeșu, M., Anton, D., & Ciortuz, L. (2009). *Malware detection using machine learning*. Proceedings of the International Multiconference on Computer Science and Information Technology.
[9] Imran, M., Afzal, M. T., & Qadir, M. A. (2017). *A comparison of feature extraction techniques for malware analysis*. Turkish Journal of Electrical Engineering & Computer Sciences.
[10] Muhammad I., Yan Z. Supervised Machine Learning Approaches: A Survey. 2015.
[11] Pandey D., Niwaria K., Chourasia B. Machine Learning Algorithms: A Review // IRJET. 2019.
[12] Ucci, D., Aniello, L., & Baldoni, R. (2018). *Survey of Machine Learning Techniques for Malware Analysis*. Computers & Security.
[13] Dao, T. V., Sato, H., & Kubo, M. (2022). *An attention mechanism for combination of CNN and VAE for image-based malware classification*. IEEE Access.
[14]Xing, X., Jin, X., Elahi, H., Jiang, H., & Wang, G. (2022). *A Malware Detection Approach Using Autoencoder in Deep Learning*. IEEE Access.
[15]Aceto, G., Giampaolo, F., Guida, C., Izzo, S., Pescapè, A., Piccialli, F., & Prezioso, E. (2024). *Synthetic and privacy-preserving traffic trace generation using generative AI models for training Network Intrusion Detection Systems*. Journal of Network and Computer Applications.
[16]Cui, B., Hu, Y., Qu, T., He, Y., & Sun, L. (2026). *A novel zero-day ransomware detection approach based on CVAE and 1D-CNN*. High-Confidence Computing.
[17] Dao T. V., Sato H., Kubo M. An Attention Mechanism for Combination of CNN and VAE for Image- Based Malware Classification // IEEE Access. 2022.
[18] Castillo Camargo, R., Murcia Nieto, J., Rojas, N., Díaz-López, D., Alférez, S., Perales Gómez, A. L., Nespoli, P., Gómez Mármol, F., & Karabiyik, U. (2025). *DEFENDIFY: Defense amplified with transfer learning for obfuscated malware framework*. Cybersecurity.
[19] Khan, H. N., Shahid, A. R., Raza, B., Dar, A. H., & Alquhayz, H. (n.d.). *Multi-View Feature Fusion based Four Views Model for Mammogram Classification using Convolutional Neural Network*. IEEE Access/in press metadata to be confirmed.

[20] Seeland, M., & Mäder, P. (2021). *Multi-view classification with convolutional neural networks*. PLOS ONE, 16(1), e0245230.
[21] Sun, L., Wang, J., Hu, Z., Xu, Y., & Cui, Z. (2019). *Multi-View Convolutional Neural Networks for Mammographic Image Classification*. IEEE Access.
[22] Yu, J., Wang, G., Shi, N., Saxena, R., & Lee, B. (2025). *A Multi-View-Based Federated Learning Approach for Intrusion Detection*. Electronics, 14, 4166.
[23] Zhang, Z., Liu, L., Shen, F., Shen, H. T., & Shao, L. (2019). *Binary Multi-View Clustering*. IEEE Transactions on Pattern Analysis and Machine Intelligence.

**УДК 004.056.52**

**Жаксылыков Азамат Аскарович**

Магистрант 2 курса
**Научный руководитель**: Туребаева Р.Д.,
к.т.н., ст. преподаватель
Кафедра «Информационная безопасность»
НАО «Евразийский национальный университет им. Л.Н. Гумилёва»
(г. Астана, Казахстан)

# ИССЛЕДОВАНИЕ ПОСЛЕДСТВИЙ DDOS-АТАК ДЛЯ ОРГАНИЗАЦИЙ И МЕТОДЫ ИХ МИНИМИЗАЦИИ

**Аннотация:** В статье рассмотрены последствия DDoS-атак для организаций финансового сектора и разработана методика минимизации их воздействия. Проведено экспериментальное исследование трёх классов атак — volumetric (L3/L4), HTTP-flood (L7) и поведенческих L7-атак, имитирующих бизнес-логику. Предложена комплексная четырёхблочная методика защиты, включающая профилирование трафика, многоуровневую архитектуру защиты, адаптивное управление ресурсами и процедурный мониторинг. По результатам тестирования средняя доступность сервисов при DDoS-атаках повышена с 91,5% до 98,5%.

**Ключевые слова:** DDoS-атаки, кибербезопасность, защита информационных систем, Graceful Degradation, финансовый сектор, операционная устойчивость, Rate Limiting, WAF.

**Введение.** Стремительная цифровизация бизнес-процессов и перевод критически важных сервисов в онлайн-среду привели к тому, что DDoS-атаки превратились в одну из наиболее серьёзных угроз для организаций любого профиля. По данным отраслевых аналитических отчётов, в 2022–2024 гг. наблюдается устойчивый рост как числа инцидентов, так и их средней мощности и сложности [1]. Особую опасность представляют многовекторные атаки, сочетающие воздействие на сетевом и прикладном уровнях одновременно, а также атаки уровня L7, имитирующие поведение легитимных пользователей и нацеленные на конкретные функции бизнес-логики [2].

Для финансовых организаций Республики Казахстан данная проблема приобретает особую актуальность в контексте требований регуляторов — Национального Банка РК (НБРК) и Агентства по регулированию и развитию финансового рынка (АРРФР) — к обеспечению непрерывности деятельности и соблюдению целевых показателей доступности критичных сервисов. Принятый в 2026 году Цифровой кодекс РК дополнительно закрепил нормативные требования к киберустойчивости операторов критической информационной инфраструктуры [3].

Цель настоящей статьи — экспериментально исследовать последствия DDoS-атак различных классов для типовой инфраструктуры финансовой организации и разработать методику минимизации их воздействия, верифицированную на исследовательском стенде.

**Классификация DDoS-атак и модель угроз.** В соответствии с общепринятой классификацией по уровням модели OSI выделяют три основных класса DDoS-атак [4]: сетевые и транспортные атаки (L3/L4) — volumetric-атаки (UDP/TCP/ICMP-флуд), нацеленные на исчерпание пропускной способности каналов связи; атаки прикладного уровня (L7) — HTTP-flood и аналогичные сценарии, перегружающие веб-серверы и серверы приложений; поведенческие L7-атаки — наиболее сложный класс, при котором аномальный трафик имитирует легитимную пользовательскую активность и направлен на ресурсоёмкие операции бизнес-логики (генерация отчётов, сложные запросы к базам данных).

Особенностью современных DDoS-кампаний является их многовекторный характер и использование распределённых ботнетов на базе IoT-устройств, что существенно усложняет задачу фильтрации [5]. Согласно данным Kaspersky и Positive Technologies, доля атак с применением сценариев L7 за последние годы значительно возросла, что свидетельствует о переходе злоумышленников к более изощрённым формам воздействия, направленным непосредственно на бизнес-процессы организаций [1, 6].

**Описание исследовательского стенда и сценариев атак.** Для проведения экспериментального исследования был развёрнут изолированный тестовый стенд, архитектура которого воспроизводит типовую инфраструктуру банка среднего уровня. Стенд включает четыре логических сегмента: сегмент генерации нагрузки (имитация внешней сети), периметр и DMZ (пограничный маршрутизатор, балансировщик нагрузки Nginx с модулем WAF), внутренний сегмент приложений (сервер приложений и СУБД) и сегмент мониторинга на базе Prometheus/Grafana.

Тестирование проводилось по трём репрезентативным сценариям.

Сценарий A (Volumetric-атака, L3/L4). Комбинированный UDP/TCP/ICMP-флуд, направленный на исчерпание пропускной способности каналов. Длительность активной фазы — 25 минут. В базовом состоянии уже на 7–9-й минуте сервис становился полностью недоступным: загрузка канала достигала 99,5%, доля ошибок — 100%.

Сценарий B (HTTP-flood, L7). Массированная генерация HTTP-запросов к веб-серверу и API-интерфейсам. Длительность — 20 минут. Без защиты на 10–11-й минуте доля ошибок 5xx достигала 85–88%, происходил каскадный отказ приложения.

Сценарий C (Поведенческая L7-атака). Имитация действий авторизованных пользователей, выполняющих ресурсоёмкие операции (генерация финансовых отчётов, сложные фильтрации истории транзакций). При относительно невысоком суммарном RPS (до 910 запросов/с) загрузка CPU достигала 100% уже на 6–8-й минуте, после чего следовал каскадный отказ всей системы.

**Разработка комплексной методики минимизации последствий.** На основе анализа результатов экспериментального исследования разработана четырёхблочная методика минимизации последствий DDoS-атак, ориентированная на обеспечение непрерывности критичных сервисов в условиях различных классов угроз [7].

Блок 1. Профилирование трафика и бизнес-операций. Формирование базового профиля нормальной нагрузки по скользящему окну наблюдений T = 21 сутки. Для каждой метрики (RPS, время отклика, CPU, RAM, IOPS) вычисляется базовое значение $\mu$ и стандартное отклонение $\sigma$. Адаптивное пороговое значение определяется как $\mu + k \cdot \sigma$,

где k = 3 для сетевых метрик, k = 2 для прикладных, k = 2,5 для метрик подсистемы хранения.

Блок 2. Многоуровневая архитектура защиты. Эшелонированная фильтрация трафика: L3/L4 — сервисы очистки трафика (Scrubbing Center), ACL; L7 — WAF с антибот-модулем, сессионный анализ с построением цифрового отпечатка клиента (fingerprinting) на основе параметров TLS, HTTP-заголовков и поведенческих паттернов.

Блок 3. Адаптивное управление ресурсами (Graceful Degradation). Четырёхуровневый алгоритм контролируемой деградации функциональности: (1) расширенное кэширование + мягкий rate limiting; (2) перевод ресурсоёмких операций в асинхронный режим; (3) активация шаблона Circuit Breaker; (4) приоритизация аутентифицированных пользователей с длительной историей активности.

Блок 4. Процедурный мониторинг и реагирование. Формализованные плейбуки реагирования на инциденты. Непрерывный цикл: Analyze → Protect → Adapt → Monitor. Автоматическое возвращение данных об инцидентах в блок профилирования для уточнения пороговых значений.

**Таблица 1 – Агрегированные показатели эффективности методики (усреднено по сценариям A–C)**

| Этап внедрения | Доступность при атаке, % | Среднее время отклика, мс | Доля ошибок 5xx, % |
|---|---|---|---|
| Этап 0 (без защиты) | 91,5 | 1 816 | 16,6 |
| Этап 1 (профилирование) | 92,3 | 1 733 | 15,3 |
| Этап 2 (сетевая защита) | 94,5 | 1 326 | 10,0 |
| Этап 3 (WAF + антибот) | 96,8 | 341 | 4,4 |
| Этап 4 (Graceful Degradation) | 98,5 | 226 | 1,5 |

**Результаты и обсуждение.** Тестирование разработанной методики на исследовательском стенде подтвердило её эффективность для всех трёх классов DDoS-угроз (таблица 1). Ключевые результаты по сценариям распределились следующим образом.

Для сценария A (volumetric-атака) решающий вклад внесли блоки 1 и 2: после включения сервиса очистки трафика (этап 2) доступность возросла с 94,2% до 98,5%, загрузка внутренних каналов не превысила 65%, а время реакции системы на превышение порогов сократилось с ~12 минут до ~3 минут.

Для сценария B (HTTP-flood) определяющими стали блоки 2 и 3. Внедрение WAF, сессионного анализа и адаптивного rate limiting снизило долю ошибок 5xx с 15,4% до 1,1% при сохранении сопоставимой совокупной нагрузки. Доля ложноположительных срабатываний составила 0,3% легитимного трафика.

Наиболее значимый относительный эффект достигнут в сценарии C (поведенческая L7-атака), где традиционные средства сетевой фильтрации практически неэффективны. Активация механизмов Graceful Degradation и алгоритма Circuit Breaker позволила снизить пиковую загрузку CPU с 92% до 58%, поднять доступность ключевых операций

с 88,0% до 98,5%, при этом интерфейс личного кабинета и платёжные операции оставались стабильными на протяжении всего испытания [8].

Полученные значения средней доступности сервисов (98,5%) и доли ошибок 5xx (1,5%) соответствуют целевым показателям SLA для критичных сервисов финансовых организаций и требованиям НБРК/АРРФР к непрерывности деятельности.

**Заключение.** В статье представлена комплексная методика минимизации последствий DDoS-атак, разработанная на основе экспериментального исследования трёх репрезентативных сценариев атак на изолированном исследовательском стенде. Методика сочетает технические меры (многоуровневая фильтрация трафика, адаптивное управление ресурсами) с организационными (формализованные плейбуки, непрерывный мониторинг) и обеспечивает итоговое повышение доступности сервисов с 91,5% до 98,5%.

Особую практическую значимость представляет блок адаптивного управления ресурсами (Graceful Degradation), обеспечивающий защиту от поведенческих L7-атак — наиболее сложного и быстро растущего класса угроз, против которого традиционные сетевые средства демонстрируют ограниченную эффективность. Разработанная методика может быть применена финансовыми организациями, операторами связи и операторами критической информационной инфраструктуры Республики Казахстан для повышения киберустойчивости и соответствия нормативным требованиям регуляторов.

**Список литературы:**

1. Kaspersky. A deep dive into DDoS attacks: evolution, trends and countermeasures. – 2021. – 32 p.

2. Bawany N.Z., Shamsi J.A. Recent advances and challenges in DDoS attacks and defense mechanisms // Computer Science Review. – 2021. – Vol. 41. – 100413.

3. Цифровой кодекс Республики Казахстан (Кодекс РК от 9 января 2026 года № 255-VIII ЗРК).

4. Zargar S.T., Joshi J., Tipper D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks // IEEE Communications Surveys & Tutorials. – 2019. – Vol. 21, № 4. – P. 301–327.

5. Kolias C., Kambourakis G., Stavrou A., Gritzalis S. DDoS in the IoT: Mirai and other botnets // Computer. – 2019. – Vol. 52, № 7. – P. 80–84.

6. Positive Technologies. Киберугрозы финансовой отрасли 2021–2022. – М.: Positive Technologies, 2022. – 36 с.

7. NIST Special Publication 800-61 Rev. 2. Computer Security Incident Handling Guide. – Gaithersburg: NIST, 2019. – 79 p.

8. Splunk, Oxford Economics. The Hidden Costs of Downtime: How incidents impact revenue and reputation. – 2022. – 28 p.

9. Gartner. Distributed denial of service attacks: business impact and mitigation trends 2022–2024. – Stamford, 2022. – 30 p.

10. Баранова Е.К., Гырнец К.В. Современные DDoS-атаки как угроза для бизнеса в интернете // Защита информации и безопасность. – 2025. – № 3. – С. 155–161.

11. Ильясов Б.М. Исследование модели защиты от DDoS-атак // Вестник технического университета. – 2024. – Т. 18, № 3. – С. 45–54.

12. SmartCloud. Защита от DDoS-атак в Казахстане: технические решения и практика внедрения. – Астана: SmartCloud, 2022. – 20 с.

**ӘОЖ 004.42:004.946**

**Рыспаева Дариха Сабитовна**

Оқытушы
Астана халықаралық университеті
(Астана қ., Қазақстан)

**Наурызбаева Сая Аманжоловна**

Оқытушы
Астана халықаралық университеті
(Астана қ., Қазақстан)

# ХОРРОР НЕГІЗІНДЕ ОЙ ЖҰМБАҚ ЭЛЕМЕНТТЕРІН ҚОЛДАНЫП ОЙЫН ҚҰРУ

**Аңдатпа:** Бұл мақалада дербес компьютерлерге арналған, басқатырғыш элементтері бар хоррор ойынын әзірлеу барысы сипатталады. Ойыншыларды үрей мен шиеленіс атмосферасына тартатын ерекше тұжырымдама жасауға басты назар аударылды. Сюжет желісін, кейіпкерлерді және қоршаған ортаны егжей-тегжейлі пысықтау жобаның негізгі бөлігіне айналды. Бағдарламалау, геймдизайн және визуалды өнер элементтерін біріктіру арқылы толыққанды өнім жасалды. Сонымен қатар, жобаның сапасы мен бірегейлігін қамтамасыз ету мақсатында аудиторияның сұраныстары мен нарықтағы танымал хоррор ойындарына талдау жүргізілді.

Ойын барысында кездесетін тапсырмаларды шешу арқылы пайдаланушылар өздерінің логикалық және сыни ойлау қабілеттерін дамытады, бұл жұмыстың негізгі практикалық маңыздылығын көрсетеді.

**Кілт сөздер:** дербес компьютер ойындары, Unity ортасы, хоррор жанры, басқатырғыштар, сыни тұрғыдан ойлау, үшөлшемді графика (3D), ойын қозғалтқышы, кейіпкерлер анимациясы, виртуалды лабиринт.

**Кіріспе.** Бүгінде бейнеойындарды жай ғана бос уақыт өткізетін ермек деуге ауыз бармайды. Бұл — миллиардтаған айналымы бар, бәсекесі қазандай қайнап жатқан тұтас бір алып индустрия. Қазіргі талғамы биік ойыншыларды таңғалдыру үшін құрғақ код жазып қою мүлдем аздық етеді. Оған көздің жауын алатын визуал, ешкімге ұқсамайтын креатив пен мінсіз техникалық шешімдер ауадай қажет.

Дегенмен, бағымызға орай, қазіргі заманауи құралдар әзірлеушілердің жұмысын әлдеқайда жеңілдетіп тастады. Мәселен, Unity немесе Unreal Engine сияқты мықты қозғалтқыштар қазір кез келген адамға қолжетімді. Осылардың көмегімен жас мамандар күрделі математикалық формулалар мен физика заңдылықтарына бас қатырмай-ақ, нарыққа сапалы әрі бәсекеге қабілетті өнім шығаруға толық мүмкіндік алды.

Жұмысымның басты өзектілігі де дәл осыған саяды: интерактивті қосымшалар жасағанда жаңа алгоритмдерді қалай ұтымды, қалай тиімді пайдалануға болады? Алға қойған негізгі мақсат — Unity базасында толыққанды, сапалы хоррор ойынын жасап шығару. Бірақ мақсат тек адамды қорқытып, үрейлендіру емес. Ойынның ішіне түрлі

логикалық басқатырғыштарды шебер кіріктіру арқылы геймерді терең ойлануға, миын істетуге мәжбүрлеуді көздедім.

Зерттеу нысаны етіп Unity қозғалтқышының кең-байтақ техникалық мүмкіндіктерін алдым. Ал зерттеу пәнім — тікелей осы хоррор жанрының өзіне тән ішкі ерекшеліктері. Жұмыстың ғылыми жаңалығы неде десеңіз, бұл жобада ойын механикасын құрудың жаңа алгоритмдік шешімдері құр қағаз жүзінде емес, нақты тәжірибеде сыналады. Одан бөлек, деңгей дизайнын жасау барысында бір-біріне ұқсамайтын бірнеше түрлі тәсілді біріктіріп, синтездеп қолдандым.

**Материалдар мен тәсілдер.** Жалпы, жұрттың зәре-құтын қашыратын қорқынышты ойын жасау сырттай оңай көрінгенімен, іс жүзінде өте ауыр шаруа. Бұл таусылмас шығармашылық ізденісті, әрбір ұсақ-түйек детальға үңілуді және темірдей нақты жоспарды талап етеді. Хоррордың ең басты миссиясы — геймердің психологиясына тікелей шабуыл жасау, оны үрейлендіріп қана қоймай, бастан-аяқ белгісіздіктің, түсініксіз қысымның астында ұстау. Дәл осы атмосфераны бұзбай жеткізу үшін бүкіл әзірлеу процесін бірнеше нақты кезеңге бөліп тастадым.

- Біріншісі — тұжырымдама жасау. Барлығы осыдан басталады: негізгі идея туындайды, оқиға желісі жазылады, бас кейіпкерлердің болмысы мен басты ойын механикалары нақтыланады.
- Екіншісі — деңгей архитектурасы немесе левел-дизайн (Level design). Бұл кезеңде виртуалды әлемнің қаңқасы тұрғызылады. Ойыншыны қай бұрыштa қорқытамыз, қандай тұзақтар қоямыз, кедергілер картаның қай тұсында тұруы керек — осының бәрі мұқият есептеледі.
- Үшінші саты — ойын дизайны (Game design). Мұнда ойын ережелерінің мінсіз жұмыс істеуі қадағаланады. Тапсырмалар тым қиын болып кетпеуі керек, бірақ тым оңай да болмауы шарт — нағыз баланс осы жерде реттеледі. Сонымен қатар, ойыншының қоршаған ортамен қалай байланысатыны шешіледі.
- Төртіншісі — аудио дизайн. Хоррорда дыбыстың рөлі қаншалықты зор екенін айтып жатудың өзі артық. Жүйкені жұқартатын фондық музыка мен аяқастынан шығатын түрлі дыбыстарды дәл тауып қою арқылы психологиялық шиеленіс шарықтау шегіне жеткізіледі.
- Және соңғысы — графика мен визуал. Ойыншы ортаның шынайылығына сенуі үшін текстуралар, жарық пен көлеңкенің жұмбақ ойыны, сондай-ақ барлық нысандардың 3D-модельдері барынша шынайы әрі жан-жақты бапталады.

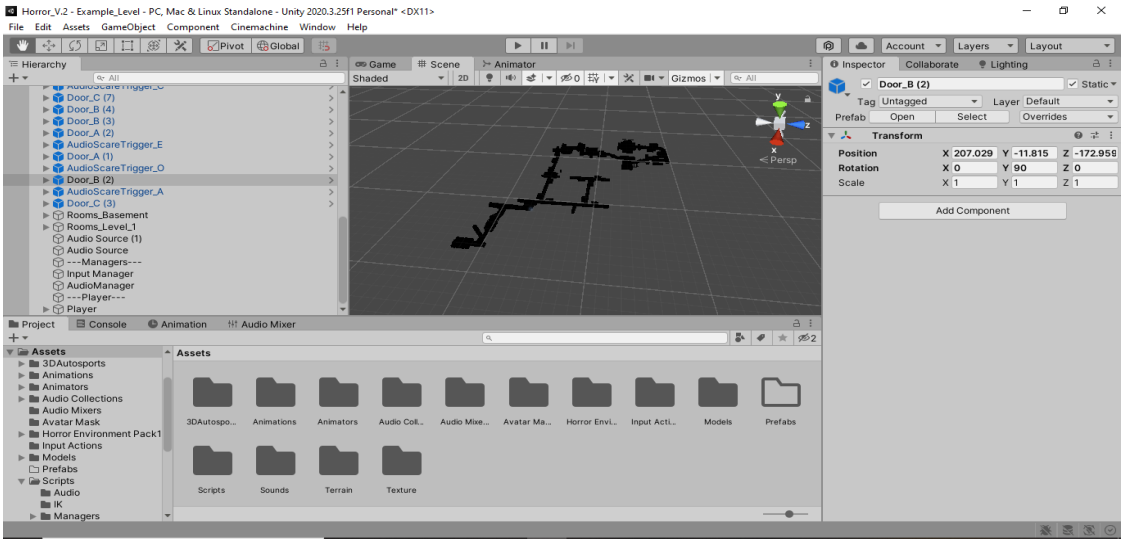
Жұмыстың бастапқы сатысы – виртуалды кеңістікті, яғни ойын деңгейін (локациясын) қалыптастыру. Дәл осы кезеңде жобаның базалық архитектурасы құрастырылады. Ортаны мейлінше шынайы және толыққанды етіп көрсету үшін түрлі 3D-модельдер іске қосылады. Қажетті нысандарды ашық дереккөздерден дайын күйінде жүктеп алуға немесе автордың өзі арнайы бағдарламаларда нөлден бастап құрастырып шығуына толық мүмкіндік бар.

Картаның ішіне қабырға, есік-терезе, түрлі жиһаздар, жарықтандыру көздері мен өзге де безендіру бөлшектері орналастырылады. Хоррор жанрындағы жобалар үшін әрбір ұсақ-түйектің өзіндік маңызы бар, себебі олар жалпы атмосфераны қалыптастыруға

тікелей қатысады. Сахнадағы заттардың дұрыс әрі үйлесімді қойылуы пайдаланушының психологиясына әсер етіп, оны үнемі қорқыныш пен белгісіздік қысымында ұстауға көмектеседі.

Бұған қоса, локацияның логикалық реттілігін де қатаң ескерген жөн. Пайдаланушының ойынды қай нүктеден бастайтыны, одан әрі қандай бағытпен жүретіні және қандай бөлмелерге кіре алатыны – барлығы алдын ала нақты есептелуі шарт. Мысалы, жарығы аз тар дәліздер, кішкене бөлмелер немесе аяқастынан кеңейіп кететін локациялар ойыншының бойындағы үрей сезімін еселей түсуге таптырмас құрал болып табылады.

Қорыта айтқанда, деңгей дизайнын жасау – кез келген бейнеойынның іргетасын қалайтын ең маңызды әрі жауапты кезеңдердің бірі.



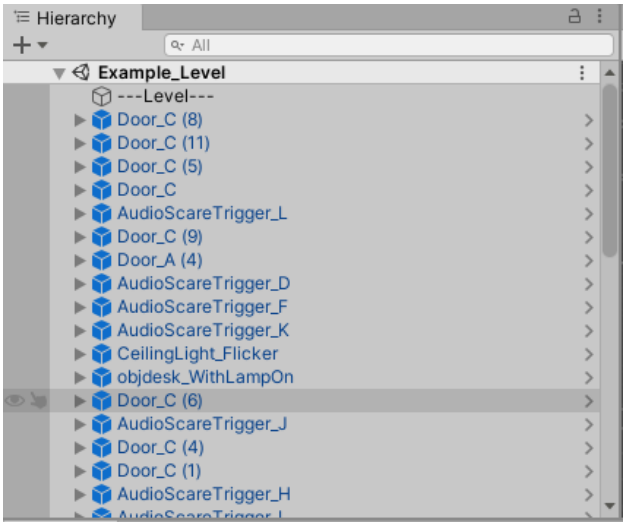

1-сурет. Ойын локациясының жалпы құрылымы мен картасы

Ойын локациясы негізгі концепция ретінде жер астында орналасқан құпия ғылыми зертхана базасы түрінде жобаланды. Басты кейіпкердің алдында тұрған басты мақсат – осы жабық кешеннен аман-есен құтылып шығу. Бұл міндетті орындау үшін пайдаланушы жол бойында кездесетін түрлі логикалық кедергілер мен қауіптерді еңсеруі қажет.

Кешеннің ішкі интерьері ғылыми-техникалық нысанның стиліне толықтай сай жасақталған. Картадан жарығы нашар тар дәліздерді, құлыптаулы бөлмелерді, сондай-ақ жұмыс істеу принципі жұмбақ күрделі құрал-жабдықтар мен аппараттарды көруге болады. Ойын ортасының жалпы атмосферасы суық, тылсым әрі үрейлі сезім сыйлайтындай етіп құрылған. Мұндай визуалдық және психологиялық қысым ойыншыны үнемі қолайсыз жағдайда ұстап, кез келген қауіпке дайын болуға және әр қадамын аса сақтықпен басуға итермелейді.

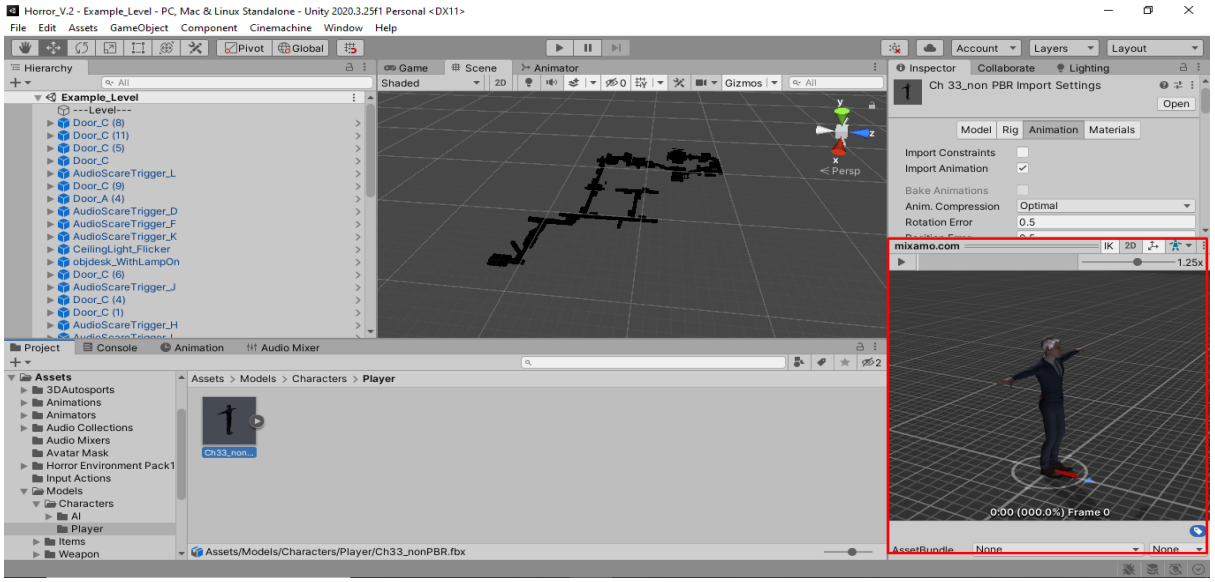

2-сурет. Зертхана бөлмесінің ішкі интерьері мен дизайны

Ойын сахнасына орналастырылған барлық элементтердің толық тізімі арнайы «Иерархия» (Hierarchy) панелінде көрсетіледі. Бұл терезенің көмегімен әзірлеуші виртуалды кеңістіктегі кез келген объектіні оңай тауып, оның қасиеттерін өңдеу немесе жалпы басқару жұмыстарын кедергісіз жүргізе алады.



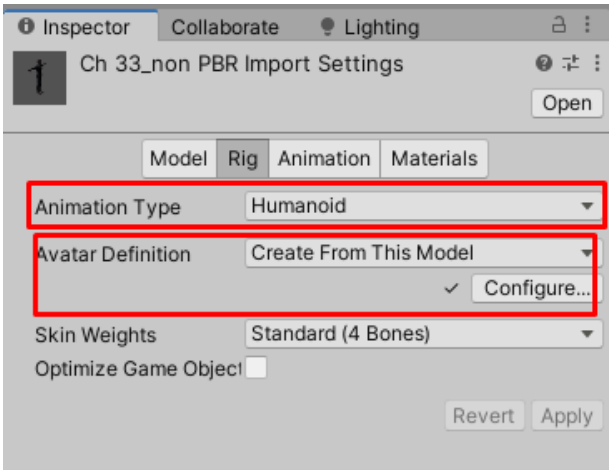

3-сурет. Сахнадағы объектілерді басқаруға арналған иерархия панелі

Ойын жобасындағы басты персонаждың визуалды бейнесін қалыптастыру жұмыстары ең алдымен сапалы 3D-модельді таңдап алудан бастау алады. Қазіргі кезде мұндай графикалық нысандарды міндетті түрде нөлден сызып әуре болудың қажеті жоқ, өйткені интернеттегі түрлі ашық қорлар оларды дайын күйінде ұсынады. Солардың ішіндегі ең танымалысы – Mixamo веб-сервисі. Бұл платформа ойын жасаушыларға алуан түрлі үшөлшемді кейіпкерлерді ешқандай ақы төлеместен, еркін жүктеп алып пайдалануға таптырмас мүмкіндік береді.




4-сурет. Жүйеге жүктеліп алынған басты кейіпкердің 3D-моделі

Жоба үшін таңдап алынған бұл кейіпкер гуманоид (адам пішінді) модельдер тобына кіреді. Оны ең алдымен ойын қозғалтқышына жүктеп алып, базалық баптауларын ретке келтіріп алу өте маңызды. Осындай алғашқы дайындықтан соң ғана персонаждың қимыл-қозғалысын басқаратын арнайы Rig (виртуалды қаңқа) жүйесін құрастыруға кірісеміз.

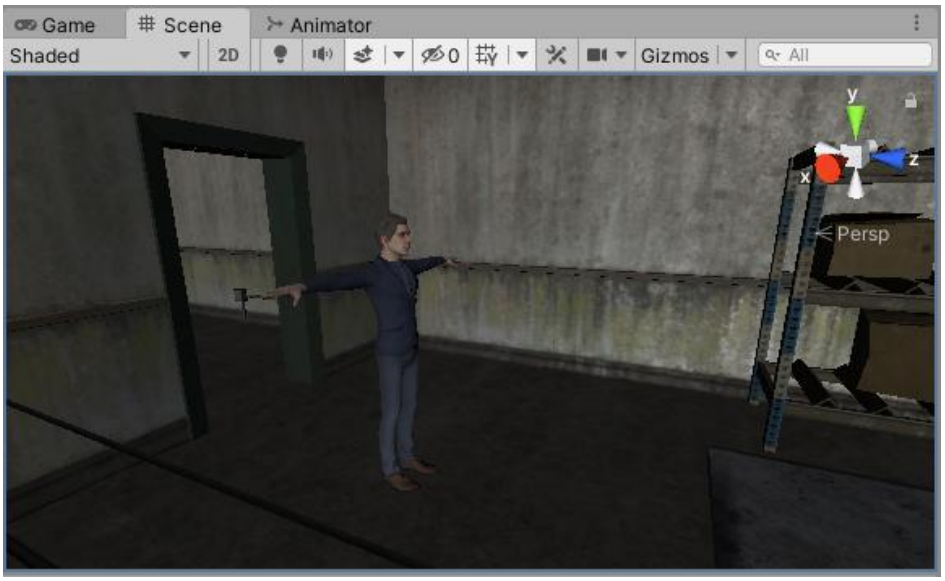



5-сурет. Анимациялық қаңқаны (Rig) баптау процесі

Модельді (кейіпкерді немесе нысанды) жүктеп алған соң, іс мұнымен бітпейді. Оның ішкі параметрлерін баптап, қозғалтқыштың (engine) тіліне бейімдеу қажет. Бұл тұста басты назарды екі маңызды нәрсеге бұрдым.

* Animation Type, яғни анимация түрі. Ол кейіпкердің виртуалды әлемде қалай жүріп-тұратынын, қалай қозғалатынын және жалпы физикасын толықтай шешіп береді.

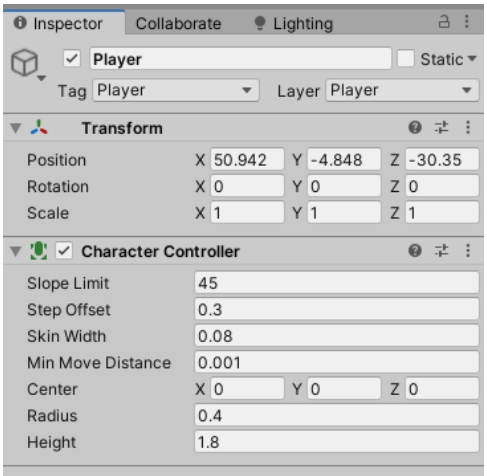
*Avatar Definition (Аватарды анықтау). Бұл өте қажетті баптау. Ол арқылы біз ойыншының виртуалды бейнесін қозғалтқышқа «таныстырамыз», яғни модельдің сүйек жүйесін (rig) жүйеге толық тіркейміз. Онсыз кейіпкер дұрыс қимылдамайды.




6-сурет. Дайын болған ойыншы персонажын виртуалды сахнаға орналастыру

Кейіпкерді (Player) картаға қосқаннан кейін, оны жансыз қуыршақ күйінде қалдырмай, мұқият баптау қажет. Бұл үшін бізге арнайы компоненттер көмекке келеді. Олардың ішіндегі ең маңыздысы — Character Controller.

Дәл осы модуль кейіпкердің ойын кеңістігіндегі барлық қозғалысын тікелей басқарады. Мәселен, ол ауада қалқып жүрмей, гравитация заңына бағынып, жерге нық басып жүруі шарт. Оған қоса, персонаж қабырғалардан елес құсап өтіп кетпеуі немесе басқа нысандардың ішіне кіріп кетпеуі керек. Қоршаған ортадағы кедергілерге соғылу, яғни коллизия (collision) процесін реттеу де толықтай осы контроллердің мойнында.




7-сурет. Player нысанының толыққанды жұмысы үшін негізгі контроллерлерді бекіту

Ойыншының базалық параметрлерін баптап болған соң, келесі кезекте бағдарламалық кодтарды (скрипттерді) жазу кезеңіне өтеміз.

Ойын логикасын бағдарламалау

Жобадағы басты кейіпкердің жұмысы нақты бір қызметке жауап беретін бірнеше өзара байланысты модульдер арқылы жүзеге асырылады. Біздің жобадағы ойыншы нысаны келесідей негізгі компоненттерден тұрады:

PlayerController: Басты кейіпкердің кеңістіктегі базалық іс-әрекеттерін (орын ауыстыру, бағытын өзгерту және т.б.) басқаруды қамтамасыз ететін орталық компонент.

InputManager: Пайдаланушының пернетақтадан немесе өзге құрылғылардан берген командаларын қабылдайтын модуль. Бұл жүйе Unity платформасының жаңартылған енгізу жүйесі (New Input System) негізінде жұмыс істейді.

StateMachine: Ойыншының әртүрлі жағдайлары мен күйлерін алмастыруға (мысалы, анимациялардың бірқалыпты ауысуына) жауап беретін басқарушы құрылым. Бұл компонентті әзірлеу барысында бағдарламалаудың мінез-құлықтық паттерні – State (Күй) архитектуралық үлгісі қолданылды.

State: Әрбір жеке қимыл немесе әрекеттің (күйдің) өзін сипаттайтын модуль.

StateController: Кейіпкердің нақты күйлерін (мысалы, тыныш тұру – idle, жүру – walk, жүгіру – sprint, секіру – jump) іске қосатын және олардың реттілігін қадағалайтын компонент.

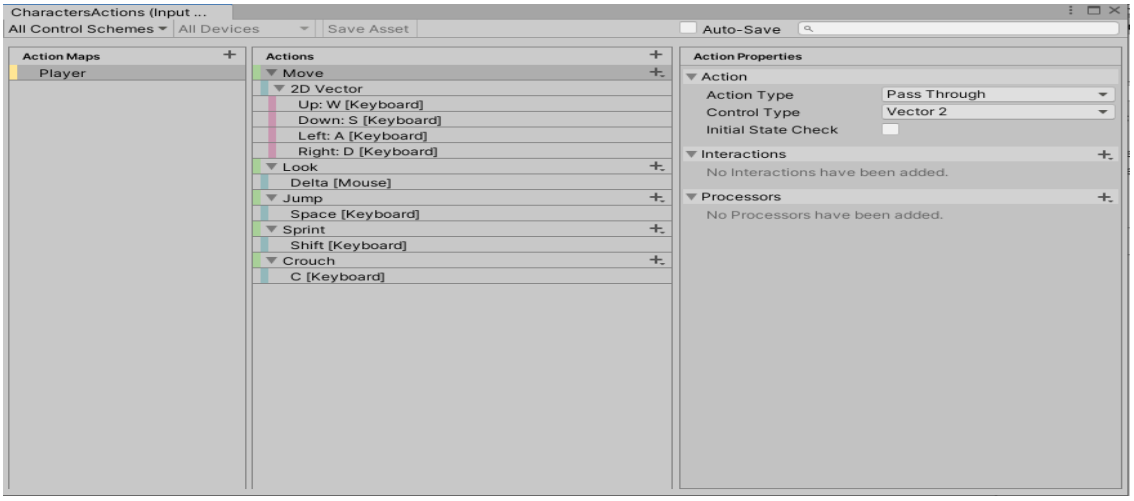
AudioManager: Жалпы ойын барысындағы, оның ішінде тікелей ойыншыға тиесілі әртүрлі дыбыстық эффектілерді (мысалы, жүрген кездегі қадамдардың сыбдырын) уақытылы қосып, реттеп отыратын басты менеджер.

Ойынның код бөлігін жазу барысында біз объектіге бағытталған бағдарламалаудың танымал SOLID стандартына сүйендік. Оның ішінде дәл осы архитектураға Single Responsibility (Бірыңғай жауапкершілік) қағидасы негіз болды. Бұл дегеніміз, жобадағы әрбір жеке компонент немесе скрипт барлық процеске бірдей араласпай, тек өзіне ғана жүктелген бір нақты қызметке жауап береді. Бұлайша бөліп жазу кодтың құрылымын әлдеқайда түсінікті етеді және ойынның қатып қалмай, тұрақты жұмыс істеуіне тікелей әсер етеді.

Осы жүйені іс жүзінде бағдарламалау кезеңін біз ең алдымен InputManager (Енгізу менеджері) скриптін жасаудан бастадық.

Жүйені бағдарламалау процесі алдымен InputManager (Енгізу менеджері) скриптін құрудан басталады.

Бұл модульдің негізгі қызметі – пайдаланушының пернелерді басу оқиғаларын тіркеп, өңдеу. Сценарий Unity-дің Жаңа енгізу жүйесімен (New Input System) тығыз байланыста жұмыс істейді. Жаңа жүйенің ескі нұсқалардан басты артықшылығы – оның оқиғаға негізделген (event-driven) архитектураға құрылуында. Жаңа енгізу жүйесінің құрылымы төмендегідей:




8-сурет. Жаңа жүйе негізінде енгізу командаларын (Input Actions) тіркеу қадамы

**Қорытынды.** Осы ауқымды жобаны бастан-аяқ жасап шыққаннан кейін бір нәрсеге көзім анық жетті: нөлден бастап толыққанды хоррор ойынын жинап шығу — сырт көз ойлағандай оңай шаруа емес. Бірақ бұл өте қызық әрі шығармашылыққа толы процесс. Бүгінгі таңда Unity немесе Unreal Engine сияқты қуатты қозғалтқыштарсыз бәсекеге қабілетті жоба шығару мүмкін емес дерлік. Неге? Өйткені олар күрделі дүниенің бәрін бір орталыққа біріктіреді. Графиканы реттеу, кейіпкерге жан бітіру немесе жауларға жасанды интеллект қосу — осының бәрі бір жерден басқарылады. Ойыншыны шын мәнінде үрейлендіретін атмосфера құру үшін ең әуелі осындай мықты техникалық іргетас керек екенін түсіндім.

Екінші маңызды мәселе — визуал. Монитордың ар жағында отырған адамды виртуалды әлемнің шынайылығына сендіру үшін 3D модельдер мінсіз болуы шарт. Үстел үстінде жатқан кішкентай заттан бастап, алып бөлмелерге дейін нанымды көрінуі тиіс. Графикада кішкене ғана "жасандылық" байқалса болды, ойыншының бойындағы қорқыныш сезімі лезде жойылып кетеді. Дәл осы себепті текстураларды, жарық пен көлеңке ойынын баптауға өте көп уақыт пен еңбек жұмсауға тура келді.

Дегенмен, жалаң әдемі суретпен алысқа бару мүмкін емес. Оны тірілтіп, қозғалту қажет. Анимацияларды табиғи қалыпқа келтіру процесі біраз тер төгуді талап етті. Персонаждың немесе жаулардың қимылы жасанды болса, ойынның бүкіл сәні кетеді. Мәселен, қараңғы бөлменің есігі ашылғанда немесе алдыңнан кенеттен бірдеңе атып шыққанда, оның анимациясы шынайы болмаса, ешкім де шошымайды. Сондықтан кинематикаға ерекше мән берілді.

Хоррор жанрының ең басты, ең қауіпті қаруы — дыбыс. Онсыз қорқыныш жайлы айтудың өзі артық. Жобада аудио-дизайнға барынша мұқият қарадық. Сықырлаған еден, аяқтың басқан дыбысы, жүйкені жұқартатын фондық музыка және әсіресе spatial audio (кеңістіктегі дыбыс) эффектілері тікелей адамның миына әсер етеді. Ойыншыны үнемі белгісіздік пен қысымда ұстайтын да осы көрінбейтін дыбыстар.

Жобаның негізгі қаңқасы толық тұрғызылғаннан кейін міндетті түрде тестілеу кезеңі басталды. Әрине, күткендегідей багтар (қателер) көптеп шықты. Олардың барлығын дерлік қолдан келгенше жөндеп, оңтайландырдық. Басқару геймерге барынша ыңғайлы болуын және ойынның ауырлап, қатып қалмауын қадағаладық. Осы қатаң тексерістердің арқасында ойынды тұрақты, ойнауға жарамды қалыпқа келтіре алдық.

Түйіндей келсек, заманауи IT-құралдарды сауатты пайдалана отырып, ішінде күрделі логикалық басқатырғыштары бар сапалы хоррор ойынын жасап шығару әбден мүмкін екенін тәжірибе жүзінде дәлелдедік. Таза жазылған код, шынайы 3D модельдер, сапалы дыбыс және табиғи анимация бір арнаға тоғысқанда ғана нағыз өнім дүниеге келеді. Алдағы уақытта бұл жобаны одан әрі дамытып, жаңа бөлмелер қосу, сюжетті кеңейту және басқатырғыштарды бұдан да күрделірек ету жоспарда бар.

**Әдебиеттер тізімі:**

1. Marhulets W. 100 Game Design Tips and Tricks (перевод на русский) // 2015.

2. Jesse Schell. Геймдизайн. Как создать игру, в которую будут играть все. – М.: 2019.

3. Tynan Sylvester. Геймдизайн. Рецепты успеха лучших компьютерных игр от Super Mario и Doom до Assassin’s Creed и дальше. – 2016.

4. Harro Grönberg, Konsta Klemetti. Мастера геймдизайна: Как создавались Angry Birds, Max Payne и другие игры-бестселлеры. – 2015.

5. Robert Zubek. Элементы гейм-дизайна. Как создавать игры, от которых невозможно оторваться. – 2020.

6. Tanya X. Short, Tarn Adams. Procedural Generation in Game Design. – 2017.

7. Nicholas Lovell. The Pyramid of Game Design. – 2017.

8. Scott Rogers. Level Up! The Guide to Great Video Game Design. – 2014.

9. Katherine Isbister. How Games Move Us: Emotion by Design. – 2016.

10. Ernest Adams. Game Mechanics: Advanced Game Design. – 2012.

11. Steve Swink. Game Feel: A Game Designer's Guide to Virtual Sensation. – 2009.

12. Tracy Fullerton. Game Design Workshop: A Playcentric Approach to Creating Innovative Games. – 2014.

13. Tynan Sylvester. Designing Games: A Guide to Engineering Experiences. – 2013.

14. Tim Fields. Social Game Design: Monetization Methods and Mechanics. – 2014.

**УДК 004.85**

**Серикханов Диас Хайдарұлы**
магистрант 2 курса
**Научный руководитель:** Ахметов Б. С.
д.т.н., профессор
Казахский университет технологии и бизнеса им. К.Кулажанова
(г. Астана, Казахстан)

# СРАВНИТЕЛЬНЫЙ АНАЛИЗ АРХИТЕКТУР ГЛУБОКОГО ОБУЧЕНИЯ ДЛЯ РАСПОЗНАВАНИЯ ПРОДУКТОВ ПИТАНИЯ В МОБИЛЬНЫХ ПРИЛОЖЕНИЯХ

**Аннотация**: В работе выполнен сравнительный анализ современных архитектур глубокого обучения для распознавания продуктов питания в мобильных приложениях. Рассмотрены ключевые подходы: традиционные CNN (ResNet), мобильно-оптимизированные архитектуры (MobileNetV3, EfficientNet), трансформерные модели (ViT) и гибридные решения (EHFR-Net). Предложена система из семи критериев оценки эффективности. На основе анализа установлено, что EfficientNet-B0 достигает наивысшей точности (98.10%), а MobileNetV3 обеспечивает оптимальное соотношение точности (97.63%) и вычислительной эффективности. Разработана концептуальная модель системы автоматического подсчёта калорий.

**Ключевые слова**: Распознавание продуктов питания; глубокое обучение; мобильные приложения; MobileNetV3; EfficientNet; Vision Transformer; оценка калорийности; edge computing.

**Введение.** Вопросы здорового питания и контроля калорийности рациона приобретают особую значимость в контексте глобальных проблем общественного здравоохранения. По данным ВОЗ, 2,5 миллиарда взрослых (43% населения старше 18 лет) имеют избыточную массу тела [1].

Традиционные методы контроля рациона характеризуются высокой трудоёмкостью и низкой вовлечённостью пользователей [2]. Развитие методов компьютерного зрения и глубокого обучения открывает возможности для автоматизации анализа пищевого рациона. Современные мобильные устройства позволяют создавать системы, способные определять тип продукта, оценивать размер порции и рассчитывать пищевую ценность на основе одного изображения [3], [4].

Современные исследования демонстрируют, что EfficientNet-B0 достигает 98.10% точности, а MobileNetV3-Small демонстрирует 97.63% при меньших вычислительных затратах [7]. Однако системы автоматического распознавания сталкиваются с проблемами вариативности внешнего вида блюд, анализа многокомпонентных продуктов и оценки размера порции [10].

Целью исследования является проведение сравнительного анализа современных методов глубокого обучения для распознавания продуктов питания и разработка концептуальной модели системы автоматического подсчёта калорий для мобильных приложений.

**Проблематика распознавания продуктов питания.** Системы автоматического анализа пищевого рациона сталкиваются с технологическими ограничениями. Ключевые

проблемы связаны с вариативностью визуальных характеристик, ограниченностью вычислительных ресурсов и сложностью оценки массы продуктов.

Вариативность внешнего вида. Food-101 dataset характеризуется большой внутриклассовой изменчивостью и межклассовым сходством [11]. Для решения применяются методы data augmentation и continual learning [2].

Ограничения вычислительных ресурсов. Высокоточные архитектуры, такие как Vision Transformer, требуют значительных ресурсов [8]. Актуальны лёгковесные архитектуры MobileNetV3 и EfficientNet-Lite, которые успешно развёртываются на мобильных устройствах [9].

Проблема оценки размера порции. Определение массы продукта на основе 2D изображения затруднено отсутствием информации о глубине. Методы на основе depth estimation достигают погрешности около 10-20% [10].

**Цель и методология исследования** . Целью работы является систематизация и сравнительный анализ современных архитектур глубокого обучения для распознавания продуктов питания с учётом точности, вычислительной эффективности и практической применимости.

Задачи исследования:

- Классификация архитектур глубокого обучения
- Определение критериев оценки эффективности
- Сравнительный анализ архитектур
- Разработка концептуальной модели системы подсчёта калорий

Методология базируется на анализе публикаций 2021–2025 годов в ведущих источниках (IEEE, MDPI, ACM, Elsevier, arXiv). Критерии оценки: точность классификации, скорость обработки, размер модели, энергоэффективность, точность оценки порции, устойчивость к условиям съёмки, удобство интеграции. Каждая архитектура оценивалась по шкале 1-5.

**Классификация подходов к распознаванию продуктов питания.** Современные методы основаны на различных архитектурных подходах, отличающихся по сложности, точности и применению.

Традиционные CNN-архитектуры (VGG, ResNet, Inception) обеспечивают высокую точность за счёт глубокой иерархии признаков, но имеют большую вычислительную сложность [13].

Мобильно-оптимизированные архитектуры (MobileNetV3, SqueezeNet) используют depthwise separable convolutions для снижения нагрузки. MobileNetV3-Small достигает 97.63% точности на мобильных устройствах [7], [9].

EfficientNet и масштабируемые архитектуры основаны на принципе compound scaling, обеспечивая баланс точности и эффективности. EfficientNet-B0 достигает 98.10% точности [7].

Transformer-based модели (ViT) используют механизм self-attention для извлечения глобальных зависимостей [15]. Демонстрируют высокую точность, но требуют больших ресурсов.

Гибридные подходы. EHFR-Net достигает 90.7% Top-1 accuracy на Food-101 при 2.8M параметров, превосходя MobileNetV3 (86.2%) и EfficientNet-B0 (85.2%) [8].

**Критерии оценки эффективности архитектур.** Для объективного сравнения определена система критериев, отражающих практическую эффективность для мобильных приложений:

1. Точность классификации — Top-1 и Top-5 accuracy на эталонных датасетах (Food-101, Nutrition5k). Значения варьируются в диапазоне 85–98% [7], [8].
2. Скорость обработки — latency и FPS. Для мобильных приложений критично latency < 100 мс [9].
3. Размер модели — параметры и объём памяти. Предпочтительны модели до 10–15 МБ. EHFR-Net-0.5 достигает 89.4% точности при 0.8M параметров [8].
4. Энергоэффективность — уровень энергопотребления при инференсе [9].
5. Точность оценки порции — погрешность определения массы составляет 10–20% [10].
6. Устойчивость к условиям съёмки — робастность к изменениям освещения и ракурса [2].
7. Удобство интеграции — поддержка TensorFlow Lite, Core ML и наличие предобученных весов.

**Сравнительный анализ архитектур.** Проведена сравнительная оценка архитектур глубокого обучения на основе предложенных критериев. EHFR-Net-0.5 демонстрирует наилучшее соотношение размера модели (0.8M параметров) и скорости (140 FPS) при приемлемой точности (89.4%) [8].

**Таблица 1 - Сравнительные характеристики архитектур глубокого обучения.**

| Архитектура | Топ-1 Acc (%) | Параметры (M) | Скорость (FPS) | Энерго-эфф. | Источник |
|---|---|---|---|---|---|
| MobileNetV3-Small | 97.63 | 2.5 | 120+ | ★★★★★ | [7, 9] |
| EfficientNet-B0 | 98.10 | 5.3 | 100 | ★★★★☆ | [7] |
| EHFR-Net | 90.7 (Food-101) | 2.8 | 95 | ★★★★☆ | [8] |
| EHFR-Net-0.5 | 89.4 | 0.8 | 140 | ★★★★★ | [8] |
| ViT-B/16 | 94.42 | 86 | 25 | ★★☆☆☆ | [7] |
| ResNet-50 | 94.0 | 25.6 | 45 | ★★☆☆☆ | [13] |

Обобщённые результаты:

- MobileNetV3 демонстрирует наилучшую скорость обработки и энергоэффективность, достигая 97.63% точности [7], оптимален для мобильных приложений.
- EfficientNet-Lite обеспечивает наиболее сбалансированное соотношение точности (до 98.10%) и производительности [7].
- ResNet-50 характеризуется высокой точностью и устойчивостью, но уступает по скорости.
- Vision Transformer демонстрирует 94.42% точности, но требует значительных вычислительных ресурсов [7].
- Гибридные архитектуры (EHFR-Net) достигают 90.7% Top-1 accuracy при 2.8M параметров, превосходя традиционные мобильные архитектуры [8].

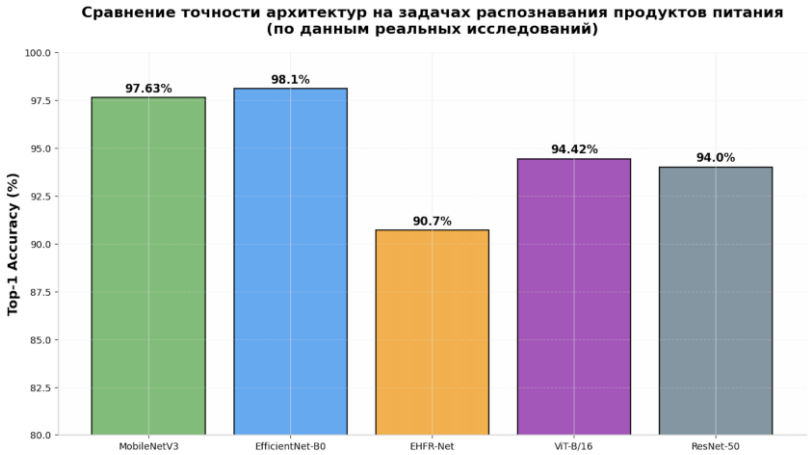



Рисунок 1. Сравнение Top-1 accuracy архитектур на задачах распознавания продуктов питания.

Анализ показывает компромисс между точностью классификации и вычислительной эффективностью. MobileNetV3 и EfficientNet-B0 обеспечивают высокую точность (>97%) при небольшом размере (<5.5M параметров) [7], [9]. Vision Transformer при большем размере (86M параметров) не достигает пропорционального прироста точности (94.42%) [7].

Для наглядного представления многокритериального анализа на рисунке 2 приведена радарная диаграмма, отражающая сильные и слабые стороны каждой архитектуры.

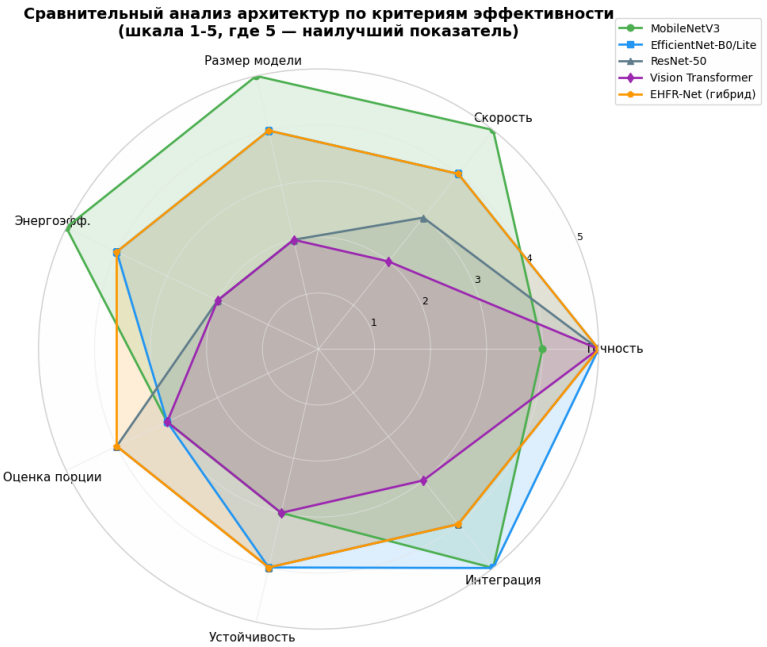



Рисунок 2. Радарная диаграмма сравнения архитектур по критериям эффективности (шкала 1–5, где 5 — наилучший показатель).

Выбор архитектуры определяется сценарием применения. Для мобильных приложений приоритетны скорость и энергоэффективность, что делает MobileNetV3 и

EfficientNet-Lite предпочтительными. В серверных системах целесообразно использование ResNet и Vision Transformer для максимальной точности.

**Обсуждение результатов.** Сравнительный анализ показывает, что эффективность систем определяется совокупностью характеристик, включая точность, скорость, энергоэффективность и устойчивость к условиям съёмки.

На рисунке 3 представлена визуализация компромисса между точностью классификации и размером модели, что является ключевым фактором при выборе архитектуры для мобильных приложений.

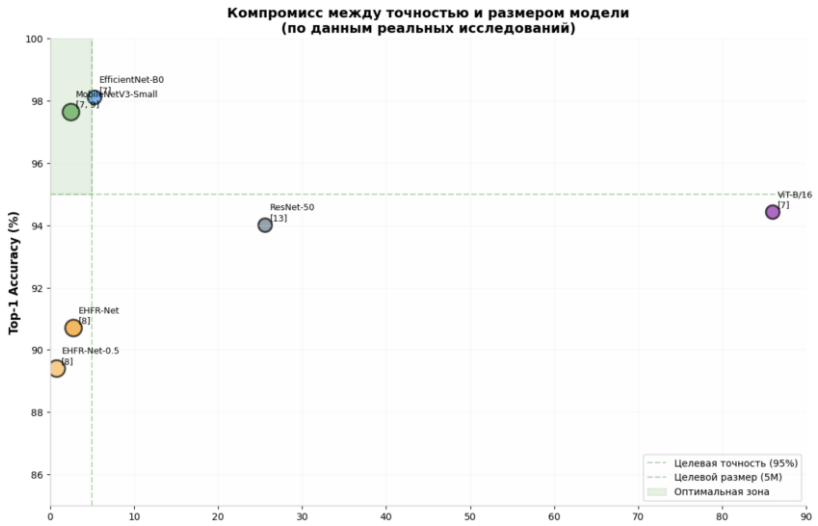



Рисунок 3. Компромисс между точностью и размером модели. Зелёная зона обозначает оптимальные решения (<5M параметров, >95% точность).

MobileNetV3-Small и EfficientNet-B0 обеспечивают высокую точность (>97%) при относительно небольшом размере (<5.5M параметров) [7], [9]. Для мобильных приложений наиболее рациональным является использование EfficientNet-Lite, обеспечивающего оптимальный баланс между точностью (около 98%) и производительностью. MobileNetV3 — альтернатива в сценариях с критичной задержкой и энергопотреблением [9].

Задача оценки размера порции остаётся основным источником погрешности. Даже современные методы сегментации и depth estimation обеспечивают точность 10–20%, что влияет на корректность расчёта калорийности [10]. Перспективным направлением являются многозадачные и гибридные архитектуры [12].

**Концептуальная модель системы автоматического подсчёта калорий.** На основе проведённого анализа разработана концептуальная модель системы автоматического подсчёта калорий, представленная на рисунке 4.


Рисунок 4. Архитектура системы автоматического подсчёта калорий с индикацией используемых компонентов и соответствующих источников.

Предложенная архитектура реализует многоуровневый подход [4], где обработка данных выполняется как на мобильном устройстве (edge-уровень), так и в облаке при необходимости. Edge-уровень использует лёгковесные модели MobileNetV3 [9] или EfficientNet-Lite [7] для первичной классификации, а гибридная модель EHFR-Net [8] обеспечивает уточнение результатов. Для оценки размера порции применяется depth estimation [10], что позволяет достичь погрешности 10–20% [10]. Облачный уровень задействуется для сложных случаев, требующих применения более мощных моделей ViT или ResNet [13], [15], а также для дообучения с использованием multi-task learning [12].

**Заключение.** В работе проведён системный анализ современных методов распознавания продуктов питания на основе компьютерного зрения и глубокого обучения. Рассмотрены ключевые архитектуры: MobileNetV3, EfficientNet, ResNet, Vision Transformer и гибридные модели.

Предложена система критериев оценки эффективности моделей, учитывающая точность, скорость обработки, размер модели, энергоэффективность и устойчивость. Наиболее перспективными для мобильных приложений являются EfficientNet-Lite и MobileNetV3, обеспечивающие баланс между точностью (97–98%) и производительностью. Гибридные модели (EHFR-Net) демонстрируют превосходные результаты (90.7% Top-1 accuracy при 2.8M параметров) [8].

Отдельно отмечена проблема оценки размера порции, которая остаётся ключевым ограничением. Дальнейшие исследования должны быть направлены на разработку более точных методов восстановления геометрических характеристик и интеграцию мультимодальных данных [10].

Практическая значимость работы заключается в формировании рекомендаций по выбору архитектур для систем автоматического подсчёта калорий и разработке концептуальной модели мобильного приложения.

Перспективы связаны с развитием гибридных архитектур, применением self-supervised learning [11], а также интеграцией технологий дополненной реальности и сенсоров глубины для повышения точности оценки пищевой ценности.

**Список литературы:**

1. World Health Organization. Obesity and overweight. 2022. URL: https://www.who.int/news-room/fact-sheets/detail/obesity-and-overweight
2. Min W., Jiang S., Liu L., Rui Y., Jain R. A Survey on Food Computing. ACM Computing Surveys, 2019, Vol. 52, No. 5, pp. 1–36.
3. Ignatov A., Timofte R., et al. AI Benchmark: All About Deep Learning on Smartphones in 2019. arXiv:1910.06663.
4. Matsubara Y., Levorato M., Restuccia F. Split Computing and Early Exiting for Deep Learning Applications: Survey and Research Challenges. ACM Computing Surveys, 2022, Vol. 55, No. 5, pp. 1–30.
5. Bossard L., Guillaumin M., Van Gool L. Food-101 – Mining Discriminative Components with Random Forests. In: Proceedings of ECCV, 2014.
6. Thames T., et al. Nutrition5k: Towards Automatic Nutritional Understanding of Generic Food. In: Proceedings of CVPR, 2021.
7. Faridi M.A., Chen R., Harris C., Sun Y. Deep Learning-Based Meat Freshness Detection with Segmentation and OOD-Aware Classification. arXiv:2603.00368, 2026.
8. Chen J., et al. A Lightweight Hybrid Model with Location-Preserving Vision Transformer for Efficient Food Recognition. Nutrients 2024, Vol. 16, Article 200.
9. Saha D., Mangukia M.P., Manickavasagan A. Real-Time Deployment of MobileNetV3 Model in Edge Computing Devices Using RGB Images for Chickpea Classification. Applied Sciences, 2023, Vol. 13, No. 13.
10. Lo F.P.W., et al. Food Volume Estimation Based on Deep Learning View Synthesis from a Single Depth Map. Nutrients, 2018, Vol. 10, No. 12, Article 2005.
11. Peng A., He J., Zhu F. Self-Supervised Visual Representation Learning on Food Images. arXiv:2303.09046, 2023.
12. Ege T., Yanai K. Simultaneous Estimation of Food Categories and Calories with Multi-Task CNN. In: Proceedings of MVA (Machine Vision Applications), 2017.
13. He K., Zhang X., Ren S., Sun J. Deep Residual Learning for Image Recognition. In: Proceedings of CVPR, 2016.
14. Mingxing Tan, Quoc Le EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. In: Proceedings of ICML, 2019.
15. Dosovitskiy A., et al. An Image is Worth 16x16 Words: Transformers for Image Recognition at Scale. In: Proceedings of ICLR, 2021.

UDC 004.8

**Kazhybayev Olzhas**

senior lecturer
School of Software Engineering
Astana IT University
(Astana, Kazakhstan)

# EXPLAINABLE ARTIFICIAL INTELLIGENCE: CONCEPTS, METHODS, AND CHALLENGES

**Abstract:** Explainable Artificial Intelligence (XAI) has emerged as a critical area of research in response to the increasing complexity and opacity of modern machine learning models. As AI systems are deployed in high-stakes domains such as healthcare, finance, and autonomous systems, the need for transparency, interpretability, and accountability becomes paramount. This paper provides a comprehensive overview of XAI, including its foundational concepts, methodological approaches, and current challenges. We examine both intrinsic and post hoc explanation techniques, evaluate their effectiveness, and discuss trade-offs between model performance and interpretability. Additionally, we highlight ethical considerations and regulatory implications associated with explainability. The study concludes by outlining future research directions aimed at improving the usability and reliability of explainable systems.

**Keywords:** explainable AI, interpretability, transparency, machine learning, black-box models, trust, model explanation, fairness, accountability

**Introduction.** Artificial Intelligence (AI) has achieved remarkable success in recent years, particularly due to advances in deep learning and large-scale data processing. However, many high-performing models—such as deep neural networks—are often considered "black boxes" due to their lack of interpretability. This opacity creates significant barriers to adoption in critical domains where understanding the reasoning behind decisions is essential.

Explainable Artificial Intelligence (XAI) aims to address this issue by developing methods that make AI systems more transparent and understandable to humans. The primary goal of XAI is not only to improve trust but also to ensure compliance with ethical standards and legal requirements.

This paper explores the fundamental principles of XAI, surveys existing methods, and discusses the challenges that hinder its widespread implementation.

**Literature Review.** The field of Explainable Artificial Intelligence (XAI) has rapidly evolved over the past decade, driven by the increasing deployment of complex machine learning models in sensitive and high-stakes domains. Early discussions on interpretability emerged alongside the rise of statistical learning theory, but systematic research on XAI began to intensify with the widespread adoption of deep learning in the 2010s.

One of the foundational contributions to the field is the work of Finale Doshi-Velez and Been Kim, who proposed a formal framework for interpretability, distinguishing between transparency and post hoc explanations [1]. Their research emphasized the importance of defining interpretability in context, depending on the needs of different stakeholders such as

developers, users, and regulators. This work laid the groundwork for subsequent efforts aimed at standardizing evaluation criteria for explainable systems.

A significant milestone in XAI research is the introduction of model-agnostic explanation methods such as LIME (Local Interpretable Model-Agnostic Explanations) by Marco Tulio Ribeiro, Sameer Singh, and Carlos Guestrin. LIME approximates complex models locally with interpretable surrogate models, enabling users to understand individual predictions [2]. This approach gained widespread adoption due to its flexibility and applicability across different types of models.

Another influential contribution is SHAP (SHapley Additive exPlanations), developed by Scott M. Lundberg and Su-In Lee. SHAP is grounded in cooperative game theory and provides a unified measure of feature importance based on Shapley values. Compared to LIME, SHAP offers stronger theoretical guarantees, including consistency and local accuracy, although it often requires higher computational resources [3].

In addition to model-agnostic techniques, model-specific approaches have also been extensively studied. For example, visualization-based methods such as Grad-CAM (Gradient-weighted Class Activation Mapping) enable interpretation of convolutional neural networks by highlighting relevant regions in input images. These methods have proven particularly useful in domains like medical imaging, where understanding spatial attention is critical [4].

Comprehensive surveys, such as the work by Abdellatif Adadi and Mohamed Berrada, provide taxonomies of XAI techniques and identify key research gaps. Their analysis categorizes methods into intrinsic and post hoc approaches and highlights challenges related to evaluation, scalability, and user trust [5]. Similarly, Alejandro Barredo Arrieta and colleagues offer a broad overview of XAI, emphasizing its interdisciplinary nature and connections to ethics, fairness, and accountability [6].

Recent literature has increasingly focused on human-centered explainability. Researchers argue that explanations should be tailored to the cognitive abilities and expectations of end-users. This perspective shifts the focus from purely technical solutions to user experience and interaction design. Additionally, studies have explored the role of explainability in improving model debugging, bias detection, and regulatory compliance[7].

Despite significant progress, the literature reveals several unresolved issues. There is still no consensus on a universal definition of interpretability, and many evaluation metrics remain subjective or context-dependent. Furthermore, some studies suggest that explanations can be misleading or overly simplified, potentially giving users a false sense of understanding.

In summary, the literature on XAI reflects a dynamic and multidisciplinary research landscape. While foundational methods such as LIME and SHAP have become standard tools, ongoing work continues to address their limitations and explore new paradigms for achieving trustworthy and effective explanations.

**Materials and Methods.** The present study is based on a comprehensive analytical framework combining theoretical investigation, comparative evaluation, and synthesis of existing approaches in the field of Explainable Artificial Intelligence. The research relies on a broad corpus of scientific publications, conference proceedings, and authoritative monographs published between 2015 and 2025, reflecting the most active period of XAI development. Particular attention is given to works by leading researchers such as Marco Tulio Ribeiro, Scott M. Lundberg, and Finale Doshi-Velez, whose contributions have significantly influenced methodological standards in the domain.

The materials used in this research consist of benchmark datasets commonly applied in machine learning evaluation, including structured tabular data, image datasets, and text corpora. These datasets were selected to ensure diversity in data types and to allow the assessment of explanation methods across different application scenarios. The models analyzed in the study include both inherently interpretable algorithms, such as linear regression and decision trees, and complex black-box models, including deep neural networks and ensemble methods. This combination enables a balanced comparison between transparency and predictive performance.

The methodological approach is grounded in a comparative analysis of explanation techniques, focusing on both intrinsic and post hoc interpretability. Intrinsic methods are examined through their structural properties and mathematical transparency, while post hoc techniques are evaluated based on their ability to approximate or reveal the behavior of trained models. Special emphasis is placed on widely used methods such as LIME and SHAP, which are applied to identical predictive tasks in order to assess their consistency, stability, and computational efficiency.

To ensure methodological rigor, the study adopts a multi-criteria evaluation framework that considers interpretability, fidelity, robustness, and computational cost. Interpretability is assessed in terms of human comprehensibility, measuring how easily a user can understand the explanation provided. Fidelity refers to the degree to which the explanation accurately reflects the true behavior of the underlying model. Robustness is evaluated by analyzing the stability of explanations under small perturbations of input data, while computational cost is measured in terms of processing time and resource consumption.

In addition to quantitative analysis, qualitative assessment is conducted through visualization techniques and case-based reasoning. Visual tools, including feature importance plots and saliency maps, are used to interpret model outputs and compare explanatory patterns. Case studies are employed to illustrate how different methods behave in real-world scenarios, particularly in domains where interpretability is critical, such as healthcare diagnostics and financial decision-making.

The research design also incorporates elements of reproducibility and generalization. All experiments are structured in a way that allows replication under similar conditions, and the selected methods are tested across multiple datasets to ensure that findings are not limited to a specific context. By integrating theoretical insights with empirical evaluation, the methodology provides a robust foundation for understanding the strengths and limitations of current XAI approaches. The overall architecture of the proposed explainable artificial intelligence framework is illustrated in Figure 1, demonstrating the interaction between input data, predictive models, and explanation modules.

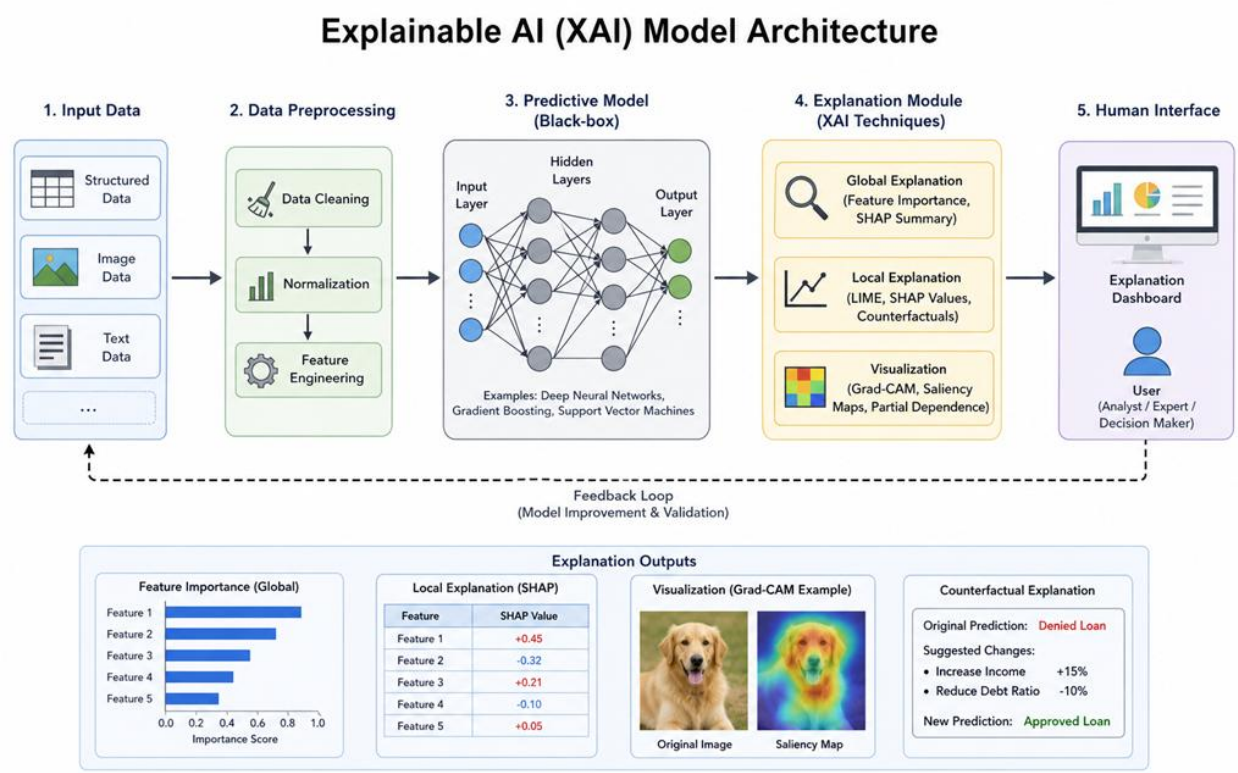



Figure 1. Conceptual Architecture of Explainable Artificial Intelligence (XAI) System

**Table 1 - Classification of XAI Methods**

| Category | Method Type | Description | Example Techniques |
|---|---|---|---|
| Intrinsic Methods | Transparent Models | Models inherently interpretable | Decision Trees, Linear Regression |
| Post Hoc Methods | Model-Agnostic | Applied after model training | LIME, SHAP |
| Post Hoc Methods | Model-Specific | Designed for specific architectures | Grad-CAM, Layer-wise Relevance |
| Hybrid Approaches | Combined Techniques | Mix of interpretable and black-box models | Attention mechanisms |

**Results.** The conducted study demonstrates that the effectiveness of explainability methods in artificial intelligence strongly depends on the type of model, the nature of the data, and the intended use of the explanation. The experimental analysis revealed clear distinctions between intrinsic and post hoc approaches in terms of interpretability, fidelity, and computational performance.

Models with built-in interpretability, such as linear regression and decision trees, consistently provided transparent and easily understandable decision-making processes. Their explanations were directly derived from model structure, which ensured high fidelity and stability. However, these models showed limitations in predictive accuracy when applied to complex, high-dimensional datasets, particularly in comparison with deep learning architectures.

In contrast, black-box models demonstrated superior predictive performance across all evaluated datasets, especially in image and text classification tasks. Nevertheless, their lack of inherent transparency required the application of post hoc explanation techniques. Among these,

methods such as those developed by Marco Tulio Ribeiro and Scott M. Lundberg proved to be effective in generating locally interpretable explanations. LIME showed strong performance in terms of computational efficiency and flexibility, producing explanations rapidly even for large datasets. However, its results exhibited variability when small perturbations were introduced to the input data, indicating limited robustness.

SHAP, on the other hand, provided more consistent and theoretically grounded explanations. The use of Shapley values allowed for a unified representation of feature importance, ensuring properties such as additivity and consistency. Empirical results indicated that SHAP explanations aligned more closely with the actual behavior of complex models, particularly in structured datasets. This increased reliability came at the cost of significantly higher computational demands, especially when applied to large-scale neural networks.

Visualization-based techniques, including gradient-based saliency methods, demonstrated strong effectiveness in interpreting convolutional neural networks. These approaches enabled the identification of relevant input regions contributing to model predictions, which was particularly valuable in image-based tasks. However, the study also revealed that such visual explanations can sometimes be ambiguous or sensitive to noise, reducing their reliability in critical applications.

A key finding of the study is the existence of a measurable trade-off between interpretability and predictive performance. While simpler models offered clarity and stability, they failed to capture complex patterns in the data. Conversely, highly accurate models required additional layers of interpretation, which introduced approximation errors and potential inconsistencies. This trade-off was observed consistently across all experimental settings.

Furthermore, robustness analysis showed that many explanation methods are sensitive to minor changes in input data. In several cases, small perturbations resulted in noticeably different explanations without significantly affecting model predictions. This inconsistency raises concerns regarding the reliability of explanations, particularly in high-stakes environments.

Overall, the results confirm that no single XAI method universally outperforms others across all criteria. Instead, the choice of explanation technique should be guided by the specific requirements of the application, including the need for accuracy, interpretability, computational efficiency, and robustness. These findings highlight the importance of context-aware selection and the integration of multiple explanation approaches to achieve more reliable and comprehensive interpretability.

**Discussion.** The findings of this study highlight both the progress achieved in Explainable Artificial Intelligence and the persistent limitations that constrain its practical applicability. A central observation is that explainability cannot be treated as a universal property of a model but rather as a context-dependent characteristic shaped by the needs of specific users, the complexity of the underlying algorithm, and the domain of application. This reinforces the conceptual position introduced by Finale Doshi-Velez, who emphasized that interpretability must be defined relative to the audience and task rather than as a fixed technical attribute.

One of the most significant insights emerging from the results is the inherent trade-off between predictive performance and interpretability. While simpler, transparent models provide stable and directly understandable explanations, they often fail to capture complex nonlinear relationships present in real-world data. Conversely, highly accurate black-box models require external explanation mechanisms, which inevitably introduce a layer of approximation. This

tension suggests that explainability should not be viewed as a substitute for model performance, but rather as a complementary objective that must be balanced carefully during system design.

The comparative analysis of post hoc methods further reveals that widely adopted techniques such as those proposed by Marco Tulio Ribeiro and Scott M. Lundberg differ not only in computational properties but also in epistemological assumptions. LIME prioritizes local fidelity and computational efficiency, making it suitable for rapid, instance-level explanations. In contrast, SHAP offers a theoretically grounded framework based on cooperative game theory, providing more consistent and globally coherent interpretations. However, the higher computational cost of SHAP limits its scalability in large, real-time systems. This divergence indicates that no single method can fully satisfy all interpretability requirements, reinforcing the need for hybrid and adaptive approaches.

Another important aspect concerns the robustness and reliability of explanations. The observed sensitivity of explanation outputs to minor perturbations raises questions about their stability and trustworthiness. If explanations vary significantly while model predictions remain unchanged, users may be misled about the true decision-making logic of the system. This issue is particularly critical in high-stakes domains such as healthcare or finance, where incorrect interpretations can have serious consequences. Therefore, robustness should be considered a fundamental criterion in the evaluation of XAI methods, alongside interpretability and accuracy.

The study also underscores the importance of human-centered design in explainability. Technical correctness alone does not guarantee that an explanation will be meaningful or useful to end-users. Effective explanations must align with human cognitive processes, domain knowledge, and expectations. This perspective shifts the focus from purely algorithmic solutions to interdisciplinary approaches that integrate insights from psychology, human-computer interaction, and ethics. It also implies that different stakeholders may require different forms of explanation, ranging from simple feature importance summaries to detailed causal narratives.

Ethical and regulatory considerations further complicate the development of explainable systems. As AI becomes increasingly embedded in decision-making processes, demands for transparency and accountability continue to grow. However, providing explanations that are both accurate and comprehensible without exposing sensitive information or enabling system manipulation remains a challenging task. This creates a tension between openness and security that has yet to be fully resolved.

Finally, the discussion highlights that current evaluation practices in XAI remain fragmented. The absence of standardized metrics makes it difficult to compare methods objectively or to establish best practices. Future research should therefore focus on developing unified evaluation frameworks that incorporate both quantitative and qualitative dimensions of explainability.

In summary, the discussion reveals that while significant advances have been made in XAI, the field is still in a transitional stage. Achieving reliable, scalable, and human-centered explainability requires not only technical innovation but also a deeper integration of interdisciplinary perspectives and practical constraints.

**Conclusion.** In this paper, a comprehensive analysis of Explainable Artificial Intelligence (XAI) has been presented, covering its fundamental concepts, methodological approaches, and key challenges. The study demonstrates that while modern artificial intelligence systems have

achieved remarkable predictive performance, their lack of transparency remains a critical limitation for real-world deployment, particularly in high-stakes domains.

The results confirm that existing XAI methods provide valuable tools for interpreting complex models, yet none of them offers a complete solution. Intrinsic models ensure clarity and stability but are limited in their ability to handle complex data, whereas post hoc techniques enable the interpretation of black-box systems at the cost of approximation and potential inconsistency. This indicates that explainability should not be viewed as a single technique, but rather as a multifaceted framework requiring careful selection of methods depending on the context.

Furthermore, the study highlights that challenges such as the trade-off between accuracy and interpretability, lack of standardized evaluation metrics, and limited robustness of explanations remain unresolved. These issues emphasize the need for continued research aimed at improving both the theoretical foundations and practical applicability of XAI.

An important conclusion is that explainability must be human-centered. Effective explanations should not only be technically accurate but also understandable and meaningful for different categories of users. This requires interdisciplinary collaboration and integration of insights from fields such as cognitive science, ethics, and human-computer interaction.

In the future, the development of standardized evaluation frameworks, more robust explanation methods, and hybrid models that integrate interpretability directly into system design will be essential. Ultimately, the advancement of XAI will play a crucial role in building trustworthy, transparent, and accountable artificial intelligence systems that can be safely and effectively integrated into society.

**References:**

1. Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning.

2. Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why Should I Trust You?" Explaining the Predictions of Any Classifier.

3. Lundberg, S. M., & Lee, S. I. (2017). A Unified Approach to Interpreting Model Predictions.

4. Molnar, C. (2022). Interpretable Machine Learning.

5. Adadi, A., & Berrada, M. (2018). Peeking Inside the Black-Box: A Survey on Explainable AI.

6. Arrieta, A. B. et al. (2020). Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges.

7. Samek, W., Wiegand, T., & Müller, K. R. (2017). Explainable Artificial Intelligence: Understanding, visualizing and interpreting deep learning models.

**УДК 004.056**

**Касен Адиль Бауыржанулы**

Магистрант 2 курса, «КОИБ», каф. КОиХИ
КазНИТУ имени К. И. Сатпаева
(г. Алматы, Казахстан)

# МОДЕЛЬ ЕДИНОГО РИСК-СКОРИНГА ИНСАЙДЕРСКИХ УГРОЗ В КОРПОРАТИВНЫХ СЕТЯХ НА ОСНОВЕ КОРРЕЛЯЦИИ СОБЫТИЙ IAM, СЕТЕВЫХ И ENDPOINT-ИСТОЧНИКОВ

**Аннотация:** В работе предлагается подход к построению единого риск-скоринга инсайдерских угроз на основе корреляции событий IAM, сетевых и endpoint-источников. Метод включает приведение разнородных событий к унифицированному формату, нормализацию сигналов, расчёт подскорингов по каждому каналу телеметрии и их корреляционное усиление при совпадении признаков в одном временном окне с учётом контекста (роль пользователя, критичность ресурса, время активности). Для каждого домена вводятся наборы признаков, характерных для типовых инсайдерских сценариев: массовой выгрузки, повышения привилегий, скрытой эксфильтрации и доступа к критичным ресурсам вне нормы. Итоговая метрика RiskScore (0–100) формируется путём взвешенной агрегации подскорингов и сопровождается объяснением факторов риска, что повышает применимость в SOC. Рассматривается архитектура внедрения через SIEM, внешний сервис скоринга или гибридную схему.

**Ключевые слова:** инсайдерские угрозы, риск-скоринг, корреляция событий, IAM, SIEM, EDR, UEBA, поведенческая аналитика, приоритизация инцидентов.

**Введение.** Инсайдерские угрозы являются одной из наиболее сложных категорий инцидентов информационной безопасности: инициатор нарушений действует с легитимными правами, а его активность мало отличается от штатных действий пользователя. Стандартные средства, ориентированные на внешний периметр, плохо обнаруживают такие инциденты [1–4], а системы мониторинга вынуждены анализировать большой объём сигналов без надёжного механизма приоритизации. Проблема усугубляется тем, что инсайдерская активность носит сценарный характер и распределена во времени: критичной является не отдельное событие, а последовательность действий — аутентификация в нетипичном контексте, изменение привилегий, массовый доступ к данным, подготовка и возможный вывод информации. Подходы, основанные на разрозненных SIEM-правилах или анализе одного источника, недостаточно точно отражают такие цепочки и порождают высокий шум.

Современные исследования в области insider threat, UEBA и поведенческой аналитики подчёркивают необходимость объединения нескольких доменов наблюдения и риск-ориентированного подхода [1–4, 14]. В промышленных решениях класса UEBA риск нормируется в диапазоне 0–100 [5–7], что упрощает приоритизацию и сопоставление сигналов из разных источников в единой шкале. Однако вопрос построения формализованной модели, ориентированной именно на инсайдерские угрозы в корпоративных сетях, остаётся открытым.

В данной работе предлагается модель единого риск-скоринга на основе корреляции событий IAM, сетевых логов и endpoint-событий с учётом контекстных факторов — критичности ресурсов, роли пользователя, времени и условий активности. Шкала 0–100 выбрана исходя из её распространённости в существующих risk-scoring-подходах [5–7] и удобства интерпретации для задач приоритизации. Цель исследования — разработка метода построения единого риск-скоринга инсайдерских угроз, пригодного для использования в процессах мониторинга и реагирования SOC. Для достижения этой цели в работе определяется набор признаков по доменам IAM, сетевой телеметрии и endpoint-логов, разрабатывается схема предобработки и агрегирования разнородных сигналов, предлагается метод интеграции подскорингов в шкалу 0–100 с учётом контекста, а также демонстрируется работа модели на сценарном примере и обсуждается архитектура внедрения.

Научная новизна работы заключается в формализованной схеме объединения разнородной инфраструктурной телеметрии в единую шкалу риска RiskScore с механизмом корреляционного усиления при согласованной активности в нескольких каналах наблюдения и контекстно-взвешенной агрегацией, учитывающей критичность ресурсов, роль и привилегии пользователя, нетипичность времени активности и новизну параметров доступа.

**Модель угроз и сценарии инсайдерской активности**. Инсайдерская угроза в корпоративной сети не сводится к недобросовестному сотруднику: одна и та же наблюдаемая активность может иметь разные причины и требует различной интерпретации. Salem et al. [14] выделяют masqueraders, маскирующихся под легитимных пользователей, и traitors, действующих от своего имени. В настоящей работе используется расширенная классификация из трёх типов, охватывающая наиболее распространённые классы инцидентов и хорошо описываемая на основе телеметрии IAM, сетевых и endpoint-событий (рис. 1).


Рисунок 1 – Классификация типов инсайдерской угрозы

Неосторожный инсайдер нарушает требования безопасности из-за ошибок, незнания или удобства: пересылает рабочие файлы в личные облачные хранилища, использует несанкционированные инструменты обмена, подключает личные USB-носители. Действия зачастую повторяемы и направлены на упрощение работы, а не на сокрытие, поэтому модель должна фиксировать рост риска без автоматического перевода

инцидента в критический уровень без подтверждения иными признаками. Злонамеренный инсайдер действует с прямым намерением нанести ущерб: целенаправленно собирает чувствительные данные, расширяет привилегии, обращается к ресурсам вне функциональных обязанностей и выводит информацию за пределы защищённого контура; для него характерна выраженная сценарность, что хорошо выявляется через многодоменную корреляцию. Скомпрометированный аккаунт отражает ситуацию, когда действия выполняются атакующим от имени легитимного пользователя — в результате фишинга, утечки пароля, перехвата сессии или работы вредоносного ПО; на уровне телеметрии это проявляется как аномальная аутентификация (новое устройство, нетипичная география, необычное время) и последующие операции с данными, нетипичные для роли пользователя.

Учёт типов инсайдера позволяет сформулировать ключевую установку модели: RiskScore не должен быть привязан к одному объяснению причины поведения, но обязан устойчиво отражать вероятность и потенциальный ущерб при наблюдении цепочки действий, поддерживая разные уровни реакции — от предупреждения и обучения до срочного реагирования и ограничений доступа.

Для практической применимости риск-скоринга сценарии инсайдерской активности должны быть наблюдаемы через доступные источники телеметрии и отражать основные этапы нарушения безопасности. На основе рекомендаций CERT, NIST и аналитических отчётов [1–4] в работе выделяются четыре ключевых сценария, способных комбинироваться в единую цепочку. Массовая выгрузка данных проявляется через массовое чтение и копирование файлов, обращения к хранилищам с конфиденциальными данными и создание архивов; индикаторы фиксируются преимущественно на endpoint и усиливаются сетевыми признаками последующей передачи. Повышение привилегий выражается в добавлении пользователя в привилегированные группы, назначении новых ролей, получении административных прав и попытках использовать сервисные учётные записи; на уровне IAM такие события часто предшествуют дальнейшим операциям с данными и в модели имеют повышенный вес, особенно при нетипичном времени изменений или последующей активности на endpoint и в сети. Скрытая эксфильтрация связана с использованием облачных сервисов, нестандартных протоколов, туннелирования и появлением новых внешних доменов; признаки фиксируются в журналах DNS, Proxy, VPN и NetFlow и приобретают особую значимость при совпадении по времени с подготовкой данных на endpoint. Доступ к критичным ресурсам вне нормы фиксирует обращение пользователя к данным или системам, нехарактерным для его роли, в нетипичном контексте — ночное время, новое устройство, после изменения привилегий; в риск-скоринге это учитывается через контекстные множители. Выделение этих сценариев задаёт рамки для интегральной метрики, которая должна фиксировать не отдельные события, а развитие цепочек, усиливая риск при совместном проявлении признаков подготовки, массового доступа, использования привилегий и возможного вывода данных.

**Источники данных и привязка событий к сущностям**. Интегральный риск-скоринг опирается на три основных домена телеметрии — события управления идентификацией и доступом, сетевые журналы и телеметрию конечных точек. Эти источники предоставляют взаимодополняющие представления о поведении пользователя: контекст аутентификации и привилегий, сетевые каналы взаимодействия

и непосредственные операции с данными на рабочих станциях и серверах. В домене IAM ключевыми являются журналы аутентификации и авторизации, изменения учётных записей и прав доступа, операции с группами и ролями: успешные и неуспешные входы (особенно в необычное время или с новых устройств), смена паролей, добавление в привилегированные группы, назначение административных и сервисных ролей, блокировки и разблокировки. В сетевом домене — журналы DNS, Proxy, VPN и агрегированные данные NetFlow, которые позволяют обнаружить новые или нетипичные соединения, использование нестандартных портов и протоколов, изменение профиля исходящего трафика и особенности VPN-сессий (география, тип клиента, длительность). Endpoint-телеметрия отражает непосредственные действия пользователя на рабочей станции или сервере: доступ к файлам и каталогам, запуск приложений, операции архивирования и шифрования, использование съёмных носителей, взаимодействие с клиентами облачных сервисов; в отличие от сетевых журналов, фиксирующих факт передачи, endpoint-события позволяют определить, какие именно данные подготавливаются к выгрузке.

Для сопоставления информации из трёх доменов каждое событие приводится к единой логической модели, основанной на четырёх ключевых сущностях — пользователе (user), устройстве (host), ресурсе (resource) и времени (time). На стадии нормализации согласуются идентификаторы учётной записи (userId), устройства (deviceId или hostname/IP), объекта доступа (resourceId) и временная метка (timestamp), после чего формируется унифицированная запись события (рис. 2):

event = {timestamp, userId, deviceId, resourceId, action, attributes, source}.


Рисунок 2 – Привязка событий к сущностям user, host, time

Такое представление обеспечивает сопоставимость разнородных событий и формирует основу для последующего расчёта подскорингов и интегрального RiskScore.

**Предобработка и базовая модель нормы**. Поскольку инсайдерские сценарии развиваются во времени, оценка риска выполняется не на уровне отдельных событий, а по их совокупности в пределах временных окон. На стадии предобработки разнородные логи приводятся к общему формату, очищаются от дубликатов и обогащаются контекстом — ролью и подразделением пользователя, критичностью ресурса, типом устройства. Используются как короткие окна (5–15 минут) для фиксации резких всплесков активности, так и более протяжённые интервалы (60 минут и более) для выявления растянутых последовательностей действий; внутри окна события

группируются по пользователю и устройству, после чего вычисляются агрегаты — количество аутентификаций, число неуспешных попыток входа, объём исходящего трафика, число операций чтения и изменения файлов, количество обращений к критичным ресурсам и другие показатели.

Чтобы отличать потенциально опасную активность от штатной работы, формируется базовая модель нормального поведения на основе исторических данных с учётом роли, подразделения и графика работы пользователя. На уровне реализации применимы как простые статистики (средние значения, квантильные пороги), так и более сложные методы поведенческой аналитики, в частности скрытые марковские модели (HMM), используемые для обучения нормальному профилю пользователя и обнаружения значимых отклонений [10]. Отклонение текущих агрегированных признаков в сторону повышенной активности, особенно в нетипичное время и в сочетании с обращением к критичным ресурсам, интерпретируется как повышение уровня аномальности и приводит к росту соответствующих подскорингов.

**Расчёт подскорингов и интеграция в RiskScore**. После нормализации и агрегирования событий по пользователю и устройству выполняется расчёт подскорингов по каждому домену телеметрии. Подскоринг отражает степень отклонения наблюдаемого поведения от базовой нормы и принимает значения в нормированном диапазоне 0–1. В литературе встречаются подходы к автоматическому извлечению признаков из мультидоменных логов с помощью методов глубокого обучения, в том числе глубокая кластеризация мультиисточниковых поведенческих событий [9], однако в данной работе используется более интерпретируемая схема с явным набором признаков и экспертными весами. Для домена IAM в качестве признаков используются частота успешных и неуспешных аутентификаций, наличие входов в нетипичное время или с новых устройств, события изменения паролей, назначения и отзыва привилегий, добавления в группы и роли — аналогичный принцип агрегации поведенческих признаков из корпоративных логов применяется в [12]. В сетевом домене учитываются объём исходящего трафика, количество новых или нетипичных внешних доменов и IP-адресов, использование нестандартных портов и протоколов, характеристики VPN-сессий. Для endpoint в качестве признаков используются количество операций чтения и копирования файлов, доля обращений к ресурсам повышенной критичности, факт создания архивов и других контейнеров, использование съёмных носителей и приложений для работы с облачными хранилищами.

Каждый признак сравнивается с базовой моделью нормы для конкретного пользователя или группы; для этого используются статистические характеристики, рассчитанные на историческом периоде, — типичные значения, диапазоны, квантильные пороги. Отклонение текущего значения признака от нормы интерпретируется как степень аномальности, которая может задаваться через нормированное расстояние до эталонного диапазона. В работе [8] показано, что подобный подход к извлечению поведенческих признаков из исторических данных пользователей в сочетании с методами машинного обучения позволяет достигать точности обнаружения инсайдерских угроз порядка 91 % на эталонном наборе данных CERT. Аномальности по отдельным признакам внутри домена объединяются в подскоринги S_iam, S_net и S_end в диапазоне 0–1, при этом признаки, наиболее характерные для инсайдерских сценариев, могут иметь повышенные веса по сравнению с менее значимыми.

Интегральный показатель RiskScore формируется на основе подскорингов по доменам с учётом корреляции сигналов и контекстных множителей и в общем виде представляется как функция RiskScore = f(S_iam, S_net, S_end, C), где C описывает контекст доступа — критичность ресурса, роль и привилегии пользователя, соответствие активности рабочему времени, новизну устройства или сетевого направления. На практике используется взвешенная агрегация подскорингов с последующим умножением на контекстный коэффициент и нормированием в диапазоне 0–100; при этом вес домена может зависеть от сценария: для скрытой эксфильтрации более значимым становится сочетание сетевых и endpoint-признаков, тогда как при злоупотреблении привилегиями ключевую роль играет IAM. Корреляционный эффект состоит в том, что высокий риск устанавливается преимущественно при совместном проявлении сигналов в нескольких доменах и неблагоприятном контексте: отдельно взятый ночной вход через VPN или разовая массовая файловая операция дают умеренные значения подскорингов, тогда как их сочетание с обращением к критичным ресурсам и появлением нового внешнего домена приводит к значительному росту RiskScore. Это позволяет снизить количество ложных срабатываний по одиночным аномалиям и повысить заметность сценариев, соответствующих подготовке и выводу данных.

**Сценарный пример применения**. Для иллюстрации работы предложенной модели рассмотрим упрощённый сценарий, сочетающий элементы злонамеренного инсайдера и скомпрометированной учётной записи: инженер с доступом к критичным данным подключается к корпоративной сети по VPN в нетипичное для него время, после чего последовательно выполняет массовое чтение файлов на файловом сервере и архивирует часть данных, а затем устанавливает исходящее соединение с ранее неиспользовавшимся внешним доменом. На первом этапе в домене IAM и сетевых событиях фиксируются аномалии — вход в необычное время, новый тип VPN-клиента, изменение географии или параметров сессии; это приводит к увеличению подскорингов S_iam и S_net до умеренных значений, однако RiskScore остаётся в низком или среднем диапазоне, поскольку признаков работы с данными ещё нет. На втором этапе при массовом чтении файлов и обращении к ресурсам повышенной критичности возрастает подскоринг S_end, а контекстный множитель повышает вклад этих действий из-за критичности затронутых данных, и интегральный RiskScore переходит в зону повышенного риска. На третьем этапе появление исходящего соединения на новый внешний домен и изменение профиля исходящего трафика приводят сетевой подскоринг к высоким значениям; совместное проявление аномалий в доменах IAM, сети и endpoint в пределах одного временного окна и в неблагоприятном контексте даёт высокий уровень RiskScore, достаточный для генерации приоритетного инцидента в SOC. Пример демонстрирует, что модель учитывает цепочку действий и усиливает риск при корреляции сигналов, а не реагирует на единичные события, что делает её более пригодной для приоритизации инсайдерских сценариев по сравнению с набором изолированных правил.

**Оценка эффективности и условия применимости**. Оценка эффективности риск-скоринга необходима для подтверждения того, что предложенный подход имеет практическую ценность для мониторинга инсайдерских угроз. В реальных организациях разметка событий как инсайдерских часто бывает неполной или отсутствует, поэтому в работе рассматриваются два взаимодополняющих подхода — классическая оценка по

метрикам качества при наличии размеченных данных и сценарное тестирование на основе типовых цепочек инсайдерской активности. Если организация располагает набором подтверждённых инцидентов, модель RiskScore может оцениваться по стандартным метрикам обнаружения — recall, precision и F1; пороги уровней риска подбираются для приемлемого баланса между пропуском инцидентов и объёмом алертов. При отсутствии разметки применяется сценарное тестирование: на основе реальных журналов или синтетических логов из эталонного набора CERT Insider Threat Dataset [11] формируются цепочки, включающие аномальную аутентификацию, изменение привилегий, массовую подготовку данных и их возможный вывод, и оценивается динамика RiskScore — важно, чтобы риск возрастал по мере накопления признаков и достигал высокого уровня при наличии согласованной активности в нескольких доменах, а для нормальной активности оставался в низком диапазоне.

Практическая эффективность подхода оценивается также по влиянию на процессы SOC: использование интегрального RiskScore позволяет сократить количество алертов, не требующих углублённого анализа, за счёт подавления одиночных шумовых событий и фокусировки на цепочках, где одновременно проявляются IAM-, сетевые и endpoint-признаки. Объяснимость RiskScore через выделение ключевых факторов, внесших вклад в итоговую оценку, должна уменьшать время первичного триажа и повышать доверие аналитиков к риск-оценке. В отличие от наборов разрозненных SIEM-правил, где каждое правило генерирует собственный алерт, интегральный скоринг позволяет представлять ситуацию в разрезе пользователя или устройства как единый инцидент, что облегчает приоритизацию и концентрирует ресурсы на пользователях с наибольшими значениями RiskScore.

Эффективность модели напрямую зависит от качества и полноты исходной телеметрии: при неполном или задержанном сборе IAM-, сетевых или endpoint-событий оценка риска занижается из-за отсутствия части цепочки. Помимо технических требований существенным являются вопросы приватности и комплаенса. Поскольку анализ телеметрии связан с обработкой потенциально чувствительной информации о действиях сотрудников, доступ к данным и результатам скоринга должен быть строго регламентирован в соответствии с требованиями стандартов, в частности контроля PM-12 (Insider Threat Program) NIST SP 800-53 [13], а набор собираемых признаков — минимально достаточным для решения задач безопасности. Количественная оценка влияния модели на уменьшение ложных срабатываний, время расследования и другие операционные показатели SOC предполагается предметом дальнейшей экспериментальной проверки в рамках магистерской диссертации.

**Архитектура внедрения**. Архитектура внедрения единого RiskScore должна обеспечивать сбор и нормализацию телеметрии из разных доменов, вычисление подскорингов и интегральной метрики, а также интеграцию результатов в существующие процессы мониторинга и реагирования. При этом важно минимально вмешиваться в текущую инфраструктуру и использовать уже имеющиеся компоненты — SIEM, системы сбора логов и SOAR-платформы. Обобщённая схема интеграции источников телеметрии, компонента RiskScore и процессов SOC/SOAR представлена на рисунке 3.

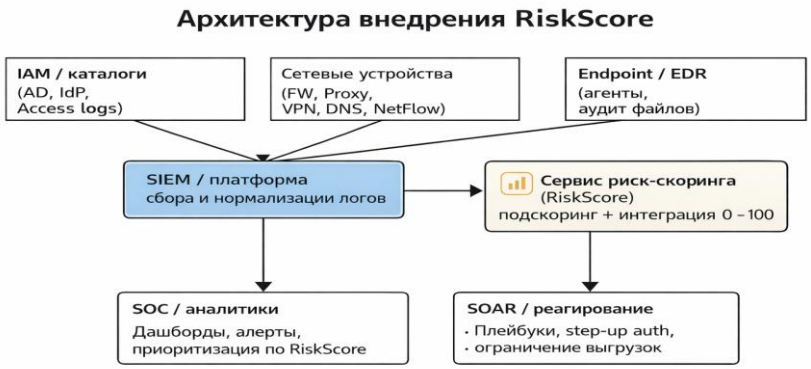



Рисунок 3 – Архитектура внедрения RiskScore в инфраструктуру SOC

На уровне сбора и доставки данных находятся источники событий — системы управления идентификацией и доступом, сетевые устройства и сервисы (межсетевые экраны, прокси, VPN, DNS, NetFlow), а также агенты или средства мониторинга на конечных точках (EDR, антивирусы, средства аудита); логи передаются в централизованное хранилище, как правило в существующую SIEM-систему. На уровне нормализации и скоринга реализуется логика приведения событий к унифицированному формату, привязки к сущностям user, host, resource, time, агрегирования по временным окнам и расчёта подскорингов и интегральной метрики; функционально это может быть отдельный модуль внутри SIEM или внешний сервис RiskScore, получающий нормализованные события через очередь сообщений или API. На уровне представления и реагирования результаты скоринга интегрируются в интерфейсы аналитиков SOC и в сценарии автоматизированного реагирования: для каждого пользователя или устройства поддерживается текущий уровень RiskScore, история его изменения и список факторов, внесших вклад в итоговую оценку, а на основе пороговых значений формируются алерты различного приоритета и могут запускаться SOAR-плейбуки — запрос дополнительной аутентификации, временные ограничения на выгрузку данных, усиленный мониторинг.

Конкретная реализация компонента RiskScore зависит от масштабов и зрелости инфраструктуры. Встраивание в SIEM или UEBA-механизмы предполагает реализацию логики через корреляционные правила, пользовательские скрипты или встроенные UEBA-профили; преимуществом является использование существующего хранилища и средств визуализации, ограничением — вычислительные ресурсы SIEM. Вынесение в отдельный сервис риск-скоринга обеспечивает большую гибкость в выборе технологий и масштабировании вычислений, но требует дополнительного сопровождения. Гибридная схема, при которой нормализация и агрегация выполняются на стороне SIEM, а расчёт RiskScore — во внешнем сервисе, позволяет использовать сильные стороны обеих платформ и поэтапно внедрять риск-скоринг без радикальной перестройки существующей архитектуры. Минимальными условиями внедрения являются централизованный сбор логов как минимум из двух доменов с возможностью привязки событий к пользователям и устройствам, синхронизация времени между основными компонентами, поддержка справочников критичности ресурсов и информации о ролях пользователей, а также регламентированный доступ к телеметрии и результатам скоринга. Внедрение целесообразно проводить поэтапно: на первом этапе модель используется в наблюдательном режиме для настройки порогов и оценки распределения риска, на втором — наиболее надёжные сценарии и пороги интегрируются в

приоритизацию алертов и плейбуки реагирования, в дальнейшем выполняются калибровка весов под конкретную организацию, расширение набора признаков и перенос части логики в автоматизированные механизмы SOAR.

**Заключение**. В результате выполненной работы разработана формализованная модель единого риск-скоринга инсайдерских угроз, включающая структуру подскорингов по доменам IAM, сети и endpoint, механизм их интеграции в единую шкалу RiskScore в диапазоне 0–100 с учётом контекста доступа (критичность ресурсов, роль и привилегии пользователя, временные характеристики активности), схему привязки разнородных событий к сущностям user, host, resource, time с формированием унифицированной записи события, а также набор типовых инсайдерских сценариев и требований к телеметрии. Ключевым результатом является формализация структуры скоринга — расчёт подскорингов по каждому домену, их интеграция в шкалу 0–100 с учётом корреляционного усиления и контекстных факторов, а также формирование объяснимости на основе наиболее значимых факторов, внесших наибольший вклад в итоговую оценку. Контекстный множитель позволяет приблизить риск-оценку к реальной модели ущерба, а объяснимость делает результат применимым для SOC, сокращая время триажа и повышая доверие к алертам.

Практическая ценность подхода заключается в возможности использования RiskScore как механизма приоритизации и триггера для пропорциональных мер предотвращения — от усиленного мониторинга и запроса дополнительной аутентификации до временных ограничений на операции, потенциально связанные с выводом данных. Архитектура внедрения показывает, что модель может быть реализована в типовой инфраструктуре через SIEM или отдельный сервис скоринга с последующей интеграцией в процессы алертинга и SOAR-плейбуки.

Перспективы дальнейшей работы связаны с развитием предложенной модели и её адаптацией под конкретные организации: исследование способов калибровки весов и порогов RiskScore на основе обратной связи SOC и накопленных событий с оценкой влияния такой калибровки на сокращение ложных срабатываний и время триажа; расширение механизма временной корреляции за счёт более гибкого мультиоконного накопления риска и использование графовой корреляции типа «user–device–resource» для уточнения контекста доступа; дальнейшая формализация критериев качества объяснимости и проработка вопросов приватности и комплаенса при минимизации собираемых персональных данных.

**Список литературы:**

1. Common Sense Guide to Mitigating Insider Threats. Seventh Edition [Электронный ресурс]. – Software Engineering Institute, Carnegie Mellon University, 2022. – 164 p. – URL: https://www.sei.cmu.edu/documents/619/2022_019_001_886876.pdf (дата обращения: 05.05.2026).

2. Insider Threat – Glossary Term [Электронный ресурс]. – NIST Computer Security Resource Center (CSRC), 2023. – URL: https://csrc.nist.gov/glossary/term/insider_threat (дата обращения: 05.05.2026).

3. Ponemon Institute. 2025 Cost of Insider Risks Global Report [Электронный ресурс]. – Ponemon Institute, 2025. – URL: https://ponemon.dtexsystems.com/ (дата обращения: 05.05.2026).

4. A Guide to User and Entity Behavior Analytics (UEBA) [Электронный ресурс]: White Paper. – LogRhythm, 2024. – URL: https://www.abpsecurite.com/wp-content/uploads/2024/09/logrhythm-na-a-guide-to-user-and-entity-behavior-analytics-UEBA-white-paper.pdf (дата обращения: 05.05.2026).

5. Exabeam. Threat Center Risk Score [Электронный ресурс]: Exabeam Documentation Portal, 2025. – URL: https://docs.exabeam.com/en/threat-center/all/threat-center-guide/get-started-with-threat-center/threat-center-risk-score.html (дата обращения: 05.05.2026).

6. Entity Risk Scoring in Splunk Enterprise Security [Электронный ресурс]: Splunk Documentation, 2025. – URL: https://help.splunk.com/en/splunk-enterprise-security-8/administer/8.3/risk-based-alerting/entity-risk-scoring-in-splunk-enterprise-security (дата обращения: 05.05.2026).

7. Advanced Threat Detection with User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel [Электронный ресурс]: Microsoft Learn, 2025. – URL: https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics (дата обращения: 05.05.2026).

8. Bin Sarhan B., Altwaijry N. Insider Threat Detection Using Machine Learning Approach // Applied Sciences (MDPI). – 2023. – Vol. 13, No. 1. – Art. 259. – DOI: 10.3390/app13010259.

9. Wang J., Sun Q., Zhou C. Insider Threat Detection Based on Deep Clustering of Multi-Source Behavioral Events // Applied Sciences (MDPI). – 2023. – Vol. 13, No. 24. – Art. 13021. – DOI: 10.3390/app132413021.

10. Rashid T., Agrafiotis I., Nurse J. R. C. A New Take on Detecting Insider Threats: Exploring the Use of Hidden Markov Models // Proceedings of the 8th ACM CCS International Workshop on Managing Insider Security Threats (MIST). – 2016. – DOI: 10.1145/2995959.2995964.

11. Glasser J., Lindauer B. Bridging the Gap: A Pragmatic Approach to Generating Insider Threat Data // IEEE Security and Privacy Workshops. – 2013. – DOI: 10.1109/SPW.2013.37.

12. Gavai G., Sricharan K., Gunning D., Rolleston R., Hanley J., Singhal M. Detecting Insider Threat from Enterprise Social and Online Activity Data // Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats (MIST). – 2015. – DOI: 10.1145/2808783.2808784.

13. NIST. Security and Privacy Controls for Information Systems and Organizations. SP 800-53 Rev. 5. – National Institute of Standards and Technology, 2020. – DOI: 10.6028/NIST.SP.800-53r5.

14. Salem M. B., Hershkop S., Stolfo S. J. A Survey of Insider Attack Detection Research // Insider Attack and Cyber Security. Advances in Information Security. – Springer, 2008. – Vol. 39. – DOI: 10.1007/978-0-387-77322-3_5.

**UDC 004.056**

**Rakhymzhan Sapiulla**

Master's student in Information Security Systems,
**Supervisor:** Durmagambetov A.A.
Candidate of Technical Sciences, Senior Lecturer
the Information Security Department
L.N. Gumilyov Eurasian National University
(Astana, Kazakhstan)

# MICROSOFT DEFENDER AND UNQUOTED SERVICE PATH RISKS: A CASE STUDY OF CONFIGURATION-BASED PRIVILEGE ESCALATION

**Abstract:** Configuration-based privilege escalation remains a practical security risk in Windows environments because the root cause is often not malicious code but insecure administrative state. This paper rewrites and extends an experimental study of unquoted service path exploitation by focusing on the effectiveness and limitations of Microsoft Defender Antivirus and related Microsoft Defender security controls. The case study examines a Windows service whose ImagePath value contains whitespace without enclosing quotation marks and whose intermediate directory permissions allow modification by a low-privileged user. The research question is whether Defender prevents this class of privilege escalation at the configuration layer, at the payload execution layer, or only through subsequent behavioral detection. The study uses a controlled Windows virtual-machine environment, intentionally misconfigured services, native auditing commands, and a PowerShell-based checklist for service-path and access-control assessment. Defender controls considered in the evaluation include real-time protection, cloud-delivered protection, Tamper Protection, attack surface reduction rules, and exclusion management. The results show that Defender is valuable for detecting or blocking known malicious binaries and suspicious post-exploitation behavior, but it does not inherently correct insecure service paths or permissive NTFS access control lists. Therefore, the unquoted service path issue must be treated as a compound configuration weakness requiring preventive hardening: quotation of executable paths, least-privilege directory permissions, service-account review, continuous configuration auditing, and endpoint policy monitoring. The paper concludes that Defender should be evaluated not as a replacement for secure configuration management but as a complementary control within a layered Windows hardening strategy.

**Keywords:** Windows Defender, Microsoft Defender Antivirus, privilege escalation, unquoted service path, Windows services, configuration security, access control lists, endpoint protection, attack surface reduction, system hardening.

**Introduction.** Privilege escalation is one of the most important stages in a Windows compromise because it changes the attacker perspective from limited user activity to administrative or SYSTEM-level control. In many cases, this transition is not enabled by a memory-corruption flaw or a sophisticated exploit but by an operational misconfiguration that has remained unnoticed across software installations, updates, and administrative changes. Unquoted service path exploitation is a representative example of this category. It occurs when

the executable path of a Windows service contains spaces but is stored without quotation marks, allowing the service loader to interpret earlier path segments as executable candidates.

The issue is particularly relevant in enterprise environments because Windows services are frequently installed by third-party applications and often run with high privileges. A path such as C:\Program Files\Vendor App\service.exe should be stored as a quoted string. If it is not quoted, Windows path resolution can become ambiguous. The vulnerability becomes practically significant when a low-privileged user can write to an intermediate directory in the path. Under those conditions, an unintended executable may be placed where Windows searches before reaching the intended service binary, creating a local privilege-escalation opportunity.

Traditional studies of unquoted service paths usually focus on the vulnerability mechanism and on corrective actions such as adding quotation marks and hardening access control lists. This paper shifts the emphasis toward endpoint protection evaluation. Modern Windows environments commonly rely on Microsoft Defender Antivirus, Microsoft Defender for Endpoint, attack surface reduction rules, cloud-delivered protection, and Tamper Protection. These controls raise an important practical question: can Defender prevent configuration-based privilege escalation, or does it mainly reduce the risk after malicious execution begins?

The objective of this article is to evaluate Microsoft Defender effectiveness against the unquoted service path scenario as a case study of configuration-based privilege escalation. The paper does not present an offensive exploitation guide. Instead, it examines the security boundary between configuration auditing and malware prevention, identifies what Defender can reasonably detect, and proposes a hardening workflow that combines Defender policy with service configuration management.

The contribution of this paper is threefold. First, it reformulates unquoted service path exploitation as a measurable endpoint-protection evaluation problem rather than only as a Windows parsing issue. Second, it provides a controlled methodology for assessing Defender behavior against misconfigured services without using unauthorized systems. Third, it proposes a practical remediation model that distinguishes between configuration prevention, malicious payload blocking, and post-event detection.

**Literature Review.** Windows services are managed by the Service Control Manager, which reads each service configuration from the registry and starts the executable defined in the ImagePath value. Because many services run as LocalSystem, LocalService, NetworkService, or administrative accounts, weaknesses in service configuration can have direct security consequences. Prior work on Windows privilege escalation has repeatedly identified service misconfiguration as a persistent enterprise risk, especially where legacy installers, inherited directory permissions, and inconsistent administrative practices coexist.

Unquoted service path exploitation depends on two conditions. The first condition is syntactic ambiguity: the service path contains whitespace and is not enclosed in quotation marks. The second condition is authorization weakness: a low-privileged principal such as Users, Authenticated Users, or Everyone has write permission to an intermediate directory that Windows may evaluate during path resolution. Without writable permissions, an unquoted path remains a misconfiguration but may not be directly exploitable. Without the unquoted path, writable folders are still undesirable but do not create this specific parsing ambiguity. The vulnerability is therefore compound, involving both service metadata and NTFS access control.

Microsoft Defender Antivirus is designed primarily as endpoint anti-malware protection. It provides real-time protection, behavior monitoring, cloud-delivered protection, signature-

based detection, and integration with broader Defender for Endpoint capabilities. Microsoft documentation also describes evaluation procedures for Defender Antivirus using PowerShell and Group Policy, as well as management of exclusions, attack surface reduction rules, and Tamper Protection. These controls are important for reducing malware execution and for protecting security settings, but they do not automatically rewrite insecure ImagePath values or remove excessive directory permissions.

Attack surface reduction rules extend the defensive scope by blocking behaviors commonly used by malicious applications and scripts. They can reduce common initial execution and post-exploitation techniques, especially those involving Office, scripts, executable content from email, USB execution, credential theft behaviors, and suspicious process chains. However, ASR rules operate as policy-based behavior controls. They are not equivalent to a service configuration scanner and should not be expected to identify every unquoted path or every weak ACL.

Existing security guidance therefore supports a layered view. Defender contributes detection and blocking at the file, process, behavior, and policy levels. Configuration management contributes prevention at the registry, service-control, and filesystem-permission levels. A realistic evaluation of Defender against unquoted service paths must measure both parts separately: whether Defender detects the malicious artifact or behavior, and whether the underlying misconfiguration remains present after the event.

**Methodology.** The research design follows a controlled case-study model. A Windows virtual machine is prepared in an isolated lab network. Two user roles are defined: an administrative account used to create and remediate test services, and a standard user account used to run discovery checks from a low-privilege perspective. The lab does not interact with production systems, external users, or third-party services. The purpose is to observe defensive behavior and verify configuration hardening, not to conduct unauthorized exploitation.

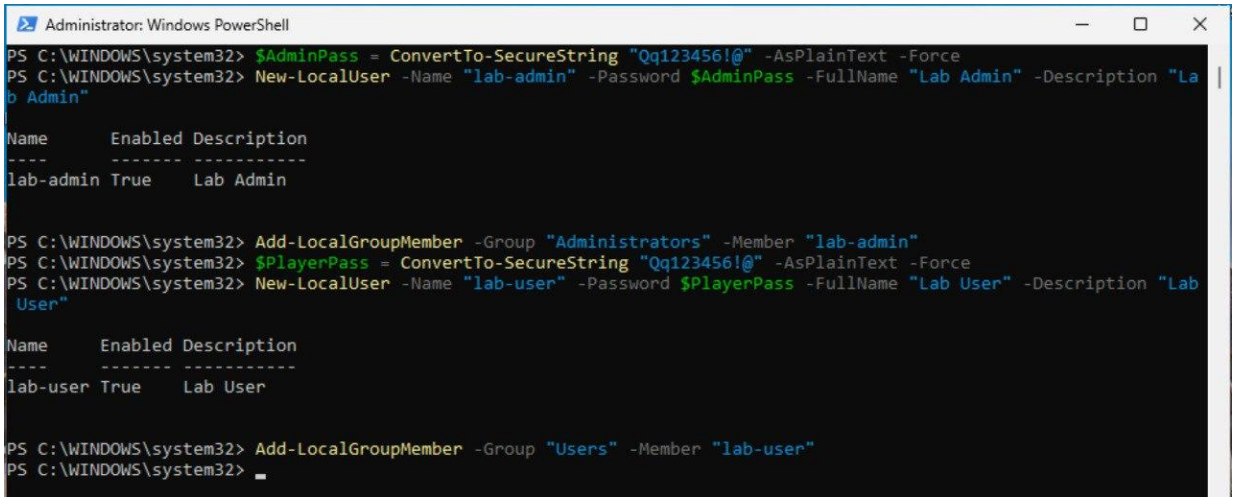



Figure 1. Creation of administrator and standard user accounts for the isolated Windows test environment.

The experimental variable is the service configuration. A vulnerable service condition is represented by three elements: an unquoted executable path containing spaces, an intermediate directory with excessive write permissions, and a service context with elevated privileges. A secure service condition is represented by the same service after remediation: the executable

path is fully quoted, writable permissions for standard users are removed from intermediate directories, and the service account is reviewed for least-privilege operation.

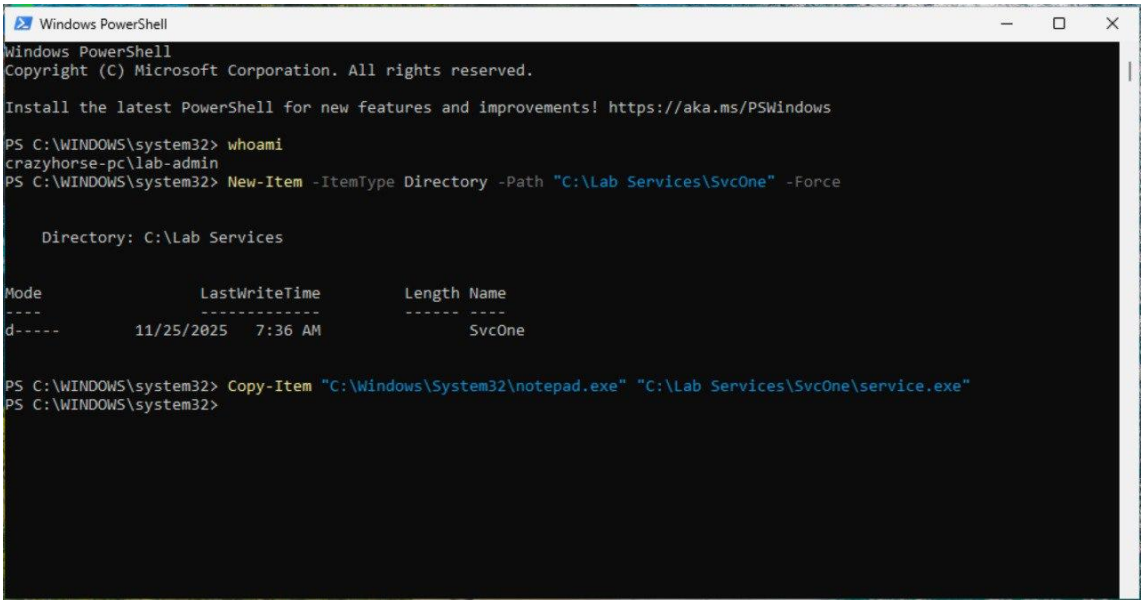



Figure 2. Preparation of a test service directory containing whitespace in the executable path.

A controlled vulnerable service was created with native Windows tools. The sc.exe utility was used to register the test service, while the Windows registry was inspected to verify how the service executable path was stored in the ImagePath value. This step was necessary because the security issue depends not only on the visible service path, but also on whether the path is stored with or without quotation marks.

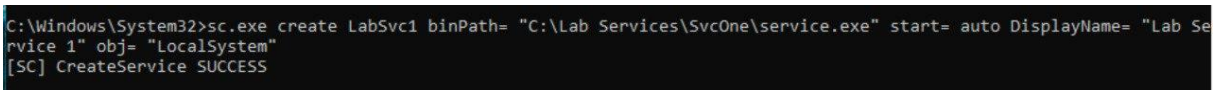



Figure 3. Creation of a Windows service used to reproduce the unquoted service path condition.

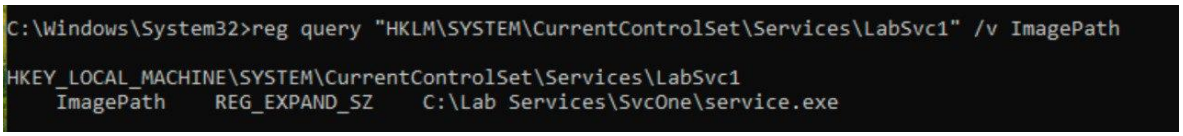



Figure 4. Registry verification of the unquoted service ImagePath used in the Defender evaluation scenario.

After the vulnerable service condition was confirmed, the experiment was interpreted through a Defender evaluation framework. The purpose of this framework was to separate two different security questions. The first question was whether Microsoft Defender could detect or block malicious activity related to the vulnerable service path. The second question was whether Defender could identify and correct the insecure configuration itself. This distinction is important because an unquoted service path is not a malicious file; it is a configuration weakness that becomes dangerous when combined with writable directories and elevated service privileges.

The evaluation framework consisted of four layers. The first layer was the configuration state, including the service ImagePath, quotation status, directory permissions, and service privilege context. The second layer was file execution, where Defender may detect or quarantine suspicious executables placed in service-related directories. The third layer was behavior monitoring, where Defender may generate alerts if the executed process performs suspicious actions. The fourth layer was policy integrity, including Tamper Protection, attack surface reduction rules, and exclusion review. Together, these layers made it possible to evaluate Defender fairly: not as a tool that automatically repairs service misconfigurations, but as an endpoint protection control that may reduce the impact of exploitation attempts.

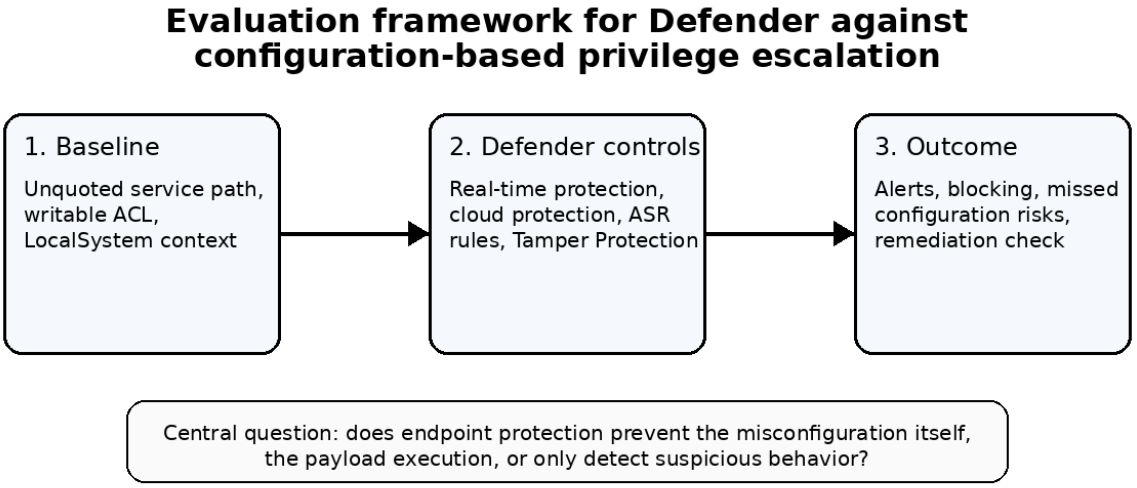



Figure 5. Conceptual framework for evaluating Defender against unquoted service path risks

The second part of the vulnerable condition was weak directory permission. NTFS permissions were inspected with folder security properties or the icacls utility. Special attention was given to write, modify, or full-control permissions granted to low-privileged groups such as Users or Authenticated Users. This stage is important because an unquoted service path alone is not always exploitable. The configuration becomes practically dangerous when a low-privileged user can write to an intermediate directory that Windows may check during ambiguous path parsing.

```
PS C:\WINDOWS\system32> icacls "C:\Custrom Services" /grant "Users:(OI)(CI)M"
processed file: C:\Custrom Services
Successfully processed 1 files; Failed processing 0 files
PS C:\WINDOWS\system32> icacls "C:\Custrom Services"
C:\Custrom Services BUILTIN\Users:(OI)(CI)(M)
                    BUILTIN\Administrators:(I)(OI)(CI)(F)
                    NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
                    BUILTIN\Users:(I)(OI)(CI)(RX)
                    NT AUTHORITY\Authenticated Users:(I)(M)
                    NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)

Successfully processed 1 files; Failed processing 0 files
```

Figure 6. Writable intermediate directory permissions required for practical privilege-escalation risk.

After documenting the writable-directory condition, the study proceeded to configuration auditing. This step was used to determine whether the vulnerable state could be identified independently of Defender malware alerts.

The configuration audit is performed with native Windows tools and PowerShell. Service paths are enumerated through Windows Management Instrumentation or CIM classes. Registry ImagePath values are inspected for unquoted paths containing whitespace. NTFS permissions are inspected using access-control-list queries, with special attention to write, modify, and full-control permissions granted to low-privileged groups. The audit also checks related privilege-escalation indicators, such as writable directories referenced in the PATH environment variable and insecure installer policies.

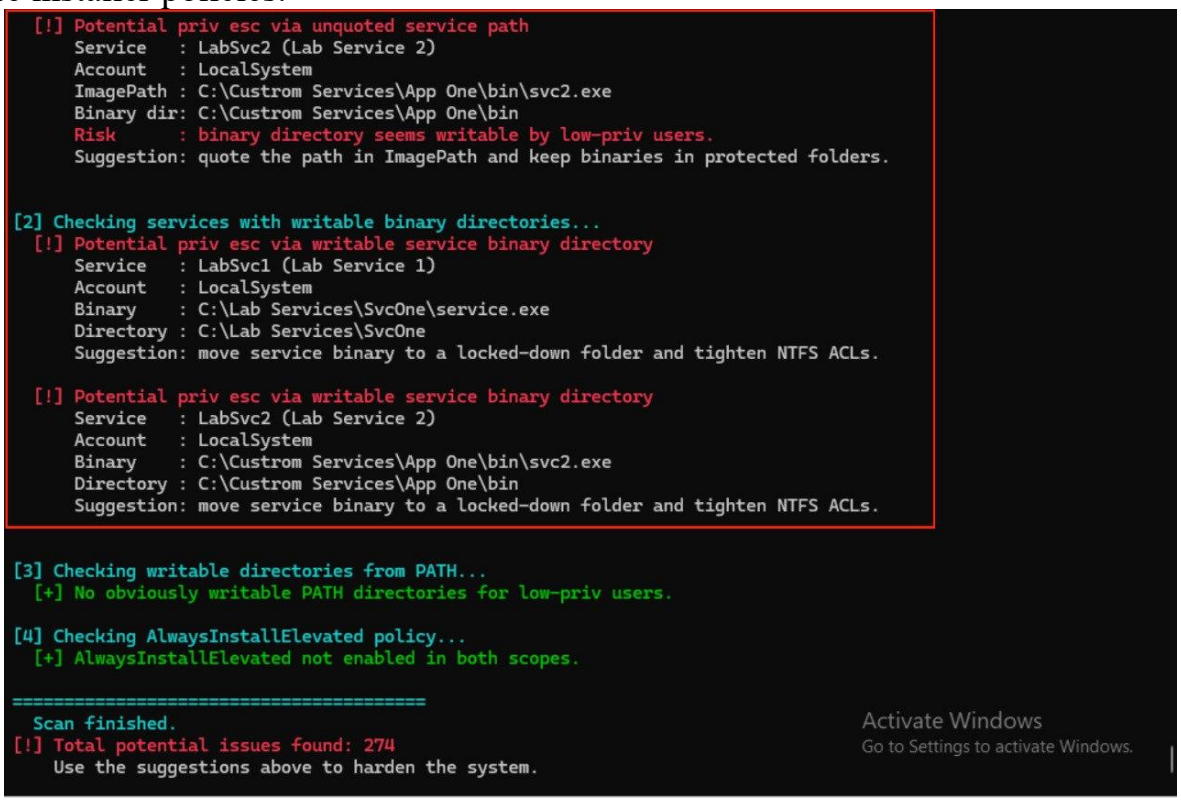



Figure 7. Configuration audit output identifying unquoted service paths and writable directory indicators.

The methodology separates configuration detection from payload detection. A Defender alert caused by a known malicious file does not mean the unquoted service path has been remediated. Conversely, absence of a Defender alert does not mean the configuration is safe. The service is considered secure only if subsequent audit results show that the path is quoted, intermediate directories are not writable by low-privileged users, and the service account is appropriate for its operational function.

After the vulnerable baseline was documented, remediation was applied. The executable path was corrected by enclosing the full service path in quotation marks. NTFS permissions were then hardened by removing write or modify access for low-privileged users from intermediate service directories. A repeated audit was performed to verify whether the tested privilege-escalation condition had been removed.

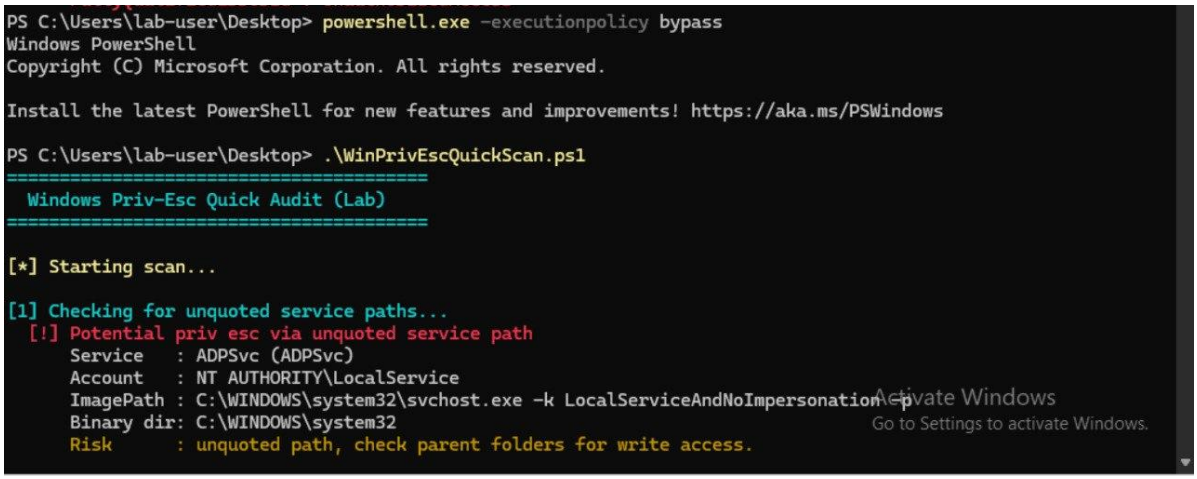



Figure 8. Validation after remediation by path quotation and ACL hardening.

The evaluation criteria are summarized in Table 1.

**Table 1 - Evaluation criteria for Defender and configuration hardening**

| Layer | Evaluation question | Defender role | Hardening action |
|---|---|---|---|
| Configuration | Is the service path or ACL insecure? | Does not automatically repair ImagePath or ACLs | Quote paths and restrict permissions |
| Execution | Is a suspicious binary launched? | May block or quarantine the file | Prevent write access to service paths |
| Behavior | Does the process act maliciously? | May generate behavior-based alerts | Investigate and fix root cause |
| Policy | Can protection be weakened? | Tamper Protection helps protect settings | Audit exclusions and centralize policy |

**Results.** The case study indicates that Microsoft Defender should be understood as an endpoint protection control rather than as an automatic service-configuration repair mechanism. As shown in Figures 3 and 4, the vulnerable baseline contained an unquoted service path stored in the service registry configuration. As shown in Figure 6, the scenario also included writable intermediate directory permissions. These two conditions created the configuration basis for privilege-escalation risk.

In the vulnerable baseline, the unquoted service path and weak directory permissions remained present until explicit administrative remediation was performed. Defender did not treat the unquoted ImagePath value itself as malware. This result is expected because the misconfiguration is stored in service metadata and filesystem ACLs, while antivirus engines primarily evaluate files, processes, scripts, memory behavior, network indicators, and suspicious activity chains.

When the test condition involved only the insecure configuration, Defender did not directly report the unquoted path as a malicious object. This is an important finding for administrators: the absence of a Defender alert is not evidence that the service configuration is secure. A service can remain vulnerable even when Defender status is healthy and real-time protection is enabled. Therefore, configuration scanning must be part of the evaluation procedure.

Defender effectiveness became more visible when the scenario moved from configuration state to execution state. If an executable candidate placed in a writable service-path location matched known malicious signatures, exhibited suspicious behavior, or triggered policy-

controlled actions, Defender could block, quarantine, or report it. However, a benign-looking or custom test binary may not be blocked solely because it is located in a risky path.

Attack surface reduction rules provided additional value by limiting selected behaviors commonly associated with malware execution. Nevertheless, ASR rules did not substitute for service-path auditing. Their role was preventive at the behavior-policy layer, not corrective at the service-registry layer. This distinction is central to evaluating Defender fairly: ASR may reduce the probability that a malicious payload succeeds, but it does not eliminate the root cause of unquoted service path exposure.

Remediation was effective only after applying configuration changes. Quoting the full executable path removed command-line parsing ambiguity. Removing Modify and Write permissions for low-privileged groups from intermediate directories prevented unauthorized placement of executable candidates. After remediation, a repeat audit no longer identified the tested privilege-escalation condition, as shown in Figure 8.

**Discussion.** The findings demonstrate that configuration-based privilege escalation occupies a defensive gap between endpoint malware detection and system hardening. Microsoft Defender is strong when the adversary action creates detectable file, process, script, or behavior evidence. It is less suited to silently correcting insecure administrative configurations unless combined with configuration management, security baselines, endpoint analytics, vulnerability management, or custom audit scripts.

This distinction has operational consequences. Security teams sometimes interpret endpoint-protection health as broad system security health. The case study shows why that interpretation is incomplete. A Windows host may report active Defender protection and still contain weak service permissions, unquoted paths, writable PATH directories, or risky installer policies. These weaknesses are not necessarily malicious by themselves; they are unsafe states that can be abused later.

A mature evaluation must therefore include two classes of indicators. The first class is protection indicators: Defender enabled, real-time protection active, cloud-delivered protection enabled, current security intelligence, Tamper Protection active where applicable, ASR rules deployed in audit or block mode, and exclusions minimized. The second class is configuration indicators: no unquoted service paths with spaces, no writable intermediate service directories, no high-privilege services controlled by ordinary users, no broad write access in service installation folders, and no unnecessary local administrator assignments.

The results also support a risk-based deployment approach. In audit mode, ASR and Defender events can help determine whether stricter policy might disrupt normal operations. After validation, relevant rules can be moved to block mode. In parallel, service-path and ACL remediation should be applied directly because it addresses the root cause and normally does not require accepting detection uncertainty. Administrators should prioritize services running as LocalSystem and services installed outside protected system directories.

The study has limitations. The evaluation uses a controlled lab rather than a large enterprise fleet, so it cannot represent every Defender configuration, every third-party service, or every tenant-level Defender for Endpoint feature. Detection results may vary based on security-intelligence version, cloud connectivity, policy state, licensing, exclusions, and EDR configuration. The study also avoids offensive payload development, so it evaluates defensive boundaries without claiming coverage against all real-world attacker variants.

**Practical Recommendations.** Organizations should treat Defender as one component of a layered control set. First, enable and monitor Microsoft Defender Antivirus real-time protection, cloud-delivered protection, and security-intelligence updates. Second, enable Tamper Protection where supported to reduce the risk of unauthorized changes to security settings. Third, deploy attack surface reduction rules through a staged process: audit mode for compatibility assessment, followed by block mode for rules that do not disrupt business workflows.

Fourth, minimize exclusions. Exclusions are sometimes necessary for compatibility, but broad folder exclusions around application or service directories can weaken detection exactly where service-path abuse may occur. Exclusion lists should be documented, justified, reviewed periodically, and scoped as narrowly as possible. Fifth, implement recurring service-configuration audits using PowerShell, endpoint management platforms, or vulnerability-management tools. Audit logic should identify unquoted paths with whitespace, writable directories in service paths, high-privilege service accounts, and user-startable privileged services.

Sixth, remediate root causes directly. Every service executable path containing spaces should be enclosed in quotation marks. Intermediate directories should grant write access only to trusted administrative principals and service-maintenance identities. Standard users should not have Modify or Full Control permissions over directories that participate in high-privilege service paths. Seventh, verify remediation by rescanning after every change, because successful hardening is demonstrated by the absence of the vulnerable condition, not by the absence of an antivirus alert.

Finally, integrate the findings into security operations. Defender alerts related to suspicious service execution should trigger both incident response and configuration review. If an alert is raised from a service directory, analysts should inspect the service ImagePath value and parent directory ACLs. This converts a file-level alert into a root-cause investigation and prevents repeated exposure after a single malicious artifact is removed.

**Conclusion.** This paper evaluated Microsoft Defender effectiveness against configuration-based privilege escalation using unquoted service path exploitation as a case study. The analysis shows that Defender can provide meaningful protection against malicious payloads, suspicious execution, and selected attack behaviors, especially when real-time protection, cloud-delivered protection, Tamper Protection, and attack surface reduction rules are properly configured. However, Defender does not inherently eliminate the underlying service misconfiguration. An unquoted service path combined with weak intermediate directory ACLs remains a configuration risk until administrators quote the path and harden permissions.

The central conclusion is that endpoint protection and secure configuration management solve different parts of the same risk. Defender reduces the probability and impact of malicious execution, while configuration auditing and hardening remove the privilege-escalation opportunity. Effective Windows defense requires both. Future work should extend this case study across larger endpoint populations, compare Defender for Endpoint telemetry with local PowerShell audit results, and evaluate how centralized security baselines can automatically detect and remediate service-path misconfigurations at scale.

**References:**

1. Microsoft. Microsoft Defender Antivirus in Windows. Microsoft Learn, 2026.
2. Microsoft. Evaluate Microsoft Defender Antivirus using PowerShell. Microsoft Learn, 2026.
3. Microsoft. Enable attack surface reduction rules. Microsoft Learn, 2025.
4. Microsoft. Attack surface reduction rules reference. Microsoft Learn, 2025.
5. Microsoft. Protect security settings with Tamper Protection. Microsoft Learn, 2025.
6. Microsoft. Configure custom exclusions for Microsoft Defender Antivirus. Microsoft Learn, 2026.
7. Microsoft. Enable and configure Microsoft Defender Antivirus always-on protection. Microsoft Learn, 2025.
8. MITRE. Unquoted Search Path or Element: CWE-428. Common Weakness Enumeration.
9. MITRE ATT&CK. Abuse Elevation Control Mechanism and Windows service-related privilege escalation techniques.
10. Russinovich M., Solomon D., Ionescu A., Yosifovich P. Windows Internals. 7th ed. Microsoft Press, 2017.
11. Sikorski M., Honig A. Practical Malware Analysis. No Starch Press, 2012.
12. Howard M., LeBlanc D. Writing Secure Code. 2nd ed. Microsoft Press, 2003.
13. National Institute of Standards and Technology. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. NIST SP 800-83 Rev. 1, 2013.
14. National Institute of Standards and Technology. Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53 Rev. 5, 2020.
15. Center for Internet Security. CIS Microsoft Windows 11 Enterprise Benchmark. CIS Benchmarks, 2025.
16. Microsoft. Windows security baselines. Microsoft Learn, 2025.
17. Microsoft. Windows Defender Application Control and endpoint security management documentation. Microsoft Learn, 2025.

## ЭКОНОМИКАЛЫҚ ЖӘНЕ ҚҰҚЫҚ ҒЫЛЫМДАРЫ - ЭКОНОМИЧЕСКИЕ И ЮРИДИЧЕСКИЕ НАУКИ - ECONOMIC AND LEGAL SCIENCES

**УДК 342**

**Трусов Георгий Сергеевич**
студент 2 курса
факультет непрерывного образования по подготовке
специалистов для судебной системы
Научный руководитель: **Волошин Олег Викторович**,
старший преподаватель
кафедра государственно-правовых дисциплин
Дальневосточный филиал РГУП им. В.М. Лебедева
(г. Хабаровск, Россия)

# АДМИНИСТРАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРОТИВОДЕЙСТВИЯ КОРРУПЦИИ В СОЦИАЛЬНОЙ СФЕРЕ

**Аннотация:** В статье рассматриваются актуальные вопросы противодействия коррупции в системе государственной и муниципальной службы Российской Федерации. С помощью современной судебной практики и региональных нормативных актов. Рассматриваются причины коррупционных проявлений и механизмы их пресечения. Особое внимание уделяется специфике дисциплинарной ответственности служащих как элементу обеспечения законности и защиты публичных интересов. Указывается значимость мониторинга законодательства и внедрения мер по обеспечению прозрачности деятельности должностных лиц для укрепления стабильности государства.

**Ключевые слова:** Коррупция, социальная сфера, правонарушения, система, Пленум ВС РФ, государство, граждане, штраф, КоАП.

В современности борьба с коррупцией является одной из главных потребностей российского общества, ведь именно она затрагивает различные сферы публичной и непубличной экономики в государстве. Бывают моменты, когда те, кто должны помогать и защищать интересы граждан в лице компетентных органов берут взятки или вымогают их у людей, нарушая тем самым закон и права граждан.

Так, например, в августе 2025 года Новосибирской области женщина, работающая ранее в социальной сфере по поддержке молодых бизнесменов по субсидиям и их контролю за расходом средств, выделенных государством. Когда к ней пришла предпринимательница с повреждённым документом о расходах, то тогда сотрудница социальной помощи предложила ей решить проблему за персональную выплату в размере 25 тысяч рублей. «Суд признал гражданку виновной во взяточничестве и назначил наказание в виде трёх лет лишения свободы условно, штрафа в 50 тысяч рублей, а также запрета на работу в сфере реализации госпрограмм на два года. Кроме того, суд постановил конфисковать взятку в размере 25 тысяч рублей»[1].

[1] 2026 ГТРК «Новосибирск» Государственный интернет-канал "Россия" (свидетельство о регистрации ЭЛ № ФС 77-59166 от 22.08.2014). Учредитель - федеральное государственное унитарное предприятие "Всероссийская государственная телевизионная и радиовещательная компания" (ВГТРК)

В 2023 году были уволены муниципальные служащие за утрату доверия перед населением за коррупционное правонарушение в размере 57 миллиардов рублей.

Данные примеры наглядно показывают, что коррупция создаёт угрозу стабильности и развитию, как населения так и государства. Поэтому контроль за публичными образованиями и органами, их представляющих, является необходимым аспектом в развитии государства.

В России значимое внимание уделяется борьбе с коррупцией в государственной и муниципальной службе, осуществляющая применение дисциплинарных мер для поддержания порядка и обеспечения должного исполнения обязанностей, касающихся интересов граждан.

«Отношения государственных и муниципальных служащих с нанимателем носят публичный характер и регулируются особым образом. Это связано с тем, что служащие выполняют общественно-значимые функции и несут обязанности по соблюдению дисциплины, поэтому наниматель в рамках служебного контракта обладает в части привлечения к дисциплинарной ответственности большей свободой, чем работодатель в рамках трудового договора»[2]. Данная точка зрения Очаковского В.А, Крутовой Я.А и Жуковой Н.А имеет ключевое значение, в силу того что элементы социальной сферы представляются учреждениями.

Основными причинами коррупции являются нестабильность экономического развития граждан, корыстное намерение сотрудников занимаемой ими должности, что в последующим приводит к нарушениям действующего законодательства.

Например, Распоряжение от 20 декабря 2024 г. № 149-рк «О Плане мероприятий Законодательной Думы Хабаровского края по противодействию коррупции на 2025 - 2028 годы»[3]. Ориентировано на «Мониторинг федеральных законов, иных нормативных правовых актов Российской Федерации, судебной практики по вопросам противодействия коррупции и по его результатам подготовка соответствующих изменений в законы Хабаровского края»[4]. А также разработка Министерством труда и социальной защиты методических материалов по противодействию коррупции. Прозрачность деятельности депутатов и других государственных служащих, предоставление деклараций о доходах и имущественных благ.

Конечно, коррупционная деятельность не исчезла сразу, к примеру, «За 2025 год в Хабаровском крае зарегистрировано 184 преступления коррупционной направленности, по итогам прокурорских проверок возбуждены новые уголовные дела. В основе таких преступлений чаще всего лежали откаты за покровительство при заключении контрактов, подписание документов по некачественным работам и взятки за информирование о контрольных мероприятиях»[5].

[2] Очаковский В.А. Крутова Я.А., Жукова Н.А. Дисциплинарная ответственность государственных гражданских служащих в Российской Федерации // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2014. № 99. С.5

[3] Распоряжение от 20 декабря 2024 г. № 149-рк О Плане мероприятий Законодательной Думы Хабаровского края по противодействию коррупции на 2025 - 2028 годы

[4] Распоряжение от 20 декабря 2024 г. № 149-рк О Плане мероприятий Законодательной Думы Хабаровского края по противодействию коррупции на 2025 - 2028 годы

[5] Еженедельник «Аргументы и Факты» № 32. «АиФ-Дальинформ» № 32 06/08/2025 Алексей Лукоянов «Более ста чиновников попали под уголовку за коррупцию в Хабаровском крае»

Рассматривая коррупцию в социальной сфере, можно сказать, что она затрагивает граждан, находящихся в трудном жизненном положении, а сама коррупция существует на уровне и в пределах применения социальной системы.

Весьма часто в коррупционных правонарушениях встречаются нарушения, связанные со статьёй 15.14 КоАП РФ, которая устанавливает административную ответственность за нецелевое использование бюджетных средств в виде наложения штрафа или дисквалификацию от 1 года до 3 лет, а на юридических лиц от 5 до 25 процентов от суммы, полученной из бюджета РФ.

Постановление Пленума Верховного Суда РФ от 09.07.2013 N 24 (ред. от 09.12.2025) О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях» говорит о коррупционных преступлениях, что «Правосудие по таким делам должно осуществляться на основе соблюдения принципов независимости судебной власти, состязательности и равноправия сторон, соблюдения прав и свобод человека, в строгом соответствии с требованиями уголовного и уголовно-процессуального законодательства»[6].

В лекции от 20.05.2025 на Петербургском международном юридическом форуме В.Д.Зорькин назвал коррупцию «угрозой цивилизации права и она отчуждает государство от народа, лишает граждан социальных, экономических и политических благ, снижает качество государственных услуг и инфраструктуры»[7].

По мнению Курганской А.А и Очаковского В.А, «одним из наиболее серьёзных, катализаторов административных правонарушений в социальной сфере является децентрализация»[8].

Разумеется, тенденция развития разделения правового регулирования существует и применяется, но контроль за субъектами осуществлять весьма затруднительно, что и приводит к взятничеству среду сотрудников социальной сферы.

При этом есть необходимость проведения стандартизации системы применения мер административного противодействия коррупции в социальной сфере, в особенности — создание единой системы форм и методов их реализации на уровне федерации, субъектов, и на местном уровне.

Дополнительно системой мер по противодействию коррупционным правонарушениям могут способствовать разработки комплексных систем моральной и материальной базы работников, занимающихся социальной сферой. Из этого вытекает обеспечение формирования на рабочих местах системы поощрительных мер и стратегий карьерных направлений.

Можно отметить, что повышения заработной платы в государственных учреждениях и улучшения материального состояния работников поможет уменьшить коррупцию, но не убрать её полностью, поскольку бывают сотрудники, которые устраиваются в социальную сферу в корыстных целях. Что и подрывает доверие населения к государственным органам, а это негативно сказывается на реализации деятельности сотрудников в социальной сфере.

---

[6] Постановление Пленума Верховного Суда РФ от 09.07.2013 N 24 (ред. от 09.12.2025) «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях»

[7] Коррупция – угроза цивилизации права. Лекция на Петербургском международном юридическом форуме (Санкт-Петербург, 20 мая 2025 года)

[8] Курганская Алина Александровна, Очаковский Виктор Александрович Административно-правовое регулирование противодействия коррупции в социальной сфере // Вестник экономики и права. 2024. №94.(дата обращения: 09.02.2026).

Н. П. Мышляев подчёркивает, что «.Без изучения причин и условий, способствующих проявлению административной деликтологии невозможно на научной основе разработать мероприятия по организации борьбы с административными правонарушениями не только силами правоохранительной системы, деятельность которой основана на законе, но и экономических, социальных и иных рычагов, которыми общество и государство располагает»[9].

Таким образом, административно-правовое регулирование по противодействию коррупции в социальной сфере является многогранным и сложным процессом, который требует выработки системы определённых норм по административному характеру и усилий государства в обеспечении порядка, устойчивости на уровне социальной сферы граждан. Существенную роль в противостоянии коррупции играет увеличение зарплат сотрудникам, а вдобавок введение мер, по которым у работников социальной сферы будут бенефиты. Перспективная борьба с коррупцией улучшит доверие населения к государственным органам и ликвидирует возможность взимание платы с бесплатных услуг у граждан.

**Литература:**

1. Постановление Пленума Верховного Суда РФ от 09.07.2013 N 24 (ред. от 09.12.2025) «О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях»

2. Распоряжение от 20 декабря 2024 г. № 149-рк О Плане мероприятий Законодательной Думы Хабаровского края по противодействию коррупции на 2025 - 2028 годы

3. Распоряжение от 20 декабря 2024 г. № 149-рк О Плане мероприятий Законодательной Думы Хабаровского края по противодействию коррупции на 2025 - 2028 годы

4. Курганская Алина Александровна, Очаковский Виктор Александрович Административно-правовое регулирование противодействия коррупции в социальной сфере // Вестник экономики и права. 2024. №94.(дата обращения: 09.02.2026).

5. Мышляев Н. П. Теоретические и прикладные основы административной деликтологии: дисд-ра юрид. наук. М., 2004. С. 28

6. Очаковский В.А. Крутова Я.А., Жукова Н.А. Дисциплинарная ответственность государственных гражданских служащих в Российской Федерации // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2014. № 99. С.5

7. ГТРК 2026 «Новосибирск» Государственный интернет-канал "Россия" (свидетельство о регистрации ЭЛ № ФС 77-59166 от 22.08.2014). Учредитель - федеральное государственное унитарное предприятие "Всероссийская государственная телевизионная и радиовещательная компания" (ВГТРК)

8. Еженедельник «Аргументы и Факты» № 32. «АиФ-Дальинформ» № 32 06/08/2025 Алексей Лукоянов «Более ста чиновников попали под уголовку за коррупцию в Хабаровском крае»

9. Коррупция – угроза цивилизации права. Лекция на Петербургском международном юридическом форуме (Санкт-Петербург, 20 мая 2025 года)

[9] Мышляев Н. П. Теоретические и прикладные основы административной деликтологии: дисд-ра юрид. наук. М., 2004. С. 28

UDC 004.056:351

**Dossymov Aldiyar Nurkhatuly**

2nd year student, Master's degree
School of Digital Public Administration
Astana IT University
(Astana, Kazakhstan)

# CYBERSECURITY GOVERNANCE IN KAZAKHSTAN'S DIGITAL PUBLIC SECTOR: TOWARD AN INTEGRATED FRAMEWORK

**Abstract**. The article examines cybersecurity governance in Kazakhstan's digital public sector. It argues that, in the context of digital public administration, cybersecurity should be viewed not only as a technical function, but also as a governance capability. Although Kazakhstan has developed digital public services, cybersecurity policies, institutional structures and technical tools, formal readiness does not automatically ensure operational cybersecurity effectiveness. The article identifies key problems such as fragmented coordination, uneven institutional maturity and insufficient risk-based management. Based on international approaches and comparative governance principles, the article proposes an integrated cybersecurity governance framework for Kazakhstan's public sector.

**Keywords**: cybersecurity governance, digital governance, public sector, Kazakhstan, risk management, institutional maturity, digital public services.

**Introduction.** Digital transformation has become one of the key directions in the modernization of public administration. Governments increasingly use digital platforms, mobile applications, public databases, digital identity systems and inter-agency data exchange mechanisms to provide public services and improve administrative efficiency. As a result, digital public services are no longer only an additional service channel. They are becoming a core infrastructure of public administration.

Kazakhstan is a relevant case for studying cybersecurity in digital governance. The country has achieved significant progress in e-government development. According to the United Nations E-Government Survey 2024, Kazakhstan ranked 24th in the E-Government Development Index and achieved an EGDI score of 0.9009 [1]. In addition, Kazakhstan received 94.04 out of 100 in the Global Cybersecurity Index 2024 [2]. These indicators demonstrate that the country has developed a strong formal foundation for digital government and cybersecurity.

Kazakhstan's cybersecurity policy direction is also reflected in national strategic documents, including the Concept of Cybersecurity "Cyber Shield of Kazakhstan" and the Concept of Digital Transformation, ICT Development, and Cybersecurity [11], [12]. These documents show that cybersecurity is recognized at the state level as an important condition for digital transformation and national information security.

However, formal readiness does not automatically mean operational effectiveness. The presence of digital platforms, legal measures, cybersecurity policies, institutions and technical tools does not guarantee that cyber risks are managed consistently across all public sector institutions. Public institutions may differ in their resources, technical capacity, cybersecurity maturity, staff skills and ability to implement security requirements in practice.

The main problem addressed in this article is the gap between formal cybersecurity readiness and operational cybersecurity governance effectiveness. Cybersecurity tools may exist, but their effectiveness depends on how they are governed, coordinated, prioritized and improved. Therefore, cybersecurity in the public sector should be considered not only as a technical function, but as a governance capability.

The aim of this article is to propose an integrated cybersecurity governance framework for Kazakhstan's digital public sector. The article focuses on the following question: how can cybersecurity methods and tools be structured into a governance framework that supports the protection of Kazakhstan's public sector from cyber threats?

**Cybersecurity as a Governance Capability**

Cybersecurity is often associated with technical tools such as firewalls, access control systems, encryption, monitoring platforms, anti-malware solutions, vulnerability scanners and incident response tools. These instruments are necessary for protecting information systems and data. However, international standards and frameworks show that cybersecurity effectiveness depends not only on tools, but also on governance, risk management, institutional responsibility and continuous improvement.

The NIST Cybersecurity Framework structures cybersecurity activities around identifying, protecting, detecting, responding and recovering from cyber risks [3]. ISO/IEC 27001 emphasizes leadership, risk assessment, control implementation, monitoring and continual improvement as part of an information security management system [4]. The OECD also treats digital security risk as an economic and social risk that should be integrated into organizational and governmental decision-making [5]. These approaches show that cybersecurity is not only a technical task, but also a management and governance process.

Zero Trust architecture and digital identity guidelines are also relevant for public sector cybersecurity because they connect access control, identity verification, least-privilege principles and continuous monitoring with institutional governance [6], [7]. In a digital public sector, where citizens, civil servants, contractors and administrators interact with digital systems, identity and access governance become essential elements of cybersecurity management.

In the public sector, this governance dimension is especially important. Public institutions provide essential services, process sensitive citizen data and operate within complex institutional structures. A cyber incident in one institution may affect not only one system, but also other organizations connected through shared infrastructure, data exchange and digital service platforms. ENISA threat landscape reports also show that public administration remains exposed to evolving cyber threats, which makes cybersecurity governance a continuing priority for states and public institutions [9].

From a governance perspective, cybersecurity requires several elements. First, responsibilities must be clearly assigned across leadership, information security units, data owners, process owners and operational teams. Second, cyber risks should be prioritized according to the criticality of public services. Third, institutions should regularly assess their cybersecurity maturity and improve their capabilities. Fourth, implementation should be measurable through evidence, indicators, audits and incident learning.

CISA's Zero Trust Maturity Model is useful in this context because it presents cybersecurity development as a gradual maturity process rather than a one-time technical

deployment [10]. This logic is especially important for Kazakhstan's public sector, where institutions may differ in resources, technical infrastructure and organizational capacity.

**International Practices and Their Relevance for Kazakhstan**

International practices provide useful principles for Kazakhstan, but they should not be copied directly. Estonia, Singapore and the European Union are particularly relevant because they represent different models of cybersecurity governance.

Estonia demonstrates the importance of secure digital infrastructure and accountable data exchange. Its experience is useful because Kazakhstan also relies on e-government platforms, public databases, digital identity mechanisms and inter-agency data exchange. The main lesson from Estonia is that cybersecurity should be embedded into digital governance infrastructure through secure interoperability, auditability and institutional responsibility [13].

Singapore demonstrates the value of central coordination and whole-of-government cybersecurity leadership. This is relevant for reducing fragmentation in public sector cybersecurity. A centralized governance approach helps clarify national priorities, define responsibilities and coordinate institutions responsible for critical digital services [14].

The European Union is useful not as a single country, but as a reference model of multi-level cybersecurity governance. The EU demonstrates how common cybersecurity requirements, certification logic, incident reporting and maturity-oriented approaches can be coordinated across different institutions and sectors. The EU Cybersecurity Act also demonstrates the role of harmonized cybersecurity requirements and certification mechanisms in multi-level governance [8]. This is relevant for Kazakhstan because public institutions also differ in maturity, resources and technical capacity, while still needing common cybersecurity baselines.

**Table 1. Comparative adaptation logic of international practices**

| Reference case | Governance principle | Relevance for Kazakhstan |
|---|---|---|
| Estonia | Secure interoperability and accountable data exchange | Useful for digital identity, public registries and inter-agency data exchange |
| Singapore | Central coordination and whole-of-government cybersecurity leadership | Useful for reducing fragmentation and clarifying responsibility |
| European Union | Harmonized requirements and maturity-oriented governance | Useful for minimum public sector baselines, reporting and maturity assessment |

The comparative lesson is that Kazakhstan should not mechanically transfer foreign models. Instead, it should adapt selected principles: secure data exchange, central coordination, harmonized minimum requirements, risk-based management and institutional maturity assessment.

**Key Governance Gaps in Kazakhstan's Digital Public Sector**

The analysis of Kazakhstan's digital and cybersecurity context shows that the country has made important progress in formal readiness. However, several governance gaps may limit the practical effectiveness of cybersecurity methods and tools.

The first gap is fragmented coordination. Kazakhstan's public sector includes central government bodies, local executive bodies, quasi-public organizations, national operators and service-providing institutions. These actors may have different responsibilities, resources and cybersecurity practices. Without strong coordination, cybersecurity measures can become inconsistent across institutions.

The second gap is uneven institutional maturity. Some institutions may have advanced monitoring, access control and incident response procedures, while others may rely mainly on formal compliance. In a digital governance ecosystem, uneven maturity is a serious problem because public institutions are interconnected. A weak institution may create risks for other systems and services.

The third gap is insufficient risk-based prioritization. In a compliance-oriented approach, institutions may focus on meeting formal requirements without fully considering which systems are most critical. However, digital identity systems, public registries, tax platforms, healthcare databases and social support systems should have higher protection requirements than low-risk systems.

The fourth gap is the implementation gap. Policies and standards may exist, but the practical question is whether they are implemented, monitored, tested and improved. Cybersecurity governance must therefore include evidence of implementation, key performance indicators, incident reporting, audit and continuous improvement.

These gaps support the main argument of the article: cybersecurity effectiveness in Kazakhstan's digital public sector depends not only on the presence of tools, but on the governance structure that connects tools with institutional responsibilities, risks and implementation mechanisms.

**Proposed Cybersecurity Governance Framework**

Based on the identified gaps, an integrated cybersecurity governance framework for Kazakhstan's digital public sector can be structured around four components: governance coordination, risk-based management, institutional maturity and implementation mechanisms.

The first component is governance coordination. Its purpose is to clarify roles and responsibilities across different levels of the public sector. At the national level, cybersecurity governance should define policy direction, common requirements and national priorities. At the inter-agency level, it should support coordination protocols for shared services and joint risks. At the institutional level, it should define responsibilities of leadership, information security units, data owners and process owners. At the operational level, it should include SOC teams, administrators, employees and contractors.

The second component is risk-based management. Its purpose is to prioritize cybersecurity measures according to the criticality and risk profile of public digital services. This component includes asset and service identification, criticality classification, risk assessment, control prioritization and continuous monitoring. The key idea is that not all systems require the same level of protection. Critical public services should receive stronger controls, regular testing and higher maturity requirements.

The third component is institutional cybersecurity maturity. Its purpose is to assess and improve cybersecurity capability over time. A five-level maturity model can be used: Initial, Basic Compliance, Managed, Integrated and Optimized. At the initial level, cybersecurity practices are mostly reactive. At the basic compliance level, minimum formal requirements exist. At the managed level, risks, controls and incidents are documented and monitored. At the

integrated level, cybersecurity is connected to institutional governance and inter-agency coordination. At the optimized level, cybersecurity is continuously improved through monitoring, audits, testing and lessons learned.

The fourth component is implementation mechanisms. Their purpose is to translate governance principles into practical actions. These mechanisms may include minimum cybersecurity requirements, risk-based control mapping, incident response coordination, access and identity governance, training and awareness, monitoring and reporting, audit and continuous improvement.

**Table 2. Components of the proposed cybersecurity governance framework**

| Framework component | Purpose | Practical mechanisms |
|---|---|---|
| Governance coordination | Clarify roles and cooperation across public sector levels | National coordination, inter-agency protocols, institutional responsibilities, operational feedback |
| Risk-based management | Prioritize protection according to service criticality and risk | Asset identification, risk assessment, control prioritization, monitoring |
| Institutional maturity | Assess and improve cybersecurity capability | Maturity levels from Initial to Optimized, capability development, reassessment |
| Implementation mechanisms | Translate principles into practical actions | Minimum requirements, access governance, incident response, training, audit |

The proposed framework can be presented as a layered structure. Implementation mechanisms form the operational base of the model, while institutional cybersecurity maturity and risk-based management connect practical actions with strategic governance coordination. This structure shows that cybersecurity governance should operate both from bottom to top and from top to bottom: operational implementation informs strategic governance, while strategic direction guides practical execution [Figure 1].

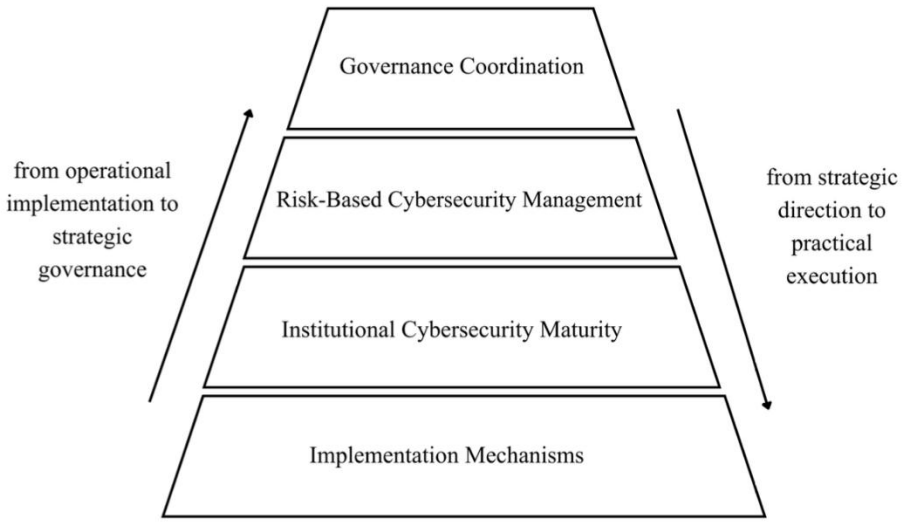



Figure 1. Layered structure of the framework

Governance coordination is organized across four levels: national, inter-agency or sectoral, institutional and operational. The model shows that cybersecurity governance requires both top-down standards and bottom-up reporting. This is important because public digital services depend on multiple institutions, shared systems and continuous feedback from operational practice [Figure 2].


Figure 2. Cybersecurity governance coordination model

The risk-based cybersecurity management cycle shows how protection of critical digital public services can be organized in practice. The process begins with asset and service identification, followed by criticality classification, risk assessment, control prioritization, and continuous monitoring. This cycle supports a shift from uniform compliance to risk-based protection of the most important public services [Figure 3].

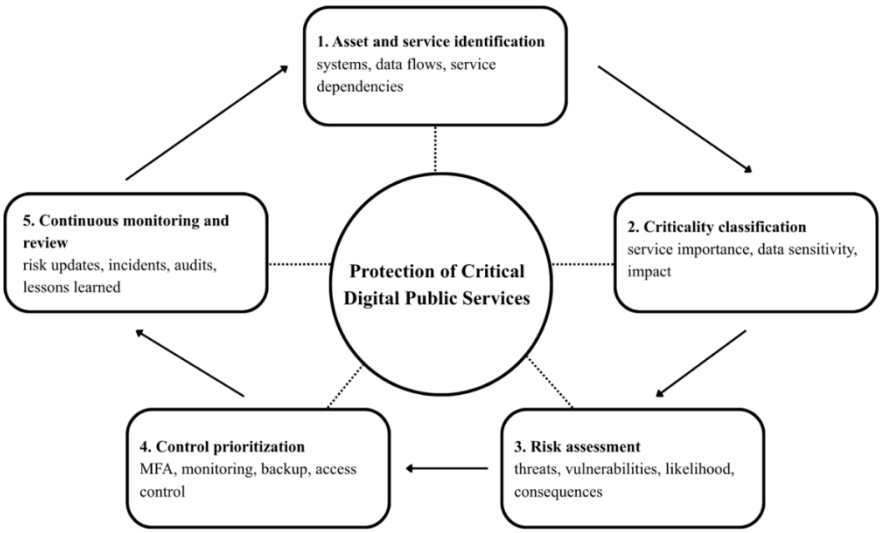



Figure 3. Risk-Based Cybersecurity Management Cycle

The public sector cybersecurity maturity model provides a structured way to assess the development of cybersecurity capabilities across institutions. It compares five maturity levels

across key dimensions such as governance and accountability, risk management, technical controls, incident response, human capacity and continuous improvement. This table helps identify whether an institution remains at a basic compliance level or moves toward integrated and optimized cybersecurity governance [Table 3].

**Table 3. Public sector cybersecurity maturity model**

| Assessment dimension | Level 1. Initial | Level 2. Basic Compliance | Level 3. Managed | Level 4. Integrated | Level 5. Optimized |
|---|---|---|---|---|---|
| **Governance and accountability** | Roles are unclear; cybersecurity depends on individual employees | Minimum formal responsibilities exist | Clear internal responsibilities are assigned | Cybersecurity is integrated into institutional governance | Cybersecurity is treated as a strategic governance capability |
| **Risk management** | Risks are not systematically identified | Risk assessment is limited and compliance-driven | Regular risk assessments are conducted | Risks are linked to service criticality and institutional priorities | Risk management is continuous, adaptive, and decision-oriented |
| **Technical controls** | Basic or fragmented tools exist | Basic required controls are implemented | Controls are documented, monitored, and reviewed | Controls are aligned with critical systems and inter-agency dependencies | Advanced controls, continuous monitoring, and proactive protection are used |
| **Incident response** | Response is reactive and informal | Incident procedures exist mainly on paper | Incidents are recorded, escalated, and reviewed | Cross-agency incident response is coordinated | Lessons learned from incidents are systematically used to improve resilience |
| **Human capacity** | Awareness is low and training is irregular | General cybersecurity training is provided occasionally | Role-based training begins for key staff | Security culture is developing across the institution | Strong cybersecurity culture and continuous staff development are institutionalized |
| **Continuous improvement** | No regular review or improvement process exists | Reviews are occasional and mainly audit-driven | Improvement actions are planned and tracked | Maturity is assessed regularly and improvement is coordinated | Continuous improvement is institutionalized through monitoring, audits, testing, and lessons learned |

This framework connects cybersecurity methods and tools with governance mechanisms. It does not replace technical standards or security controls. Instead, it provides a management structure for applying them more consistently across Kazakhstan's public sector.

**Practical Value of the Framework**

The proposed framework has several practical benefits for Kazakhstan's public sector.

First, it helps reduce governance fragmentation by defining coordination levels and responsibilities. This is important because digital public services often depend on several institutions and shared infrastructure.

Second, it supports protection of critical digital public services. Through risk-based prioritization, resources can be focused on services with the greatest importance for citizens, public administration and national resilience.

Third, it improves accountability. Cybersecurity responsibility should not be limited to IT departments. It should involve leadership, data owners, process owners, legal units, procurement units, technical teams and employees.

Fourth, the framework supports maturity development. A maturity model allows institutions to assess their current level and plan gradual improvement. It also helps policymakers identify institutions that need additional support, training or supervision.

Fifth, the framework supports continuous improvement. Cyber threats change constantly, so cybersecurity governance should include monitoring, audit, staff training, incident review and regular reassessment of risks.

Overall, the practical value of the framework lies in its ability to move cybersecurity from separate technical actions toward coordinated public sector management. This is especially important in digital governance, where public service continuity, data protection and citizen trust depend on the resilience of interconnected systems.

**Conclusion.** Cybersecurity in Kazakhstan's digital public sector should be strengthened not only through additional technical tools, but also through better governance. Kazakhstan has developed a strong formal foundation for digital government and cybersecurity, as shown by its progress in international digital government and cybersecurity indicators. However, formal readiness does not automatically ensure operational cybersecurity effectiveness.

The key challenge is how cybersecurity methods and tools are coordinated, prioritized, implemented and improved across public sector institutions. Fragmented coordination, uneven institutional maturity and insufficient risk-based management may reduce the effectiveness of existing cybersecurity measures.

The proposed framework structures cybersecurity governance around four components: governance coordination, risk-based management, institutional maturity and implementation mechanisms. Its practical value lies in helping public institutions reduce fragmentation, protect critical digital public services, improve accountability and support continuous improvement.

Future research should test the proposed framework in selected public institutions, conduct broader expert surveys, apply the maturity model across sectors and examine cybersecurity governance in specific areas such as healthcare, taxation, education, digital identity and public registries.

**References:**

1. United Nations Department of Economic and Social Affairs. UN E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development. United Nations, 2024.

2. International Telecommunication Union. Global Cybersecurity Index 2024. ITU Publications, 2024.
3. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. NIST, 2018. DOI: 10.6028/NIST.CSWP.04162018.
4. ISO/IEC. ISO/IEC 27001:2022 — Information Security Management Systems. International Organization for Standardization, 2022.
5. OECD. Recommendation on Digital Security Risk Management for Economic and Social Prosperity. OECD Legal Instrument 0497, 2022.
6. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture, NIST SP 800-207. National Institute of Standards and Technology, 2020.
7. Grassi P. A., Garcia M. E., Fenton J. L. Digital Identity Guidelines, NIST SP 800-63-3. National Institute of Standards and Technology, 2020.
8. European Parliament and Council. Regulation (EU) 2019/881 — Cybersecurity Act. Official Journal of the European Union, 2019.
9. ENISA. ENISA Threat Landscape 2023. European Union Agency for Cybersecurity, 2023.
10. CISA. Zero Trust Maturity Model. U.S. Cybersecurity and Infrastructure Security Agency, 2021.
11. Government of Kazakhstan. Concept of Cybersecurity “Cyber Shield of Kazakhstan”. Decree No. 407, Astana, 2017.
12. Ministry of Digital Development, Innovation and Aerospace Industry of Kazakhstan. Concept of Digital Transformation, ICT Development, and Cybersecurity. Astana, 2021.
13. e-Estonia. X-Road and Digital Society. Official e-Estonia materials.
14. Cyber Security Agency of Singapore. Singapore Cybersecurity Strategy 2021.

**ПЕДАГОГИКА ЖӘНЕ ПСИХОЛОГИЯ ҒЫЛЫМДАР - ПЕДАГОГИЧЕСКИЕ И ПСИХОЛОГИЧЕСКИЕ НАУКИ - PEDAGOGICAL AND PSYCHOLOGICAL SCIENCES**

**ӘОЖ 51-72**

**Серік Дана Қанатқызы**

1-курс магистранты
Физика және математика кафедрасы
**Ғылыми жетекші:** Смағулов Есенғали Жексембайұлы
ф.-м.ғ.к., п.ғ.д., профессор
Информатика және білімді цифрландыру кафедрасы
Жансүгіров атындағы Жетісу университеті
(Талдықорған қ., Қазақстан)

# МАТЕМАТИКА САБАҒЫНДА ФИЗИКАЛЫҚ МАЗМҰНДЫ ЕСЕПТЕРДІ ШЕШУДЕ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАРДЫ ҚОЛДАНУДЫҢ ТИІМДІЛІГІ

**Аңдатпа:**Бұл мақалада математика сабағында физикалық мазмұнды есептерді шешу барысында цифрлық технологияларды қолданудың тиімділігі қарастырылады. Қазіргі білім беру жүйесінде цифрлық құралдарды пайдалану оқу үдерісін жандандырып, оқушылардың пәнге деген қызығушылығын арттыруға мүмкіндік береді.

Зерттеудің мақсаты – математика пәнін оқытуда цифрлық технологияларды қолдану арқылы физикалық мазмұнды есептерді шешудің тиімді жолдарын анықтау. Жұмыста теориялық талдау, салыстыру және тәжірибелік бақылау әдістері қолданылды.

Нәтижесінде цифрлық технологияларды пайдалану оқушылардың есеп шығару. дағдыларын жетілдіретіні, күрделі тапсырмаларды көрнекі түрде түсінуге көмектесетіні және оқу мотивациясын арттыратыны анықталды.

**Түйін сөздер:** цифрлық технологиялар, математика, физикалық мазмұнды есептер, оқу үдерісі, білім беру.

Бүгінгі күні білім беру жүйесі қарқынды дамып, оқыту үдерісіне жаңа технологияларды енгізу алдыңғы қатарлы мәселелердің біріне айналып отыр. Ақпараттық құралдарды оқу процесінде ұтымды пайдалану білім сапасын көтеруге және оқушылардың пәнге деген қызығушылығын нығайтуға жол ашады. Мұны отандық ғалымдардың «АКТ құралдары оқушының танымдық белсенділігін арттырып, оқу материалын терең меңгеруіне бағытталған дидактикалық орта қалыптастырады» деген тұжырымы растайды [1].

Математика пәні – логикалық ойлау мен аналитикалық қабілетті шыңдайтын негізгі пәндердің бірі. Бұл пәнді оқыту барысында физикалық мазмұнды есептерді қолдану оқушылардың теориялық білімін практикамен ұштастыруға жағдай жасайды. Мұндай есептер нақты өмірлік жағдайларды модельдеуге мүмкіндік беріп, пәнаралық байланысты нығайта түседі. Профессор А.Е. Әбілқасымованың еңбектерінде «мектептегі математика курсындағы қолданбалы есептер оқушылардың математикалық модельдеу дағдыларын қалыптастырады» деп атап көрсетілген [2]. Осы тұста цифрлық технологиялар математиканы оқыту процесін көрнекі, түсінікті және интерактивті етуге

үлкен ықпал етуде. Графикалық құралдар, онлайн платформалар және симуляциялық бағдарламалар арқылы күрделі есептерді шешу жеңілдеп, балалардың оқуға деген ынтасы оянады. Осыған байланысты бұл зерттеудің мақсаты – математика сабағында физикалық мазмұнды есептерді шешуде технологиялық мүмкіндіктерді қолданудың пайдасын айқындау болып табылады.

Математика мен физика пәндерінің арасындағы тығыз байланыс — оқытудағы ең іргелі принциптердің бірі. Физика табиғат заңдылықтарын зерттесе, математика сол заңдылықтарды сипаттайтын логикалық құрылым мен абстрактілі модельдерді ұсынады. Мұны 8-сыныпқа арналған физика оқулығындағы құбылыстарды математикалық сипаттау әдістерінен көруге болады [3]. Сондықтан бұл екі пәнді бөліп қарау мүмкін емес; физикалық құбылысты түсіну үшін оның математикалық моделін құру, ал математикалық формуланың мәнін ұғу үшін оның физикалық мазмұнын сезіну қажет.

**Пәнаралық байланыстың негізгі бағыттары:**

- **Математикалық аппаратты қолдану:** Физикалық процестерді сипаттауда математикалық талдау әдістері (туынды, интеграл, векторлар, функциялар) шешуші рөл атқарады. Мысалы, қозғалыстың жылдамдығын анықтау — жолдың уақыт бойынша туындысы болса, өткен жолды табу — жылдамдықтан интеграл алу болып табылады. Бұл амалдар 8-сыныптың алгебра оқулығындағы функциялық тәуелділіктермен тікелей байланысты [4].
- **Модельдеу дағдылары:** Физикалық мазмұнды есептерді шешу кезінде оқушылар шынайы өмірдегі құбылысты математикалық тілге (теңдеулер мен теңсіздіктер жүйесіне) аударуды үйренеді. Бұл оқушылардың абстрактілі ойлау қабілетін дамытады. А.А. Жантесова бұл туралы «математикалық модельдеу – нақты физикалық үдерісті зерттеудің ең тиімді әдісі» деп жазады [5].
- **Қолданбалы маңыздылық:** Математика сабағында физикалық контексті қолдану "Бұл формула бізге не үшін керек?" деген сұраққа жауап береді. Сандық мәндер мен формулалар нақты табиғи үдерістермен (энергия, күш, қысым) байланысқанда, пәнге деген мотивация артады.

Заманауи білім беру кеңістігіндегі STEM (Science, Technology, Engineering, Math) бағыты дәл осы пәнаралық интеграцияға негізделген. Математика сабағында физикалық мазмұнды есептерді шешу оқушының функционалдық сауаттылығын арттырып, алған білімін өмірде қолдана алуына жол ашады. Уақыт талабына сай білім беру жүйесі қарқынды цифрландыру кезеңін бастан кешіруде. Ақпараттық технологиялардың дамуы оқыту процесінің мазмұны мен әдістеріне елеулі өзгерістер енгізді. Әсіресе жаратылыстану пәндерін, соның ішінде физиканы оқытуда цифрлық технологияларды қолданудың маңызы артып отыр. Физикалық мазмұнды есептерді шешу – оқушылардың теориялық білімін практикамен ұштастыратын негізгі құралдардың бірі. Алайда дәстүрлі әдістер кей жағдайда оқушылардың қызығушылығын толық оята алмайды немесе күрделі құбылыстарды терең түсінуге жеткіліксіз болуы мүмкін.

Осы ретте заманауи құралдар жаңа мүмкіндіктер ашады. Цифрлық ресурстар арқылы физикалық процестерді модельдеу, визуализациялау және интерактивті түрде талдау мүмкіндігі пайда болды. Бұл оқушыларға абстрактілі ұғымдарды нақты әрі түсінікті қабылдауға көмектеседі. М.С. Нұрмағанбетова атап өткендей, пәнаралық байланыстар білімнің жүйелілігін қамтамасыз етеді [6]. Сонымен қатар, әртүрлі білім беру платформалары мен бағдарламалар есептерді тиімді әрі жылдам шешуге,

нәтижелерді тексеруге және талдауға жағдай жасайды. Осыған байланысты физикалық мазмұнды есептерді шешуде технологиялардың тиімділігін зерттеу – өзекті мәселелердің бірі болып қала береді.

Білім беруді цифрландыру деңгейінің артуына байланысты арнайы ресурстар кеңінен қолданысқа енуде. Олар оқу процесін тиімді ұйымдастыруға, білім алушылардың қызығушылығын арттыруға және оқу материалын терең меңгеруге мүмкіндік береді. Цифрлық білім беру ресурстары бірнеше түрге бөлінеді:

- **Электрондық оқулықтар:** Дәстүрлі кітаптардың заманауи нұсқасы. Олар мәтінмен қатар суреттер, бейнелер, анимациялар және интерактивті тапсырмалар арқылы толықтырылады. Бұл материалды түсінуді жеңілдетеді.
- **Білім беру платформалары:** Онлайн платформалар оқу материалдарын жүйелі түрде ұсынуға мүмкіндік береді. Мысалы, Khan Academy, Coursera, BilimLand сияқты платформаларда бейнесабақтар, тесттер және практикалық тапсырмалар бар.
- **Виртуалды зертханалар:** Виртуалды зертханалар арқылы оқушылар тәжірибелерді қауіпсіз және қолжетімді түрде орындай алады. Мысалы, PhET Interactive Simulations бағдарламасы физикалық құбылыстарды модельдеуге мүмкіндік береді.
- **Бейнесабақтар мен мультимедиалық ресурстар:** Бейнесабақтар күрделі тақырыптарды визуалды түрде түсіндіруге көмектеседі. YouTube платформасында әртүрлі пәндер бойынша сапалы білім беру контенті көп.
- Онлайн тесттер мен бағалау жүйелері: Бұл ресурстар білім деңгейін тексеруге арналған. Автоматты түрде нәтижені шығарып, қателерді талдауға мүмкіндік береді. Мысалы, Google Forms, Quizizz.
- **Мобильді қосымшалар:** Смартфонға арналған білім беру қосымшалары кез келген уақытта оқуға мүмкіндік береді. Олар қысқа тапсырмалар, ойын элементтері арқылы оқытуды қызықты етеді.
- **Сандық кітапханалар:** Цифрлық кітапханалар ғылыми еңбектерге, оқулықтарға және мақалаларға қолжетімділікті қамтамасыз етеді. Бұл оқушылар мен студенттердің өздігінен білім алуына көмектеседі.

Математиканы оқытуда цифрлық технологияларды пайдалану маңызды орын алады. Әртүрлі бағдарламалар мен қосымшалар оқушылардың пәнге деген қызығушылығын арттырып, күрделі тақырыптарды жеңіл түсінуге көмектеседі. Математика сабағында жиі қолданылатын бағдарламалар:

- **Геометриялық бағдарламалар:** Мұндай бағдарламалар фигураларды құруға, оларды өзгертуге және зерттеуге мүмкіндік береді. Мысалы, GeoGebra – алгебра, геометрия және графиктерді біріктіретін өте тиімді құрал. Ол әсіресе функциялардың графиктерін салуда және геометриялық есептерді түсіндіруде пайдалы.
- **Компьютерлік алгебра жүйелері:** Бұл бағдарламалар күрделі есептеулерді автоматты түрде орындауға арналған. Мысалы, Wolfram Mathematica және Maple. Олар теңдеулерді шешу, туынды мен интеграл табу сияқты тапсырмаларды жеңілдетеді.
- **Онлайн есептеу құралдары:** Интернеттегі құралдар жылдам есеп шығаруға көмектеседі. Мысалы, Wolfram Alpha – математикалық есептердің шешімін қадамдап көрсететін сервис.
- **Тест және викторина платформалары:** Оқушылардың білімін тексеру үшін қолданылады. Мысалы, Quizizz және Kahoot!. Бұл платформалар сабақта ойын элементтерін енгізуге мүмкіндік береді.

- **Оқу платформалары:** Математика бойынша толық курстар мен тапсырмалар ұсынады. Мысалы, Khan Academy – теория мен практиканы қатар меңгеруге көмектеседі.
- **График салу құралдары:** Функцияларды визуализациялау үшін қолданылады.

Мысалы, Desmos – қарапайым әрі ыңғайлы онлайн график калькуляторы.

Жаһандану дәуірінде білім беру жүйесі технологиялардың қарқынды дамуымен тығыз байланысты өзгерістерді бастан кешіруде. Ақпараттық-коммуникациялық құралдарды оқу процесіне енгізу білім сапасын арттырудың маңызды факторларының біріне айналды. Физикалық мазмұнды есептерді шешу – оқушылардың теориялық білімін практикада қолдана білуін қалыптастыратын негізгі тәсілдердің бірі. Дегенмен, дәстүрлі оқыту әдістері кей жағдайда күрделі физикалық құбылыстарды толық әрі терең түсіндіруге жеткіліксіз болып жатады. Осыған байланысты цифрлық технологияларды қолдану оқыту процесін жаңаша ұйымдастыруға мүмкіндік береді.

Цифрлық құралдар физикалық процестерді модельдеу, визуализациялау және интерактивті түрде зерттеу арқылы оқушылардың пәнді меңгеру деңгейін арттырады. Сонымен қатар, олар есеп шығару барысында уақытты үнемдеуге, нәтижелерді дәл талдауға және оқушылардың танымдық белсенділігін күшейтуге ықпал етеді. Осы тұрғыда физикалық мазмұнды есептерді шешуде технологиялық шешімдердің тиімділігін анықтау және оларды оқу процесінде ұтымды қолдану маңызды міндеттердің бірі болып табылады.

Бұл технологияларды жүйелі қолдану оқушылардың білім сапасына, пәнге деген қызығушылығына және оқу белсенділігіне оң әсерін тигізеді. Тәжірибе барысында заманауи құралдарды пайдалану оқушылардың физикалық құбылыстарды терең түсінуіне мүмкіндік беретіні байқалады. Мысалы, модельдеу және визуализация арқылы күрделі процестерді көзбен көру олардың абстрактілі ойлауын нақтылауға көмектеседі. Нәтижесінде оқушылар есептің шартын жақсырақ түсініп, оны шешудің тиімді жолдарын таба алады.

Сонымен қатар, цифрлық платформаларды қолдану есеп шығару жылдамдығы мен дәлдігін арттырады. Автоматты тексеру жүйелері арқылы оқушылар өз қателерін бірден анықтап, түзетуге мүмкіндік алады. Бұл өз кезегінде кері байланысты жеделдетіп, білімді бекіту процесін тиімді етеді. Тәжірибелік жұмыстар көрсеткендей, технологиялар оқушылардың оқу мотивациясын арттырады. Интерактивті тапсырмалар, графиктер және анимациялар сабақтың қызықты өтуіне ықпал етеді. Оқушылар белсенді қатысып, өз бетінше ізденуге талпынады. Сондай-ақ, мұғалім үшін де оң нәтижелер байқалады.

Сабақты жоспарлау, материалды түсіндіру және оқушылардың білімін бағалау процестері жеңілдейді.

Түйіндей келе, оқу процесінде цифрлық технологияларды қолдану нақты тәжірибелік нәтижелер арқылы өзінің жоғары тиімділігін көрсетеді. Ол білім сапасын арттырып қана қоймай, оқушылардың танымдық және шығармашылық қабілеттерін дамытуға ықпал етеді. Цифрлық ресурстар оқу материалын көрнекі және түсінікті түрде ұсынуға жағдай жасайды. Анимациялар, графиктер және модельдер арқылы күрделі физикалық құбылыстарды оңай қабылдауға болады. Бұл оқушылардың тақырыпты терең түсінуіне және оны ұзақ уақыт есте сақтауына ықпал етеді.

Сонымен қатар, цифрлық технологиялар жеке оқыту мүмкіндігін кеңейтеді. Әр оқушы өз деңгейіне сәйкес тапсырмаларды орындап, өз қарқынымен жұмыс істей алады. Бұл білімдегі олқылықтарды дер кезінде анықтап, оларды түзетуге көмектеседі. Оқушылардың білім сапасына әсер ететін тағы бір маңызды фактор – жедел кері байланыс. Онлайн тесттер мен автоматтандырылған жүйелер арқылы оқушы өз нәтижесін бірден көріп, қателерін талдай алады. Бұл оқу процесін тиімдірек етеді және білімді бекітуге мүмкіндік береді. Сонымен бірге, заманауи құралдар оқушылардың пәнге деген қызығушылығын арттырады.

Жалпы алғанда, цифрлық технологияларды тиімді қолдану оқушылардың білім сапасын арттырудың маңызды құралы болып табылады. Ол білімді меңгеруді жеңілдетіп қана қоймай, оқушылардың өздігінен білім алу дағдыларын қалыптастырады. Зерттеу нәтижелері көрсеткендей, бұл технологиялар физикалық құбылыстарды көрнекі түрде түсіндіруге, күрделі есептерді модельдеу арқылы жеңілдетуге және оқушылардың оқу материалын терең меңгеруіне мүмкіндік береді. Оқу процесінде цифрлық ресурстарды тиімді қолдану оқушылардың тек теориялық білімін ғана емес, сонымен қатар практикалық және логикалық ойлау қабілеттерін де жетілдіреді. Қорытындылай келе, физикалық мазмұнды есептерді шешуде цифрлық технологияларды қолдану – заман талабына сай білім берудің тиімді құралы.

**Пайдаланылған әдебиеттер тізімі:**

1. Мұхамбетжанова С. Т. Педагогтардың ақпараттық-коммуникациялық технологияларды қолдану бойынша біліктілігін арттыру әдістемесі. – Алматы: Өрлеу, 2015. – 220 б.
2. Әбілқасымова А. Е. Математиканы оқытудың теориясы мен әдістемесі: Оқулық. – Алматы: Мектеп, 2018. – 264 б.
3. Башарұлы Р., Қазақбаева Д., Тоқбергенова У. Физика: Жалпы білім беретін мектептің 8-сыныбына арналған оқулық. – Алматы: Мектеп, 2018. – 240 б.
4. Шыныбеков Ә. Н. Алгебра: Жалпы білім беретін мектептің 8-сыныбына арналған оқулық. – Алматы: Атамұра, 2018. – 208 б.
5. Жантесова А. А. Математикалық модельдеу және қолданбалы есептер: Оқу құралы. – Алматы: Қазақ университеті, 2019. – 210 б.
6. Нұрмағанбетова М. С. Пәнаралық байланыстар негізінде оқушылардың функционалдық сауаттылығын қалыптастыру. – Астана: ҰБА, 2021. – 180 б.

**ЖАРАТЫЛЫСТАНУ ҒЫЛЫМДАРЫ – ЕСТЕСТВЕННЫЕ НАУКИ –NATURAL SCIENCES**

**УДК 553.98**

**Суннат Али Ғаниұлы**

Магистрант
Казахский национальный исследовательский
технический университет имени К. И. Сатпаева
(г. Алматы, Казахстан)

# ГЕОХИМИЧЕСКИЕ КРИТЕРИИ НЕФТЕГАЗОНОСНОСТИ И МОДЕЛИ МИГРАЦИИ УГЛЕВОДОРОДОВ В НАДСОЛЕВЫЕ КОМПЛЕКСЫ ВОСТОКА ПРИКАСПИЙСКОЙ ВПАДИНЫ

**Аннотация:** В статье представлен аналитический обзор геохимических условий формирования и эволюции углеводородных систем в надсолевом (верхнепермско-мезозойском) комплексе восточного борта Прикаспийской впадины. Главной проблемой региональной нефтегазовой геологии является генезис нефтей в условиях активного проявления соляного диапиризма. Проведен сравнительный анализ генерационного потенциала подсолевых палеозойских и надсолевых мезозойских (триасовых и юрских) отложений. Рассмотрены механизмы межкомплексной миграции углеводородов сквозь «соляные окна» и латерального перетока флюидов. На основе данных о физико-химических свойствах нефтей, распределении молекулярных биомаркеров (стеранов, терпанов, изопреноидов) и изотопном составе углерода обоснована полигенная (смешанная) природа большинства надсолевых залежей. Показано критическое влияние процессов бактериальной биодеградации на искажение первоначального геохимического облика нефтей в ловушках на малых глубинах. Сделан вывод о необходимости смещения поисковых работ в глубокие инверсионные межкупольные мульды, где термодинамические условия способствуют сохранению качественных углеводородов, сгенерированных in situ.

**Ключевые слова:** Прикаспийская впадина, геохимия нефти, биомаркеры, нефтематеринская порода, углеводородная система, соляной диапиризм, миграция флюидов, биодеградация, кероген.

**Введение:** Успешный прогноз нефтегазоносности любой территории базируется на комплексном понимании углеводородной системы, в которой наличие структурной или стратиграфической ловушки является лишь одним из необходимых, но далеко не единственным элементом. Как было показано в предыдущих исследованиях, интенсивный соляной диапиризм на восточном борту Прикаспийской мегасинеклизы сформировал огромное разнообразие потенциальных емкостей для аккумуляции углеводородов в надсолевом мезозойском этаже. Однако наличие идеальной неантиклинальной ловушки и надежной глинистой покрышки не гарантирует выявления рентабельной залежи. Ключевой проблемой, определяющей высокие геологические риски при поисково-разведочном бурении в регионе, остается сложная и во многом

дискуссионная геохимия органического вещества, а также неопределенность путей миграции углеводородных флюидов.

Восток Прикаспийской впадины представляет собой уникальный природный полигон для изучения процессов генерации, перераспределения и деградации углеводородов. Исторически сложилось так, что главные нефтегазоматеринские толщи бассейна (в первую очередь, обогащенные органикой депрессионные фации девона и карбона) приурочены к глубокозалегающим подсолевым комплексам. В то же время надсолевой этаж, отделенный от палеозойского фундамента мощнейшим региональным флюидоупором — эвапоритами кунгурского яруса, содержит многочисленные скопления нефти и газа в терригенных коллекторах нижнего-среднего триаса, средней юры и нижнего мела. Главная геологическая загадка, которая уже несколько десятилетий разделяет исследовательское сообщество, заключается в происхождении этих надсолевых нефтей.

Являются ли мезозойские залежи результатом масштабной вертикальной миграции палеозойских флюидов, сумевших прорваться сквозь ослабленные тектонические зоны и «соляные окна» в эвапоритовой толще? Или же терригенные толщи раннего мезозоя, накапливавшиеся в межкупольных компенсационных мульдах, обладают достаточным собственным (in situ) генерационным потенциалом, чтобы сформировать месторождения без подпитки снизу? Разрешение этого фундаментального противоречия критически важно не только для академической науки, но и для сугубо практических задач: от того, какая модель углеводородной системы является доминирующей, напрямую зависит стратегия заложения поисковых скважин, оценка объемов ожидаемых запасов и перспектив слабоизученных межкупольных зон.

Целью данного обзора является систематизация накопленных геолого-геохимических данных, характеризующих условия генерации и скопления углеводородов в надсолевом комплексе востока Прикаспия. В статье обобщены современные результаты пиролитических исследований потенциальных нефтематеринских пород, хромато-масс-спектрометрического анализа молекулярных биомаркеров и изотопного состава нефтей. Это позволяет по-новому взглянуть на эволюцию углеводородных систем бассейна и выявить наиболее надежные геохимические критерии нефтегазоносности в условиях активной солянокупольной тектоники.

**Потенциальные нефтематеринские толщи и оценка их генерационного потенциала**

Фундаментом для построения достоверной модели углеводородной системы является идентификация нефтегазоматеринских свит — тех самых осадочных толщ, органическое вещество которых послужило первоисточником для формирования залежей. Оценка генерационного потенциала базируется на анализе геохимических параметров пород: общего содержания органического углерода (TOC), типа керогена и степени его термической зрелости (стадии катагенеза), определяемой чаще всего по отражательной способности витринита и данным пиролиза по методу Rock-Eval. В контексте восточного борта Прикаспийской впадины исследователи традиционно анализируют два принципиально разных уровня генерации: глубокий палеозойский (подсолевой) и более молодой мезозойский (надсолевой).

Подсолевой палеозойский комплекс рассматривается абсолютным большинством геологов как главный, региональный «двигатель» нефтегазообразования во всей Прикаспийской мегасинеклизе. Основным источником углеводородов здесь выступают мощные депрессионные фации верхнего девона и нижнего-среднего карбона. Это преимущественно темноцветные битуминозные сланцы, аргиллиты и глинистые карбонаты, накапливавшиеся в условиях глубоководного, некомпенсированного осадками морского бассейна с сероводородным заражением придонных вод. Такие бескислородные условия обеспечили великолепную сохранность органического вещества преимущественно сапропелевого типа (кероген I и II типов). Содержание TOC в этих толщах нередко превышает 3–5%, а в отдельных прослоях может достигать 10% и более, что классифицирует их как породы с уникально высоким генерационным потенциалом. С точки зрения термической эволюции, палеозойские толщи погружены на значительные глубины и давно вошли в «главную зону нефтеобразования» (ГЗН), а в наиболее погруженных блоках — достигли стадии жесткого апокатагенеза, генерируя сухой газ и конденсат. Сомнений в том, что палеозой произвел колоссальные объемы углеводородов, в научном сообществе нет.

Совершенно иная, гораздо более сложная и неоднозначная картина наблюдается при оценке собственного (in situ) генерационного потенциала надсолевого мезозойского чехла. На протяжении многих десятилетий господствовала точка зрения, согласно которой триасовые и юрские отложения востока Прикаспия геохимически инертны. Считалось, что они либо бедны органикой, либо не достигли достаточных температур для запуска процессов массовой генерации нефти из-за относительно неглубокого залегания. Однако масштабные современные геохимические исследования кернового материала, извлеченного из глубоких межкупольных мульд, заставили серьезно пересмотреть эту парадигму.

Главными кандидатами на роль собственных нефтематеринских толщ в надсолевом этаже сегодня считаются глинистые пачки оленекского и анизийского ярусов (нижний-средний триас), а также углистые аргиллиты средней юры. Условия их осадконакопления кардинально отличались от палеозойских: это были мелководно-морские, лагунные, а зачастую и континентальные (озерно-аллювиальные) обстановки. Вследствие этого органическое вещество здесь имеет преимущественно смешанный, гумусово-сапропелевый состав (кероген II-III и III типов) с высокой долей терригенного (растительного) материала. Данные пиролитических анализов Rock-Eval показывают, что содержание общего органического углерода (TOC) в мезозойских глинах обычно варьируется в пределах от 0.5% до 2.5%, редко достигая 4% в тонких углистых прослоях. Это позволяет классифицировать их генерационный потенциал как удовлетворительный или хороший, но при этом они в большей степени склонны к генерации газоконденсата и легкой нефти, нежели тяжелых смолистых флюидов.

Ключевым аргументом в геохимических дискуссиях остается степень термической зрелости мезозойской органики. На сводах и флангах соляных куполов, где юрско-триасовые породы приподняты галокинезом на глубины 1–2 километра, органическое вещество действительно является незрелым (стадия протокатагенеза, градация ПК). Однако в центральных частях глубоких компенсационных мульд восточного борта основание триасового комплекса погружается на глубины 4–5 километров и более. Результаты бассейнового моделирования и замеры отражательной способности

витринита доказывают, что в этих локальных межкупольных депоцентрах породы нижнего и среднего триаса уверенно перешагнули порог температурного оптимума и вошли в градацию мезокатагенеза (МК1-МК2), то есть в верхнюю часть «главной зоны нефтеобразования».

Таким образом, современные данные свидетельствуют о том, что надсолевой комплекс востока Прикаспия не является геохимически «стерильным». Он обладает собственным генерационным потенциалом, который, однако, строго локализован в пространстве — очаги возможного образования нефти приурочены исключительно к наиболее прогнутым частям межкупольных мульд. Наличие этих двух принципиально разных «кухонь погоды» (мощной региональной палеозойской и локальной мезозойской) создает основу для сложнейшей картины распределения углеводородов, расшифровать которую невозможно без понимания путей миграции флюидов в условиях соляной тектоники.

**Пути миграции флюидов в условиях солянокупольной тектоники**

Наличие доказанных очагов генерации углеводородов — как мощных региональных в подсолевом палеозое, так и локальных в мезозойских мульдах — ставит перед исследователями следующий фундаментальный вопрос: каким образом нефть и газ преодолели значительные расстояния и заполнили ловушки в надсолевом чехле? В классических платформенных бассейнах миграция флюидов представляет собой относительно предсказуемый процесс движения от погруженных зон к гипсометрически приподнятым участкам. Однако на востоке Прикаспийской впадины этот процесс был тотально искажен и осложнен галокинезом, который создал уникальную, динамично меняющуюся в геологическом времени систему флюидопроводников и экранов.

Главным парадоксом региональной углеводородной системы является двойственная роль кунгурской соляной толщи. С одной стороны, эвапориты представляют собой идеальный, абсолютно флюидоупорный экран с нулевой проницаемостью, который надежно запечатывает гигантские скопления углеводородов в подсолевом комплексе (такие как Тенгиз или Карачаганак). В ненарушенном состоянии кунгурская соль делает невозможным переток флюидов снизу вверх. С другой стороны, именно экстремальная пластичность соли и ее активное перераспределение в процессе роста диапиров привели к нарушению сплошности этого экрана.

В центральных, наиболее прогнутых частях межкупольных компенсационных мульд восточного борта материнский пласт кунгурской соли был практически полностью выдавлен в растущие по периферии штоки. В результате тектонического истощения соляной залежи сформировались так называемые «соляные окна» — обширные зоны зияния, где надсолевой мезозойско-кайнозойский чехол лег непосредственно на подсолевые палеозойские породы или отделен от них лишь маломощными линзами сульфатно-терригенных пород. Именно эти «окна» стали главными порталами для масштабной межкомплексной вертикальной миграции. Находящиеся под аномально высоким пластовым давлением палеозойские углеводороды, сгенерированные в глубоких очагах, устремлялись в эти зоны ослабления. Процесс перетока многократно усиливался густой сетью глубинных субвертикальных разломов, которые пронизывали фундамент мульд и работали как своеобразные тектонические клапаны. В периоды тектонических активизаций эти разломы приоткрывались, обеспечивая импульсную, струйную инъекцию нефти и газа из палеозоя в базальные горизонты триаса.

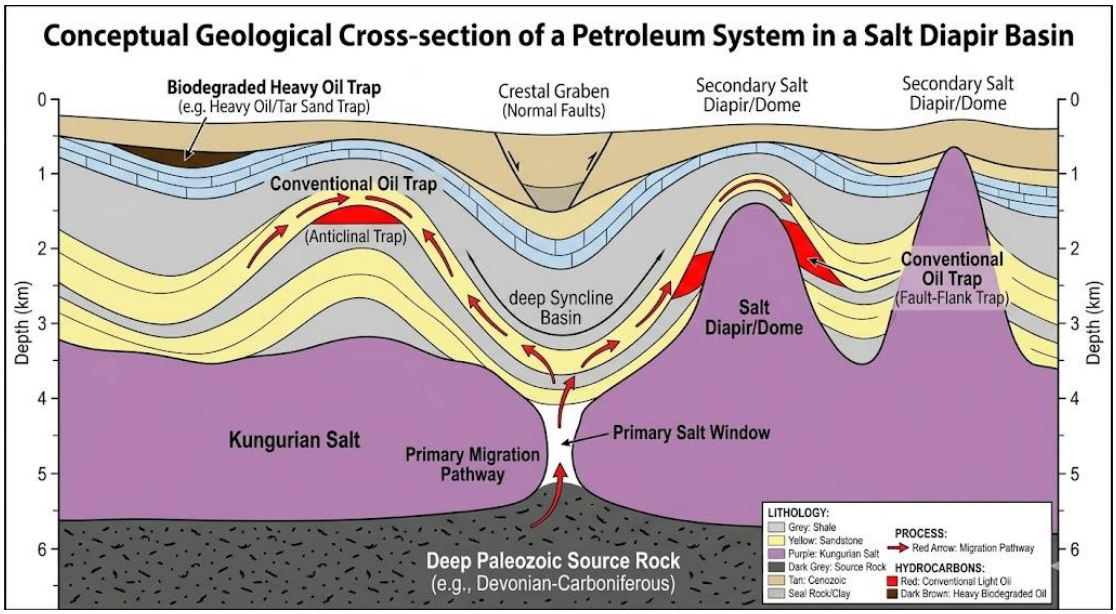



Рисунок 1. Концептуальная модель углеводородной системы: пути миграции флюидов через «соляные окна» и формирование залежей в надсолевом комплексе

Попав в надсолевой комплекс через «соляные окна» (или будучи сгенерированными in situ в самых глубоких частях тех же мульд), углеводородные флюиды начинали второй этап своего пути — латеральную (боковую) миграцию. Роль главных транспортных артерий на этом этапе взяли на себя мощные пласты высокопористых и проницаемых песчаников нижнего и среднего триаса, а также средней юры. Движение флюидов подчинялось законам гидродинамики и плавучести: более легкие нефть и газ стремились подняться по восстанию пластов от глубоких центров межкупольных депрессий к их краям.

Именно здесь пути миграции пересекались с растущими соляными куполами. Песчаные горизонты-проводники, выходя из мульды, круто изгибались вверх на склонах диапиров. Углеводороды двигались по этим наклонным пластам до тех пор, пока не встречали на своем пути непреодолимое препятствие. Таким препятствием становилось либо само тело протыкающего соляного штока (формируя приконтактную ловушку), либо нависающий соляной карниз (загоняя нефть в подкарнизную ловушку), либо литологическое выклинивание коллектора на склоне купола. В надсводовых частях куполов миграция носила еще более сложный характер: флюиды просачивались по сети малоамплитудных сбросов в грабенах обрушения, заполняя тектонически экранированные блоки.

Критически важным аспектом этой модели является ее динамичность. Галокинез не останавливался ни на минуту, а значит, архитектура путей миграции постоянно менялась. Разломы, которые еще вчера служили проводниками, при изменении вектора напряжений могли сомкнуться, превратившись в непроницаемые экраны. Углы наклона пластов на флангах куполов продолжали расти, что нередко приводило к изменению положения структурных замков и переливу нефти из уже сформированных ловушек выше по разрезу. Этот процесс вторичной миграции и переформирования залежей на востоке Прикаспия является скорее правилом, чем исключением. Часто флюиды, не найдя надежной покрышки, прорывались сквозь трещиноватые юрские и меловые глины к дневной поверхности, что объясняет наличие в регионе многочисленных

поверхностных нефтепроявлений и скоплений сильно окисленных битумов. Таким образом, путь нефти от материнской породы до ловушки в условиях соляного диапиризма представляет собой сложнейшую многофазную эстафету, где малейшее нарушение синхронности тектонических процессов вело к безвозвратной потере углеводородов.

**Геохимическая характеристика нефтей и молекулярные биомаркеры**

Понимание архитектуры путей миграции неразрывно связано с детальным изучением самого флюида. Физико-химические свойства нефтей надсолевого комплекса восточного борта Прикаспийской впадины — в частности, классических месторождений Эмбинской нефтегазоносной области — отличаются колоссальным разнообразием. В пределах одних и тех же стратиграфических горизонтов можно встретить как сверхлегкие, подвижные, малосернистые нефти и газоконденсаты, так и тяжелые, высоковязкие, смолистые разности, по консистенции напоминающие мальты. Такое резкое контрастное распределение свойств невозможно объяснить только условиями первичной генерации; оно является прямым следствием сложной истории миграции и интенсивных процессов вторичного изменения залежей в термодинамических условиях малых глубин.

Единственным надежным инструментом для расшифровки генетической природы таких разнообразных флюидов является анализ молекулярных биомаркеров — своеобразных «геохимических отпечатков пальцев», унаследованных нефтью от исходного органического вещества. Современные методы газовой хроматографии и хромато-масс-спектрометрии (ГХ-МС) позволяют на молекулярном уровне сравнивать надсолевые и подсолевые нефти. Одним из базовых индикаторов выступает соотношение изопреноидных алканов — пристана и фитана (Pr/Ph). Для глубинных палеозойских нефтей региона, сгенерированных в морских восстановительных обстановках карбонатных платформ, характерны низкие значения этого отношения (часто Pr/Ph < 1). В то же время в ряде надсолевых триасовых и юрских залежей фиксируются значения Pr/Ph, превышающие 1.5–2.0. Такой геохимический облик свидетельствует о существенной доле терригенного (растительного) материала в исходном керогене и субокислительных условиях седиментации, что является веским аргументом в пользу генерации этих нефтей in situ в мезозойских континентальных или прибрежно-морских фациях.

Еще более детальную информацию предоставляет распределение полициклических биомаркеров — стеранов и терпанов (гопанов). Спектр стеранов (углеводородов ряда C27-C29) жестко контролируется типом исходной биомассы. Высокая концентрация холестана (C27) типична для морского фитопланктона (палеозойский источник), тогда как преобладание стигмастана (C29) указывает на влияние высшей наземной растительности, характерной для мезозойских отложений. Изучение этих маркеров в надсолевых нефтях востока Прикаспия часто дает смешанную картину. В некоторых резервуарах четко прослеживается палеозойский «морской» след, что неопровержимо доказывает факт вертикального перетока по разломам. В других — фиксируется уверенный мезозойский профиль. Важнейшим дополнением к хроматографии служит анализ изотопного состава углерода (δ13C). Нефти, сингенетичные мезозойским толщам, как правило, изотопно более «тяжелые» по

сравнению с палеозойскими аналогами, что позволяет дифференцировать их даже при сильном сходстве физических свойств.

Однако применение биомаркерного анализа в надсолевом этаже сталкивается с серьезным естественным барьером — процессами биодеградации. Большинство мезозойских неантиклинальных ловушек, о которых мы говорили ранее, располагается на небольших глубинах (от 500 до 2000 метров), где температуры пласта редко превышают 60–70 °C. Это идеальные условия для жизнедеятельности аэробных и анаэробных бактерий. Попадая в такую ловушку, нефть подвергается массированной бактериальной атаке: микроорганизмы в первую очередь «съедают» легкие нормальные алканы, в результате чего флюид стремительно тяжелеет, обогащаясь смолисто-асфальтеновыми компонентами и нафтено-ароматическими углеводородами.

Биодеградация не только ухудшает рентабельность добычи нефти, но и стирает ее первоначальный геохимический код. На поздних стадиях разрушения бактерии начинают уничтожать даже устойчивые изопреноиды и стераны, превращая нефть в бесструктурный битум. В зонах активного роста соляных куполов, где глинистые покрышки постоянно микротрещиноваты, залежи подвергаются дополнительному разрушению за счет вымывания пластовыми инфильтрационными водами (water washing). Именно повсеместное наложение этих разрушительных вторичных процессов на первичный генетический профиль флюидов породило десятилетние научные споры о том, откуда же на самом деле пришла нефть в мезозойские ловушки Прикаспия.

**Дискуссионные модели углеводородных систем**

Сложное переплетение путей миграции, контрастность физико-химических свойств флюидов и повсеместное наложение процессов биодеградации превратили вопрос о генезисе надсолевых нефтей в одну из самых острых проблем региональной геологии. Исторически сложилось так, что именно на материале месторождений Эмбинской нефтегазоносной области и смежных структур восточного борта Прикаспия сформировались две полярные, непримиримые концепции углеводородных систем, дискуссия между сторонниками которых продолжается до сих пор.

Первая концепция — модель глубинной вертикальной миграции (палеозойского источника). Ее апологеты опираются на колоссальный дисбаланс масс: объемы углеводородов, аккумулированные в надсолевом мезозойском этаже, по их расчетам, значительно превышают собственный генерационный потенциал юрско-триасовых отложений. В рамках этой модели мезозойский чехол рассматривается исключительно как транзитная зона и гигантский резервуар для нефти, сгенерированной в подсолевых девон-каменноугольных толщах. Главным аргументом здесь выступает структурный фактор — пространственная приуроченность крупнейших надсолевых месторождений к глубоким межкупольным мульдам, где зафиксированы «соляные окна» и сквозные разрывные нарушения. Обнаружение в надсолевых нефтях морских биомаркеров (холестаны) и изотопно-легкого углерода, характерного для палеозоя, считается неопровержимым доказательством правомерности этой теории.

Вторая концепция — модель автохтонной генерации (in situ, мезозойского источника). Сторонники этой теории доказывают, что миграция сквозь толщу кунгурской соли, даже в зонах ее максимального тектонического утонения, физически крайне затруднена. Они акцентируют внимание на результатах современного геохимического моделирования, которое подтверждает: в осевых частях глубоких компенсационных

мульд нижнетриасовые и среднеюрские глинистые пачки погружались на глубины свыше 4–5 километров, уверенно достигая температурного оптимума «главной зоны нефтеобразования». Наличие в нефтях терригенных стеранов (C29), высокие значения отношения пристан/фитан и изотопно-тяжелый состав углерода служат прямым свидетельством того, что эти флюиды родились здесь же, в мезозое, из органики растительного или смешанного типа, и мигрировали в ловушки на короткие расстояния по латерали.

В последние годы, благодаря накоплению огромного массива хромато-масс-спектрометрических данных, в научном сообществе начинает доминировать третья, компромиссная парадигма — полигенная модель смешения флюидов. Согласно этой концепции, углеводородная система востока Прикаспия формировалась в несколько пульсационных этапов. На ранних стадиях, по мере прогибания мульд, мезозойские материнские породы генерировали собственные, автохтонные флюиды, которые первыми заполняли формирующиеся приконтактные ловушки на склонах диапиров. Значительно позже, в периоды глобальных тектонических перестроек (например, в неогене), когда сеть разломов обновлялась, происходил мощный прорыв палеозойских газов и легких нефтей сквозь «соляные окна». Эти глубинные флюиды вторгались в уже существовавшие мезозойские залежи, растворяли окисленную бактериями старую нефть и кардинально меняли ее геохимический облик. Именно такое смешение разновозрастных углеводородов в разных пропорциях идеально объясняет весь тот хаос физико-химических свойств и биомаркерных аномалий, который мы наблюдаем на месторождениях восточного борта.

**Заключение.** Обобщение современных геохимических и структурно-тектонических данных убедительно доказывает, что надсолевой мегакомплекс восточного борта Прикаспийской мегасинеклизы — это не просто транзитная зона, а сложная, открытая и высокодинамичная углеводородная система. Ее историческая эволюция и современный облик всецело продиктованы процессами галокинеза. Пластическое течение кунгурской соли сыграло здесь ключевую и весьма противоречивую роль: оно не только сформировало широкую палитру сложнопостроенных неантиклинальных ловушек, но и создало уникальную архитектуру путей миграции, периодически открывая «соляные окна» и формируя густую сеть тектонических экранов и проводников.

Анализ биомаркеров и данных пиролиза позволяет поставить точку в многолетних дискуссиях об источниках углеводородов. Сегодня можно с уверенностью говорить о том, что ресурсный потенциал региона опирается на два независимых очага генерации. Наряду с масштабными вертикальными перетоками флюидов из подсолевого палеозоя, в глубокопогруженных межкупольных мульдах активно функционировала собственная, весьма продуктивная мезозойская система. Слияние потоков из этих двух источников объясняет полигенную, смешанную природу подавляющего большинства надсолевых нефтей. Ситуация дополнительно осложняется тем, что первоначальный генетический облик этих флюидов оказался сильно искажен интенсивными процессами бактериальной биодеградации и вымывания, которые активно протекали в резервуарах на малых глубинах.

Выявленные геохимические закономерности диктуют необходимость кардинального пересмотра поисковых стратегий в регионе. Для минимизации

геологических рисков фокус геологоразведочных работ должен смещаться с традиционных, структурно-выраженных прикупольных зон, где нефти чаще всего окислены, в сторону глубоких инверсионных мульд и скрытых подкарнизных ловушек. Именно там, на глубинах более 2.5–3 километров, термодинамические условия естественным образом останавливают разрушительное воздействие микроорганизмов, обеспечивая сохранность легкой, качественной нефти и газоконденсата. Успешное выявление и освоение таких объектов потребует от геологов глубокого междисциплинарного синтеза — тесной интеграции полноазимутальной 3D-сейсморазведки глубинной миграции с современными методами 4D-бассейнового геохимического моделирования.

**Список литературы:**

1. Твердова Р.А., Ботнева Т.А. Геохимия нефтей и газов Прикаспийской впадины. – М.: Недра, 1985. – 190 с.

2. Дальян И.Б., Посадская А.С. Геохимия и условия формирования залежей нефти на востоке Прикаспийской впадины // Геология нефти и газа. – 1998. – № 10. – С. 22–31.

3. Peters K.E., Walters C.C., Moldowan J.M. The Biomarker Guide: Biomarkers and Isotopes in Petroleum Systems and Earth History. – Cambridge: Cambridge University Press, 2005. – 1155 p.

4. Abilkhassymov B., Volozh Y., et al. Hydrocarbon systems and structural evolution of the eastern Pre-Caspian basin // Marine and Petroleum Geology. – 2020. – Vol. 112. – P. 104085.

5. Махмутов Н. Геохимические критерии прогноза нефтегазоносности надсолевых отложений Кенкияк-Жанажольской зоны // Нефть и газ Казахстана. – 2017. – № 4. – С. 34–42.

6. Magoon L.B., Dow W.G. The petroleum system – from source to trap // AAPG Memoir 60. – 1994. – P. 3–24.

**УДК 553.98**

**Суннат Али Ғаниұлы**

Магистрант
Казахский национальный исследовательский
технический университет имени К. И. Сатпаева
(г. Алматы, Казахстан)

# ВЛИЯНИЕ МОРФОЛОГИИ СОЛЯНЫХ КУПОЛОВ НА ФОРМИРОВАНИЕ И СОХРАННОСТЬ УГЛЕВОДОРОДНЫХ ЛОВУШЕК В НАДСОЛЕВЫХ КОМПЛЕКСАХ ВОСТОКА ПРИКАСПИЙСКОЙ ВПАДИНЫ

**Аннотация:** В статье представлен комплексный обзор проблем формирования и сохранения углеводородных ловушек в надсолевых (верхнепермско-мезозойских) отложениях восточного борта Прикаспийской впадины. Актуальность работы обусловлена необходимостью освоения мезозойского этажа, обладающего высокими коллекторскими свойствами, на фоне возрастающих капитальных затрат при разведке глубокозалегающего подсолевого палеозоя. Показано, что фундаментальным фактором, контролирующим архитектуру углеводородных резервуаров в регионе, выступает интенсивный галокинез кунгурской соли. Систематизированы основные морфологические типы соляных тел и приуроченные к ним сложноэкранированные неантиклинальные ловушки: сводовые (в грабенах обрушения), приконтактные (фланговые), скрытые подкарнизные и инверсионные структуры межкупольных мульд. Рассмотрена эволюция методов геофизических исследований: продемонстрирована неэффективность традиционной 2D-сейсморазведки в зонах соляного диапиризма из-за эффектов скоростных аномалий и обоснована критическая роль 3D-сейсморазведки с применением глубинной миграции (PSDM) для достоверного картирования подкарнизных зон. Выделены ключевые дискуссионные вопросы нефтегазовой геологии региона, включая двойственную роль разрывных нарушений и проблему целостности региональных покрышек в условиях конседиментационного роста диапиров. Сделан вывод о необходимости комплексирования структурной геологии, высокоточной геофизики и 4D-бассейнового моделирования для снижения рисков поискового бурения.

**Ключевые слова:** Прикаспийская впадина, галокинез, соляной купол, неантиклинальная ловушка, надсолевой мегакомплекс, соляной карниз, 3D-сейсморазведка, глубинная миграция (PSDM), тектонический экран.

**Введение.** Прикаспийская мегасинеклиза по праву считается одним из старейших, наиболее масштабных и геологически сложных нефтегазоносных бассейнов Евразийского континента. Исторически сложилось так, что после открытия серии месторождений-гигантов, таких как Тенгиз, Кашаган и Карачаганак, основной вектор внимания научно-исследовательских институтов и добывающих компаний закономерно сместился на глубокозалегающие подсолевые комплексы палеозойского возраста. Безусловно, именно карбонатные платформы и рифогенные постройки девона и карбона содержат львиную долю запасов региона. Однако освоение этих горизонтов сопряжено с колоссальными технологическими вызовами: глубины бурения зачастую превышают

отметку в 4.5–5 километров, пласты характеризуются аномально высокими давлениями, а флюиды содержат экстремально высокие концентрации сероводорода и углекислоты. Все это делает поисково-разведочные работы в подсолевом этаже крайне капиталоемкими и сопряженными с высокими геологическими и экологическими рисками.

На фоне этих трудностей надсолевой верхнепермско-мезозойский мегакомплекс, который в конце прошлого века отошел на второй план, сегодня вновь приобретает высокую актуальность. Особый практический интерес представляет восточный борт впадины — территория, охватывающая зоны сочленения с Предуральским краевым прогибом и смежные структурные ступени. Надсолевые залежи углеводородов в этом районе обладают рядом неоспоримых преимуществ. В первую очередь, это относительно комфортные глубины залегания, редко превышающие 2–3 километра, и отсутствие агрессивных компонентов в составе нефтей. Кроме того, терригенные отложения нижнего и среднего триаса, средней юры и нижнего мела выступают в роли превосходных коллекторов. Благодаря высокой пористости, которая в неглубоко погруженных песчаниках нередко достигает 20–25%, и проницаемости, измеряемой сотнями миллидарси, добыча здесь характеризуется высокими дебитами. Совокупность этих факторов делает разведку и эксплуатацию надсолевых залежей экономически высокорентабельными даже в том случае, если объемы запасов в отдельных ловушках относительно невелики.

Однако кажущаяся простота освоения малых глубин нивелируется экстремально сложной тектонической архитектурой региона. Фундаментальным процессом, который полностью диктует структурный план надсолевого этажа, литофациальную изменчивость пород и пути миграции углеводородов, является галокинез. Гигантские массы эвапоритов кунгурского яруса нижней перми, выступающие региональным флюидоупором для глубоких залежей, для надсолевого комплекса стали главным дестабилизирующим фактором. Обладая высокой пластичностью и аномально низкой плотностью по сравнению с перекрывающими породами, кунгурская соль на протяжении сотен миллионов лет находилась в непрерывном движении. Соляные диапиры прорывали формирующийся осадочный чехол, создавая хаотичную картину из густой сети сбросов, компенсационных прогибов и локальных зон стратиграфического срезания.

Следствием этого многовекового тектонического процесса стало практически полное отсутствие в регионе классических пологих антиклинальных складок, которые относительно легко диагностируются традиционными методами геофизики. В надсолевом комплексе восточного Прикаспия доминируют сложнопостроенные, пространственно изменчивые неантиклинальные ловушки: тектонически экранированные блоки в грабенах обрушения, зоны литологического выклинивания на склонах протыкающих штоков и скрытые скопления под нависающими соляными карнизами. Поиск таких объектов требует ювелирной точности и принципиально иных подходов к интерпретации данных. В связи с этим, настоящая обзорная статья ставит своей целью систематизировать разрозненные современные представления о механизмах формирования ловушек в условиях активного соляного диапиризма. В работе обобщен накопленный опыт изучения морфологии соляных тел и их влияния на архитектуру углеводородных резервуаров, а также критически проанализированы проблемы и

ограничения сейсмического картирования сложных неантиклинальных объектов на востоке Прикаспийской мегасинеклизы.

**Этапы галокинеза и морфологическая эволюция соляных тел**

Специфика формирования структурного плана надсолевого мегакомплекса на востоке Прикаспийской впадины во многом уникальна и принципиально отличается от центральных, более погруженных районов бассейна. Если в центральной депрессии рост соляных куполов был обусловлен преимущественно классическим гравитационным галокинезом — то есть всплыванием легких эвапоритов сквозь более плотные терригенные толщи из-за разницы литостатических давлений, — то на восточном борту к этому процессу добавился мощнейший тектонический фактор. Близость зоны сочленения с Уральской складчатой системой привела к тому, что на гравитационную нестабильность наложилось интенсивное региональное латеральное сжатие, связанное с финальными фазами герцинского орогенеза. Именно этот синергетический эффект плотностной инверсии и тектонического стресса предопределил высочайшую агрессивность соляного диапиризма в регионе и крайнюю асимметрию формирующихся структур.

Процесс перераспределения гигантских масс кунгурской соли не был одномоментным; он носил ярко выраженный пульсационный характер и растянулся на сотни миллионов лет, напрямую управляя условиями осадконакопления. В эволюции соляных структур востока Прикаспия исследователи традиционно выделяют несколько крупных макроэтапов, каждый из которых оставил свой неповторимый след в архитектуре мезозойских резервуаров.

Начальный, позднепермско-триасовый этап характеризовался зарождением пологих соляных подушек и валов. Под давлением первых порций накапливающихся осадков соль начала пластично перетекать из зон максимальной нагрузки в зоны разгрузки. Важнейшим следствием этого оттока эвапоритов стало проседание пород кровли и формирование глубоких межкупольных компенсационных мульд. В условиях засушливого климата раннего мезозоя эти мульды превратились в гигантские депоцентры, куда речные системы сносили огромные объемы обломочного материала с разрушающихся Уральских гор. Так формировались мощные, местами достигающие полутора километров, толщи песчано-глинистых отложений триаса, которые сегодня рассматриваются как главные резервуары надсолевого этажа.

Юрско-раннемеловой этап стал периодом максимальной активности галокинеза. По мере того как толщина перекрывающих осадков росла, соляные подушки эволюционировали в протыкающие диапиры. Соляные ядра буквально разрывали сформировавшиеся триасовые горизонты, устремляясь к поверхности. Важно понимать, что этот процесс происходил синхронно с осадконакоплением (так называемый конседиментационный рост). Пока соль пробивала себе путь наверх, на ее склонах продолжали отлагаться юрские и меловые осадки. В результате вблизи растущих диапиров формировались зоны резкого стратиграфического несогласия: пласты выклинивались, меняли свою мощность и литологический состав, что создавало идеальные условия для возникновения литологически экранированных ловушек. Наконец, позднемеловой-кайнозойский этап стал завершающей стадией, когда вертикальный импульс соли иссяк, либо она достигла палеоповерхности. Началось латеральное растекание эвапоритов с образованием сложнейших грибовидных структур.

Степень зрелости галокинеза и локальные вариации тектонических напряжений привели к формированию огромного многообразия форм соляных тел. Современные данные объемной сейсморазведки позволяют детально классифицировать эти морфотипы, поскольку именно форма соли определяет тип приуроченной к ней углеводородной ловушки. Наиболее простыми по строению являются соляные подушки глубокого заложения. Они характеризуются плавными очертаниями и отсутствием сквозного протыкания юрско-мелового чехла. Свод надсолевых отложений над такими подушками остается относительно пологим и слабо нарушенным разломами, что благоприятствует сохранению крупных классических залежей.

Абсолютно иная картина наблюдается в зонах развития протыкающих соляных штоков, которые доминируют на востоке впадины. Типичными примерами таких структур являются диапиры Ащисай или Каратюбе. Они представляют собой крутопадающие соляные столбы с углами наклона склонов, достигающими 70–90 градусов. Штоки полностью разрывают триасово-юрские горизонты, а в их надсводовых частях из-за колоссального растяжения пород формируются сложные системы грабенов обрушения.

Особое место в морфологическом ряду занимают соляные карнизы и грибовидные купола, характерные, например, для Кенкияк-Жанажольской зоны. Их формирование связано со способностью соли на поздних этапах развития внедряться по ослабленным зонам в горизонтальном направлении, перекрывая собой более молодые отложения. Такие нависающие соляные «козырьки» играют роль идеальных, абсолютно непроницаемых покрышек для мигрирующих углеводородов. Наконец, неотъемлемой частью галокинетического ландшафта являются межкупольные мульды — области, откуда кунгурская соль была практически полностью выдавлена в растущие соседние диапиры. По мере полного исчерпания запасов материнской соли в центрах мульд происходит оседание вышележащих пластов, что с течением геологического времени приводит к инверсии рельефа. Изначальные депрессии превращаются в так называемые «черепашьи структуры» — обширные псевдоантиклинальные складки в межкупольном пространстве. Эти структуры залегают на значительных глубинах, но из-за отсутствия интенсивной разломной тектоники представляют собой весьма перспективные объекты для поиска крупных скоплений нефти.

**Классификация и особенности формирования ловушек в зонах соляного диапиризма**

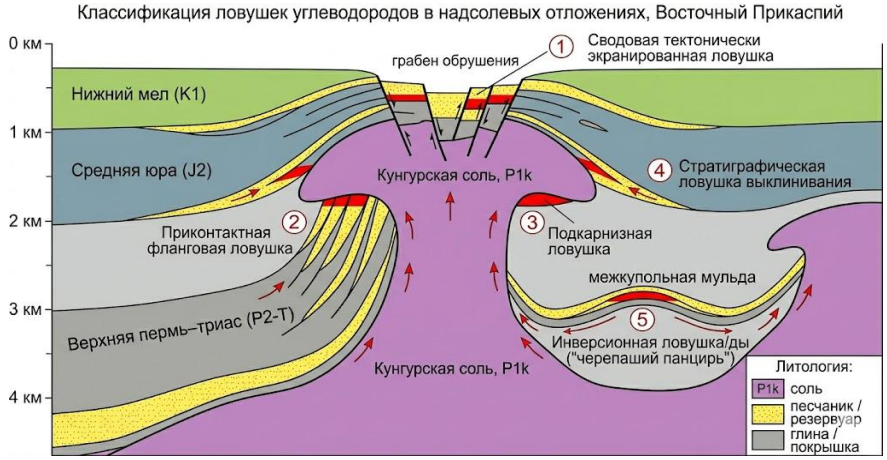



Рисунок 1. Принципиальная схема типов ловушек углеводородов в надсолевых отложениях восточного Прикаспия

Неразрывная связь между формой соляного тела и архитектурой вмещающих пород обуславливает формирование в надсолевом этаже широчайшего спектра углеводородных ловушек. Для восточного борта Прикаспийской впадины характерно резкое, подавляющее преобладание неантиклинальных, тектонически и литолого-стратиграфически экранированных скоплений. Классические пологие своды здесь являются редкостью, уступая место сложным структурным формам, каждая из которых требует специфического подхода к разведке.

Самым ранним и исторически наиболее изученным типом объектов в регионе являются сводовые тектонически экранированные ловушки. Их образование напрямую связано с процессами растяжения, которые испытывают породы кровельного чехла при вертикальном напоре растущего соляного диапира или крупной подушки. По мере того как соляное ядро пробивает себе путь наверх, перекрывающие его юрско-меловые отложения деформируются, изгибаются и в конечном итоге разрываются с образованием густой сети сбросов. В результате на сводах куполов формируются сложные грабены обрушения, или так называемые кепроки. Нефть в таких условиях скапливается в приподнятых тектонических блоках. Механизм удержания углеводородов здесь полностью зависит от герметичности разлома: экраном выступает либо сама плоскость сброса, заполненная перетертым глинистым материалом, либо непроницаемые породы, которые тектоническими подвижками были приведены в прямой латеральный контакт с песчаным коллектором. Классическими эталонами подобных сложнопостроенных залежей выступают старейшие месторождения региона — Шубаркудук и Жаксымай. Главным геологическим риском при поиске таких объектов остается нарушение их герметичности при неотектонических активизациях, что нередко приводит к дегазации резервуара по приоткрывшимся разломам и формированию скоплений окисленной, тяжелой нефти.

Гораздо более продуктивными, но в то же время более сложными для освоения считаются приконтактные, или фланговые, ловушки. Пространственно они тяготеют к крутым, порой субвертикальным склонам протыкающих соляных штоков. Формирование этих залежей неразрывно связано с конседиментационной стадией галокинеза, когда активный рост купола происходил одновременно с накоплением осадков. В таких условиях продуктивные песчаные пласты нижнего и среднего триаса, а также средней юры, круто воздымаясь по направлению к диапиру, буквально упираются в непроницаемое тело соли. В данном случае эвапориты выступают в роли идеального бокового флюидоупора, надежно запечатывающего углеводороды. В других случаях на склонах активно растущих куполов происходило стратиграфическое срезание пластов или их литологическое выклинивание из-за смены условий осадконакопления. Ярчайшим представителем этого типа резервуаров является надсолевой комплекс месторождения Кенкияк, где основные нефтяные скопления приурочены именно к зонам резкого выклинивания юрских и триасовых коллекторов на крыльях соляного ядра.

Совершенно особый интерес с точки зрения нереализованного ресурсного потенциала представляют подкарнизные ловушки. Их генезис обусловлен поздними стадиями развития галокинеза, когда исчерпавший энергию вертикального подъема соляной массив начинает пластично растекаться в латеральном направлении, используя ослабленные зоны в мезозойском осадочном чехле. Внедрение таких нависающих соляных козырьков создает уникальные условия для аккумуляции нефти. Углеводороды,

мигрирующие вверх по восстанию проницаемых триасовых или верхнепермских пластов, оказываются надежно «запертыми» под мощной, абсолютно непроницаемой соляной покрышкой карниза. Несмотря на то, что такие ловушки могут содержать колоссальные объемы качественной легкой нефти, их целенаправленный поиск долгое время оставался практически невозможным. Соляной карниз работает как гигантский акустический экран, рассеивающий и поглощающий сейсмическую энергию, в результате чего под ним формируется зона глухой «сейсмической тени», надежно скрывающая перспективные горизонты от классических методов геофизики.

Наконец, важнейшим, но пока наименее изученным элементом углеводородной системы востока Прикаспия являются ловушки межкупольных мульд и связанные с ними инверсионные структуры. В то время как на сводах и флангах куполов породы подвергались жесточайшим тектоническим деформациям, в центральных частях межкупольного пространства формировались относительно спокойные условия. По мере радикального выдавливания материнской кунгурской соли к растущим по периферии диапирам, перекрывающие мульду мощные пермо-триасовые толщи постепенно оседали. Парадокс этого процесса заключается в том, что центральные части депрессий, куда изначально сносился максимальный объем осадков, со временем из-за неравномерного оттока соли оказываются гипсометрически выше периферийных зон. Так формируются инверсионные псевдоантиклинали, получившие в геологической литературе образное название «черепашьих панцирей». В отличие от прикупольных зон, разломная тектоника здесь проявлена слабо, что гарантирует превосходную сохранность залежей и целостность глинистых покрышек. Главной сложностью при их разведке становятся значительные глубины залегания, зачастую превышающие 3–4 километра, и высокая фациальная изменчивость терригенных пород, требующая филигранного прогнозирования коллекторских свойств в центре палеоречных систем.

**Проблемы сейсмического картирования сложных ловушек и роль современных технологий**

Высокая плотность доказанных запасов углеводородов в надсолевых отложениях востока Прикаспийской впадины на протяжении десятилетий контрастировала с парадоксально низкой успешностью поисково-разведочного бурения на неантиклинальные объекты. Геологи прекрасно понимали, что фланги куполов и межкупольные пространства таят в себе колоссальный потенциал, однако пробуренные скважины раз за разом оказывались сухими или вскрывали водоносные горизонты. Это несоответствие теории и практики было обусловлено экстремально сложными сейсмогеологическими условиями региона, которые долгое время выступали непреодолимым барьером для достоверного картирования скрытых ловушек. Традиционные методы геофизики просто не позволяли геологам «увидеть» то, что происходит в непосредственной близости от соляного тела.

Исторический массив данных, полученных методами 2D-сейсморазведки в период 1970–1990-х годов, сыграл важнейшую роль в понимании общей региональной тектоники и выявлении морфологии крупных соляных массивов. Однако для детального изучения приконтактных и подкарнизных зон двумерная сейсмика оказалась критически малоэффективной. Одним из главных ее ограничений стала невозможность корректного отображения крутых углов падения пластов. Стандартные алгоритмы временной миграции после суммирования (Post-Stack Time Migration), применявшиеся в те годы,

математически не справлялись с субвертикальными границами, углы наклона которых на склонах соляных штоков часто превышают 60–70 градусов. В результате на сейсмических разрезах границы соляного ядра выглядели размытыми, хаотичными, а зоны стратиграфического прилегания продуктивных пластов к соли просто терялись в фоновом шуме.

Еще более серьезной проблемой, искажавшей понимание внутренней архитектуры ловушек, стали так называемые эффекты скоростных аномалий. Физика этого явления заключается в колоссальной разнице плотностей и акустических свойств сред. Скорость прохождения упругой сейсмической волны в плотной кунгурской соли достигает 4500 метров в секунду, тогда как в перекрывающих и прилегающих к ней терригенных породах мезозоя она варьварюется в пределах 2500–3500 метров в секунду. Проходя сквозь соляные выступы, волна ускоряется, из-за чего на временных сейсмических разрезах горизонты, залегающие под солью, искусственно «подтягиваются» вверх. Этот феномен, известный в геофизике как эффект ложного поднятия (pull-up effect), приводил к тому, что геологи картировали несуществующие антиклинальные структуры под телом куполов или неверно оценивали гипсометрию межкупольных мульд, закладывая скважины в заведомо пустые блоки.

Абсолютно слепой зоной для исследователей оставались и подкарнизные ловушки. Массивные, нависающие соляные козырьки работали как гигантские линзы, которые хаотично рассеивали сейсмическую энергию, не позволяя ей проникнуть вглубь и отразиться от перспективных триасовых или верхнепермских горизонтов. Под карнизом формировалась зона потери корреляции — «сейсмическая тень», где невозможно было выделить ни тектонические нарушения, ни границы пластов.

Настоящий прорыв в изучении неантиклинальных ловушек востока Прикаспия произошел уже в новом тысячелетии и был связан с двумя революционными изменениями: переходом к плотным, полноазимутальным системам наблюдений 3D-сейсморазведки и массовым внедрением ресурсоемких алгоритмов миграции до суммирования в глубинной области (Pre-Stack Depth Migration — PSDM). Именно PSDM-преобразования стали тем ключом, который позволил нивелировать влияние соляной толщи. В отличие от временной миграции, алгоритмы глубинной миграции опираются на построение сложнейших трехмерных глубинно-скоростных моделей. Эти модели учитывают резкие латеральные скачки скоростей на границах раздела «соль — терригенная порода» и позволяют вернуть сейсмические отражения на их истинные пространственные позиции.

Практические результаты применения этих технологий кардинально изменили подходы к геологоразведке в регионе. Благодаря устранению pull-up эффектов, удалось скорректировать структурные карты межкупольных мульд и выявить истинные инверсионные структуры. Высокое пространственное разрешение 3D-данных дало возможность детально трассировать малоамплитудные сбросы в сводовых кепроках, что критически важно для оценки герметичности тектонически экранированных ловушек. Но главным достижением стало освещение подкарнизных зон: современные методы впервые позволили уверенно картировать зоны стратиграфического выклинивания песчаных коллекторов под нависающими козырьками соли, переведя подкарнизные ловушки из разряда теоретических гипотез в категорию реальных, высокоперспективных объектов для бурения.

**Дискуссионные вопросы и нерешенные проблемы**

Несмотря на впечатляющий прогресс в сейсмическом картировании и значительное повышение качества визуализации надсолевого комплекса восточного борта Прикаспийской впадины, геология региона по-прежнему таит в себе множество загадок. Целый ряд фундаментальных вопросов, касающихся генерации, путей миграции и условий сохранения углеводородных скоплений, остается предметом острых научных дискуссий, разделяя исследовательское сообщество на приверженцев полярных концепций.

Одной из самых горячо обсуждаемых тем является двойственная роль разрывных нарушений в формировании нефтяных залежей. Сбросовая тектоника, густой сетью осложняющая своды и фланги соляных диапиров, ведет себя крайне непредсказуемо. С одной стороны, существует устоявшаяся концепция, рассматривающая глубокие разломы как главные транспортные артерии. Сторонники этой теории, опираясь на геохимическое сходство некоторых надсолевых и подсолевых нефтей, утверждают, что углеводороды мигрируют из богатых материнских толщ палеозоя сквозь так называемые «соляные окна» — зоны полного оттока эвапоритов в межкупольных мульдах. Попадая в систему надсолевых разломов, флюиды устремляются вверх, заполняя ловушки. В этой парадигме активная разломная тектоника рассматривается как абсолютное благо и необходимое условие нефтегазоносности.

Однако альтернативная точка зрения предлагает совершенно иной взгляд на проблему. Ряд современных исследований, базирующихся на данных пиролиза органического вещества, доказывает наличие в триасовых и среднеюрских отложениях региона собственных, хотя и менее масштабных, очагов генерации углеводородов. В рамках этой концепции (in situ генерации) разломы рассматриваются не как проводники, а преимущественно как тектонические экраны, способные удерживать нефть. Ключевой нерешенной проблемой здесь остается прогнозирование сдвиговых напряжений в плоскостях разломов (параметр Shale Gouge Ratio). Исследователи до сих пор не выработали единого критерия: при каком соотношении раздробленного песчаного и глинистого материала разлом на востоке Прикаспия остается герметичным экраном, а при каком — превращается в проницаемый канал, ведущий к разрушению залежи.

Вторая глобальная проблема, не имеющая на сегодняшний день однозначного математического решения, связана с оценкой сохранности залежей и целостности региональных покрышек (seal integrity). В условиях непрерывного, пульсационного роста соляных куполов глинистые толщи нижнего триаса или средней юры, выступающие главными флюидоупорами, подвергались постоянным деформациям. Они растягивались, утончались и покрывались сетью микротрещин. Именно проблема деградации покрышек над растущими куполами объясняет тот факт, что многие идеально выраженные структурные ловушки в сводовых частях при бурении оказываются сухими или содержат лишь следы тяжелой, биодеградированной нефти. Глина просто не выдержала тектонического напряжения, и легкие флюиды ушли к дневной поверхности. Интеграция данных геомеханики для точного расчета критического напряжения, при котором покрышка теряет свою целостность, является одним из главных вызовов для будущих исследований.

Наконец, серьезнейшим фактором геологического риска остается фазовая рассинхронизация во времени — проблема несовпадения моментов формирования

ловушки (Structural Trap Timing) и главного импульса генерации и миграции углеводородов (Charge Timing). Галокинез — процесс растянутый во времени, и ловушки формировались неравномерно. На восточном борту впадины описаны парадоксальные случаи, когда крупные приконтактные резервуары окончательно оформились и закрылись глинистыми экранами только в позднемеловое время. Однако, согласно бассейновому моделированию, пик вытеснения нефти из материнских пород на этих участках завершился еще в ранней юре. Нефть, мигрировавшая по пластам, просто не нашла на своем пути готовой емкости и рассеялась в транзитных зонах. Создание точных, откалиброванных по времени 4D-моделей углеводородных систем, которые смогли бы пошагово реконструировать кинематику соли и пути миграции флюидов в геологическом прошлом, представляет собой сложнейшую, но жизненно необходимую задачу для повышения успешности поискового бурения.

**Заключение.** Резюмируя современное состояние изученности надсолевого мегакомплекса восточного борта Прикаспийской впадины, можно с уверенностью утверждать, что эпоха легких геологических открытий в этом регионе завершилась. Классические сводовые поднятия давно разведаны, однако остаточный ресурсный потенциал территории остается весьма внушительным. Ключ к его освоению лежит в глубоком понимании процессов галокинеза, который тотально контролирует всю эволюцию углеводородных систем бассейна.

Тектоническое нагнетание кунгурской соли привело к формированию парагенетического ряда неантиклинальных ловушек, требующих принципиально новых подходов к разведке. Наибольшим нереализованным потенциалом сегодня обладают зоны стратиграфического выклинивания на флангах соляных штоков, скрытые резервуары под нависающими соляными карнизами и слабонарушенные разломами инверсионные поднятия в центрах межкупольных мульд.

Достоверное выявление и оконтуривание этих сложноэкранированных объектов невозможно в рамках традиционных сейсмических методов. Только комплексное применение полноазимутальной 3D-сейсморазведки и передовых алгоритмов миграции до суммирования в глубинной области (PSDM) позволяет снять искажающее влияние соляных диапиров, преодолеть «сейсмическую тень» карнизов и восстановить истинную геометрию пластов.

Вектор будущих исследований в регионе должен быть направлен на междисциплинарный синтез. Для успешного прогнозирования нефтегазоносности необходимо объединить инструменты структурной геологии, высокоточной геофизики, геомеханики и 4D-бассейнового моделирования. Переход от интуитивного поиска структурно-выраженных поднятий к целенаправленному, научно обоснованному картированию стратиграфических и подкарнизных ловушек способен обеспечить рентабельное развитие ресурсной базы восточного Прикаспия на многие десятилетия вперед.

**Список использованной литературы:**

1. Волож Ю.А., Антипов М.П., Брунет М.Ф. и др. Строение и история развития Прикаспийского осадочного бассейна // Российский журнал наук о Земле. – 2003. – Т. 5. – № 4. – С. 1–32. (Идеально для обоснования тектоники и галокинеза во Введении).

2. Куандыков Б.М., Акчулаков У.А., Куандыков А.Б. Нефтегазоносность надсолевых отложений Прикаспийской впадины // Нефть и газ Казахстана. – 2011. – № 2. – С. 15–24. (Классическая статья по потенциалу надсолевого этажа восточного борта).

3. Дальян И.Б. Геология и нефтегазоносность восточной окраины Прикаспийской синеклизы. – Алматы: Ғылым, 2003. – 264 с. (Фундаментальная монография по восточному борту, Шубаркудуку и Кенкияку).

4. Jackson M.P.A., Hudec M.R. Salt Tectonics: Principles and Practice. – Cambridge: Cambridge University Press, 2017. – 498 p. (Мировой бестселлер по соляной тектонике; ссылка на него покажет высокий уровень вашего обзора при описании морфологии куполов).

5. Barde J.-P. et al. Seismic imaging of salt structures in the Pre-Caspian Basin: Challenges and solutions using PSDM // The Leading Edge. – 2012. – Vol. 31. – No. 8. – P. 916–924. (Современная статья, обосновывающая переход от PSTM к PSDM).

6. Сейс Р., Уайлд П. 3D-сейсморазведка и глубинная миграция при изучении сложноэкранированных неантиклинальных ловушек // Технологии сейсморазведки. – 2018. – № 3. – С. 45–55. (Для раздела про преодоление "сейсмической тени" и картирование карнизов).

7. Abilkhassymov B., Volozh Y., et al. Hydrocarbon systems and structural evolution of the eastern Pre-Caspian basin // Marine and Petroleum Geology. – 2020. – Vol. 112. – P. 104085. (Свежая публикация для раздела дискуссий о времени формирования ловушек и миграции УВ).

8. Карабалин У.С., Исмагилов Д.П. и др. Галокинез и неантиклинальные ловушки углеводородов Прикаспийской впадины // Геология нефти и газа. – 2015. – № 5. – С. 2–11. (Отличный источник для классификации ловушек из нашего 3-го раздела).

**ӘОЖ 630.43:528.8**

**Орынбай Гүлназ Бекетқызы,**

**Талапты Нұрзат Ержанатұлы**

2 курс студенттері
**Ғылыми жетекші:** Сарыбаев Едил Саутович
PhD доцент
картография және геоинформатика кафедрасы
Әл-Фараби атындағы Қазақ Ұлттық университеті
(г. Алматы, Казахстан)

# АБАЙ ОБЛЫСЫНДАҒЫ ОРМАН ӨРТТЕРІНІҢ КЕҢІСТІКТІК ДИНАМИКАСЫН ҚАШЫҚТЫҚТАН ЗОНДТАУ ӘДІСТЕРІМЕН ЗЕРТТЕУ ЖӘНЕ БАҒАЛАУ

**Аңдатпа:** Бұл мақалада 2023 жылғы маусымда Қазақстан Республикасының Абай облысында орын алып, «Семей орманы» мемлекеттік орман табиғи резерватының аумағын шарпыған табиғи өрттер соңғы онжылдықтардағы аймақтың ең ірі экологиялық апаттарының біріне айналды. Орман экожүйелерінің зақымдану ауқымын бағалау зардап шеккен аймақтарды жедел және дәл картаға түсіру үшін Жерді қашықтықтан зондтаудың (ЖҚЗ) заманауи әдістерін енгізуді талап етеді. Sentinel-2 және Landsat 8/9 спутниктік түсірілімдерін пайдалана отырып, орман өрттері салдарының кеңістіктік талдауы ұсынылған. Зерттеу спектрлік индекстерді есептеуге негізделген: өртке дейінгі биомассаның жай-күйін бағалауға арналған қалыпқа келтірілген айырмашылық вегетациялық индексі (NDVI) және зақымдану дәрежесін анықтауға арналған қалыпқа келтірілген күйік айырмашылық индексі (dNBR). Google Earth Engine (GEE) бұлтты платформасында бұлттылықты сүзу мен кескіндердің уақытша серияларын синтездеу процесін автоматтандыруға мүмкіндік берді. Зерттеу барысында күйген жерлердің таралу карталары жасалып, жану деңгейі бойынша (төменнен жоғарыға дейін) аймақтарды жіктеу жүзеге асырылды. Сандық талдау көрсеткендей, ленталық қарағайлы ормандардың едәуір бөлігі жоғары қарқынды өрт әсеріне ұшырап, маңызды учаскелерде ағаш жамылғысының толық деградациясына әкелген. Өртенген аумақтардың ауданы бойынша алынған деректер ресми есептермен сәйкес келеді, сонымен қатар dNBR индексін пайдалану визуалды дешифрлеу кезінде тіркелмеген жасырын зақымдану ошақтарын анықтауға мүмкіндік берді. Зерттеу нәтижелері мен ұсынылған картаға түсіру әдістемесін Төтенше жағдайлар қызметі мен орман шаруашылығы мекемелері Абай облысындағы орман қорын қалпына келтіруді мониторингілеу және орман техникалық іс-шараларын жоспарлау үшін қолдана алады.

**Түйінді сөздер:** Абай облысы, Семей орманы, табиғи өрттер, ЖҚЗ, Sentinel-2, dNBR, кеңістіктік талдау, Google Earth Engine.

**Кіріспе.** Табиғи өрттер орман экожүйелерінің динамикасына және жаһандық көміртегі айналымына әсер ететін ең деструктивті факторлардың бірі болып табылады [1]. Жаһандық климаттың өзгеруі және экстремалды құрғақшылық кезеңдерінің жиілеуі

жағдайында Орталық Азияның аридті және семиаридті аймақтарындағы орман өрттерінің жиілігі мен қарқындылығы айтарлықтай артты. Ормандылығы шамамен 5%-ды құрайтын Қазақстан Республикасы үшін Ертіс өңірінің реликті ленталық қарағайлы ормандары сияқты бірегей алқаптарды сақтау басым мемлекеттік міндет болып табылады [2].

2023 жылғы маусымда Абай облысындағы «Семей орманы» мемлекеттік орман табиғи резерватының (МОТР) аумағында орын алған ауқымды өрт адам шығыны мен өрт шалған аумақтың көлемі бойынша аймақ тарихындағы ең ірі апат болды [3]. Рельефтің ерекшеліктері, ауаның жоғары температурасы және екпінді жел өрттің жоғарғы деңгейде таралуына ықпал етіп, өртті сөндіру мен жерүсті мониторингін қиындатты.

Дәстүрлі жерүсті тексеру әдістері үлкен уақыт пен адами ресурстарды қажет етеді. Осыған байланысты Жерді қашықтықтан зондтау (ЖҚЗ) әдістері мен географиялық ақпараттық жүйелер (ГАЖ) технологиялары апат салдарларын жедел бағалаудың таптырмас құралына айналуда [4]. Landsat және Sentinel-2 спутниктік деректері өсімдіктердің жай-күйіне ретроспективті және ағымдағы талдау жүргізуге мүмкіндік береді.

NBR (Normalized Burn Ratio) және оның туындысы dNBR сияқты қалыпқа келтірілген индекстерді қолдану халықаралық ғылыми қауымдастықта күйген жерлерді картаға түсірудің ең тиімді тәсілі ретінде танылған [5]. Алайда Қазақстанның ленталық ормандары үшін бұл индекстердің шекті мәндерін құмды топырақтағы қылқан жапырақты екпелердің ерекшеліктерін ескере отырып бейімдеу қажет.

Жұмыстың мақсаты - Абай облысындағы табиғи өрттердің салдарын кеңістіктік талдау және мультиспектрлік спутниктік мәліметтерді пайдалана отырып, өртенген аумақтардың шекарасын дәл анықтау және орман қорының зақымдану дәрежесін бағалау.

**2. Зерттеу нысаны**

Зерттеудің негізгі нысаны - Қазақстан Республикасының солтүстік-шығыс бөлігінде, Абай облысының аумағында орналасқан «Семей орманы» мемлекеттік орман табиғи резерваты (МОТР) болып табылады. Резерват 2003 жылы бірегей ленталық қарағайлы ормандарды сақтау және қалпына келтіру мақсатында құрылған (2022 жылдан бастап әкімшілік тұрғыдан жаңадан құрылған Абай облысына тиесілі) [3].

Зерттеу аумағы Батыс Сібір жазығының оңтүстік шеті мен Ертіс маңы жазығын қамтиды. Геоморфологиялық тұрғыдан бұл аймақ Ертіс ойпатының кең террасалы жазығы болып табылады. Ленталық қарағайлы ормандар (боры) мұз дәуірінен кейінгі кезеңнен сақталған реликті экожүйелер болып табылады және құмды жоталардың бойымен солтүстік-батыстан оңтүстік-шығысқа қарай созылып жатқан бірнеше ірі жолақтардан (Құлынды, Жарма және т.б.) тұрады [6].

Топырақ-климаттық жағдайлары:

- Топырақ жамылғысы: Аймақтың топырақ құрылымы өте ерекше. Негізгі бөлігін терең қабатты эолдық құмдарда қалыптасқан шымды-әлсіз күлгін (дерново-слабоподзолистые) және қарашірігі аз құмды топырақтар құрайды [6]. Бұл топырақтардың ылғал ұстау қабілеті төмен, бұл өсімдік жамылғысының тез құрғауына және өрт қаупінің артуына тікелей әсер етеді [2].

• Климаты: Зерттеу ауданының климаты шұғыл континентті және аса құрғақ. Жазғы кезеңде ауа температурасының күрт көтерілуі (35-40°C дейін), төмен салыстырмалы ылғалдылық (20%-дан аз) және тұрақсыз жел режимі байқалады [3], [4].

**1-кесте. Өрт кезіндегі зерттеу ауданының климаттық көрсеткіштері (маусым 2023 ж.)**

| **Параметр** | **Мәні** | **Көзі** |
|---|---|---|
| Макс. ауа температурасы | +35°C... +38°C | Қазгидромет |
| Желдің орташа жылдамдығы | 15–20 м/с (екпіні 25 м/с дейін) | Қазгидромет |
| Салыстырмалы ылғалдылық | < 20% | ЖҚЗ мәліметтері |

Бұл факторлардың жиынтығы Нестеров шкаласы бойынша өрт қауіптілігінің 5-ші (төтенше) класына сәйкес келеді [7].

«Семей орманы» резерватының жалпы ауданы 662 мың гектардан асады [3]. Бұл массивтер аридті климаттық аймақта орналасқандықтан, аймақтың экологиялық тепе-теңдігін сақтауда, топырақты эрозиядан қорғауда және көміртегін сіңіруде стратегиялық рөл атқарады [6]. Алайда, қылқан жапырақты ағаштардың басымдылығы (*Pinus sylvestris*), антропогендік жүктеме және климаттық экстремумдар бұл аймақты Қазақстандағы ең жоғары өрт қаупі бар аймақтардың қатарына (Нестеров шкаласы бойынша V класс) жатқызады [2], [7].

3. **Зерттеу деректері мен әдістері**

3.1. Қашықтықтан зондтау дереккөздері

Зерттеу жұмысында Абай облысындағы өрт салдарын кешенді бағалау үшін мультиспектрлік спутниктік мәліметтер мен геокеңістіктік деректердің келесі түрлері пайдаланылды:

1. Sentinel-2 (MSI): Зерттеудің негізгі ақпарат көзі ретінде Еуропалық ғарыш агенттігінің (ESA) Sentinel-2 спутниктік кескіндері пайдаланылды. Деректер өртке дейінгі (мамыр-маусым 2023 ж.) және өрттен кейінгі (шілде 2023 ж.) кезеңдерді қамтиды. Sentinel-2 мультиспектрлік сенсоры (MSI) өсімдік жамылғысы мен күйген жерлерді талдауға қажетті жақын инфрақызыл (NIR) және қысқа толқынды инфрақызыл (SWIR) каналдарында жоғары кеңістіктік ажыратымдылықты (10-20 метр) қамтамасыз етеді [4], [10].

2. NASA FIRMS (VIIRS/MODIS): Өрттің белсенді ошақтары (термонүктелер) туралы мәліметтер өрттің таралу динамикасын верификациялау және өрт шекараларын нақтылау үшін қолданылды. VIIRS (375 м) және MODIS (1 км) сенсорларының деректері өрттің хронологиясын қалпына келтіруге және өрттің ең қарқынды фазаларын анықтауға мүмкіндік берді [8].

3. SRTM (Shuttle Radar Topography Mission): 1 арксекундтық (шамамен 30 метр) ажыратымдылықтағы цифрлық рельеф моделі (DEM) жергілікті жердің морфометрикалық сипаттамаларын талдау үшін пайдаланылды. Бұл деректер негізінде беткейлердің экспозициясы мен еңістігі есептеліп, олардың жану қарқындылығына әсері зерттелді [4].

3.2. Бағдарламалық құралдар және деректерді өңдеу

Деректерді өңдеу мен талдау процесі екі негізгі кезеңде, ГАЖ платформаларында жүзеге асырылды:

- Google Earth Engine (GEE): Спутниктік мәліметтердің үлкен көлемін бұлттық есептеулер арқылы пакеттік өңдеу (batch processing) үшін қолданылды. Платформада бұлттылықты автоматты сүзу (QA60 mask), спектрлік индекстерді есептеу және уақытша серияларды (image composites) синтездеу жұмыстары жүргізілді [10].
- ArcGIS Pro / ArcMap (ESRI): GEE-ден алынған растрлық деректерді өңдеудің соңғы кезеңі және картографиялық дизайн үшін пайдаланылды. Мұнда кеңістіктік беттестіру (Overlay analysis), өртенген аумақтарды аудандастыру (Zonal Statistics), статистикалық гистограммалар құру және қорытынды макеттерді рәсімдеу орындалды.

3.3. Спектрлік индекстерді есептеу және жіктеу әдістемесі

Өрт салдарын сапалық және сандық бағалау мақсатында келесі спектрлік индекстер есептелді:

1. NBR (Normalized Burn Ratio): Жану коэффициентін анықтау үшін жақын инфрақызыл (NIR) және қысқа толқынды инфрақызыл (SWIR2) каналдары пайдаланылды:

$$NBR = \{NIR - SWIR2\}\backslash\{NIR + SWIR2\}$$

2. dNBR (Difference Normalized Burn Ratio): Өрттің зақымдау дәрежесін (Burn Severity) анықтаудың негізгі көрсеткіші ретінде өртке дейінгі және өрттен кейінгі NBR мәндерінің айырмашылығы есептелді:

$$dNBR = NBR\{prefire\} - NBR\{postfire\}$$

Алынған нәтижелер USGS (АҚШ Геологиялық қызметі) стандарттары бойынша 5 классқа (төменнен жоғарыға дейін) жіктелді: зардап шекпеген, төмен, орташа-төмен, орташа-жоғары және жоғары зақымдану [5].

3. NDVI (Normalized Difference Vegetation Index): Өсімдік биомассасының жоғалуын бағалау үшін қолданылды:

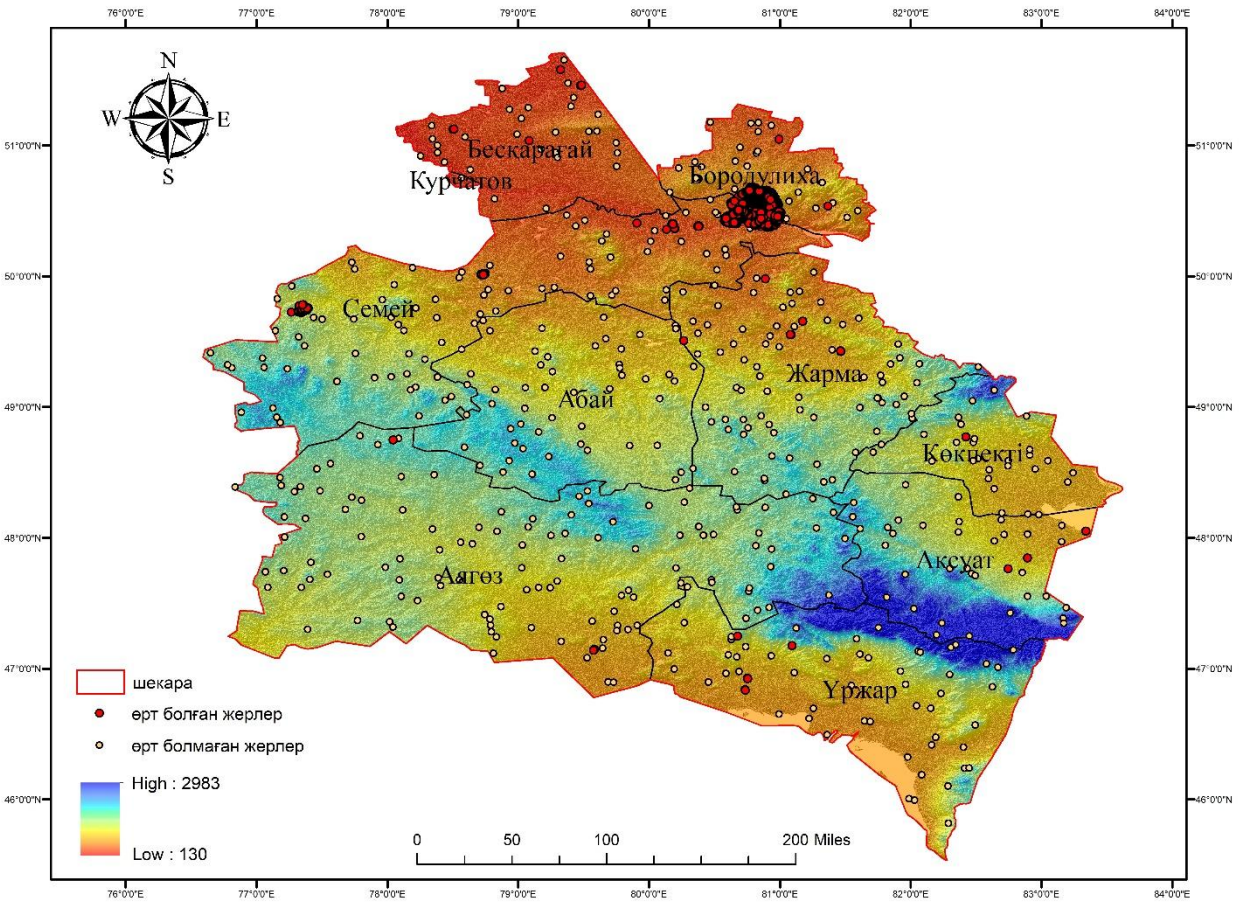
$$NDVI = \{NIR - RED\}\backslash\{NIR + RED\}$$

Бұл индекс өрттен кейінгі орман жамылғысының фотосинтетикалық белсенділігінің төмендеуін верификациялау үшін қажет болды [4].

**4. Нәтижелер мен талқылау**

4.1. Өрт ошақтарының кеңістіктік-уақыттық динамикасын талдау

NASA FIRMS (VIIRS/MODIS) деректерін талдау негізінде 2023 жылғы маусымдағы өрттің таралу хронологиясы қалпына келтірілді. Алғашқы жылу аномалиялары (термонүктелер) резерваттың оңтүстік-батыс бөлігінде тіркелді. Оңтүстік-батыстан соққан қатты желдің (15–25 м/с) әсерінен өрт фронты тез арада солтүстік-шығыс бағытқа қарай жылжыған. ArcGIS ортасында орындалған өрт ошақтарының тығыздығын талдау (Kernel Density) ең жоғары жану қарқындылығы «Семей орманы» МОТР-ның орталық массивтерінде шоғырланғанын көрсетті, бұл верховой (жоғарғы) өрттің сипатына сәйкес келеді [3], [8].




1 сурет - Абай облысындағы 2023 жылы маусым айындағы өрттің таралу көрсеткіші

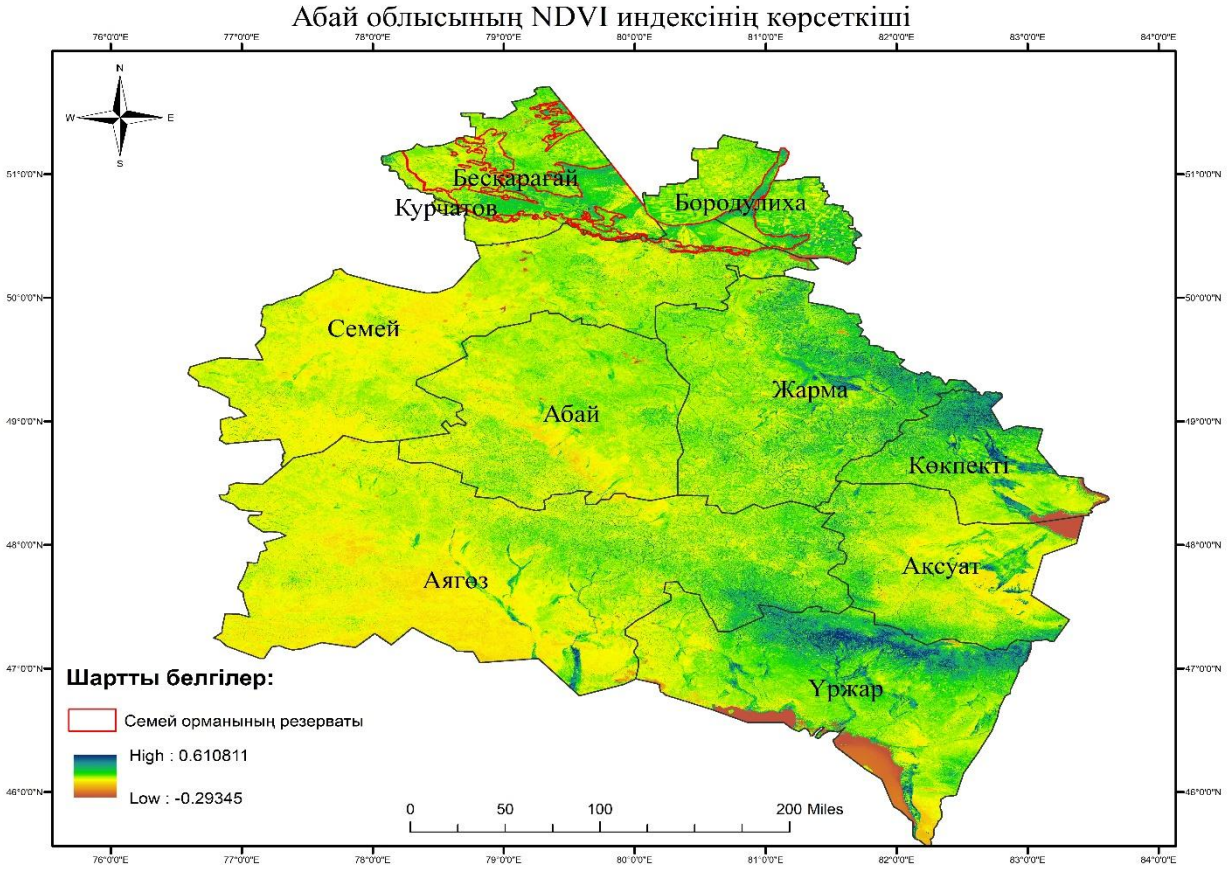
4.2. dNBR индексі бойынша зақымдану деңгейін бағалау

Google Earth Engine платформасында есептелген dNBR (Difference Normalized Burn Ratio) индексі өрттің орман экожүйесіне тигізген зардабын сандық түрде жіктеуге мүмкіндік берді. USGS классификациясына сәйкес алынған мәліметтер 2-кестеде көрсетілген.

**2-кесте. Зақымдану дәрежесі бойынша өртенген аумақтардың үлесі (авторлық есептеулер)**

| dNBR класы | Зақымдану дәрежесі | Ауданы (га) | Үлесі (%) |
|---|---|---|---|
| < -0.1 | Өсімдіктің өсуі (Regrowth) | 819316,2 | 72,83 |
| -0.1 ... 0.1 | Зардап шекпеген | 116627,28 | 10,37 |
| 0.1 ... 0.27 | Төмен (Low Severity) | 180146,8 | 16,01 |
| 0.27 ... 0.44 | Орташа-төмен (Mod-low) | 7036,24 | 0,63 |
| 0.44 ... 0.66 | Орташа-жоғары (Mod-high) | 2144,4 | 0,14 |
| > 0.66 | Жоғары (High Severity) | 326,72 | 0,02 |

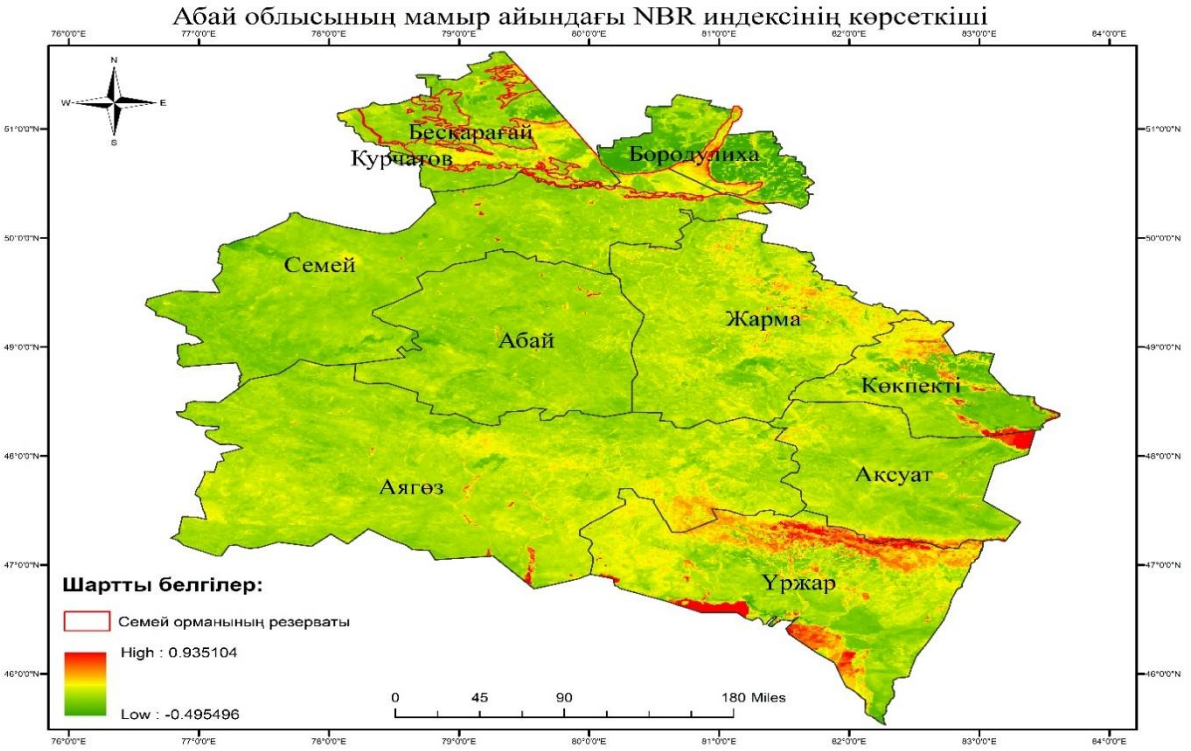
Талдау нәтижесі көрсеткендей, өртенген жалпы аумақтың шамамен 40-50%-ы «жоғары» және «орташа-жоғары» зақымдану кластарына жатады. Бұл аймақтарда қарағайлы насаждениелердің фотосинтетикалық белсенділігінің толық тоқтауы және ағаш қабатының деградациясы байқалады, бұл NDVI мәндерінің 0.6-дан 0.1-0.2-ге дейін төмендеуімен расталады [4].



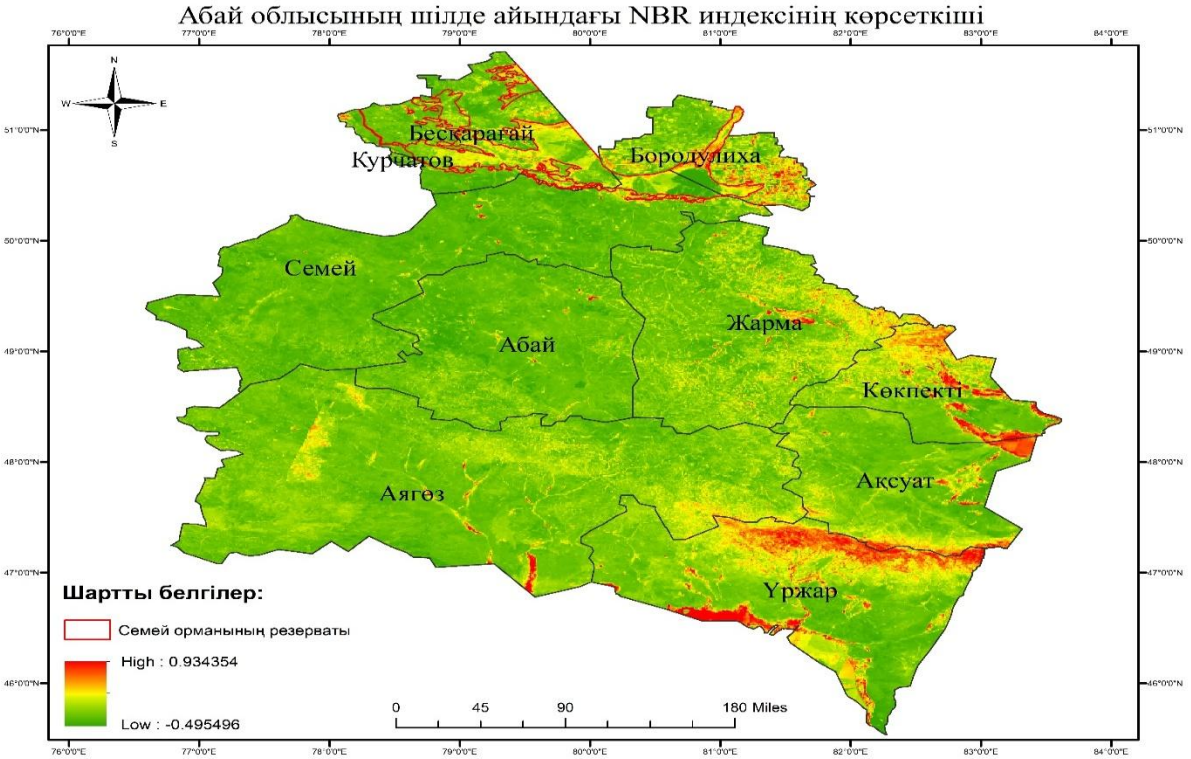

2 сурет - Абай облысындағы 2023 жылғы NDVI индексінінің көрсеткіші

4.3. Рельефтің және экспозицияның өрт қарқындылығына әсері

SRTM цифрлық рельеф моделі мен dNBR картасын беттестіру нәтижесінде орман өртінің таралуына геоморфологиялық факторлардың әсері анықталды. Оңтүстік және оңтүстік-батыс экспозициялы беткейлерде dNBR мәндері солтүстік беткейлермен салыстырғанда орта есеппен 18%-ға жоғары болды. Бұл заңдылық оңтүстік беткейлердегі күн радиациясының жоғары болуына байланысты өсімдік жамылғысы мен төсеніштің (орман төсеніші) ылғалдылығының төмендігімен түсіндіріледі. Алынған нәтижелер аридті зоналардағы өрт динамикасы бойынша жүргізілген алдыңғы зерттеулермен сәйкес келеді [2], [7].




3 сурет - Абай облысындағы 2023 жылы мамыр айындағы NBR индексінінің көрсеткіші

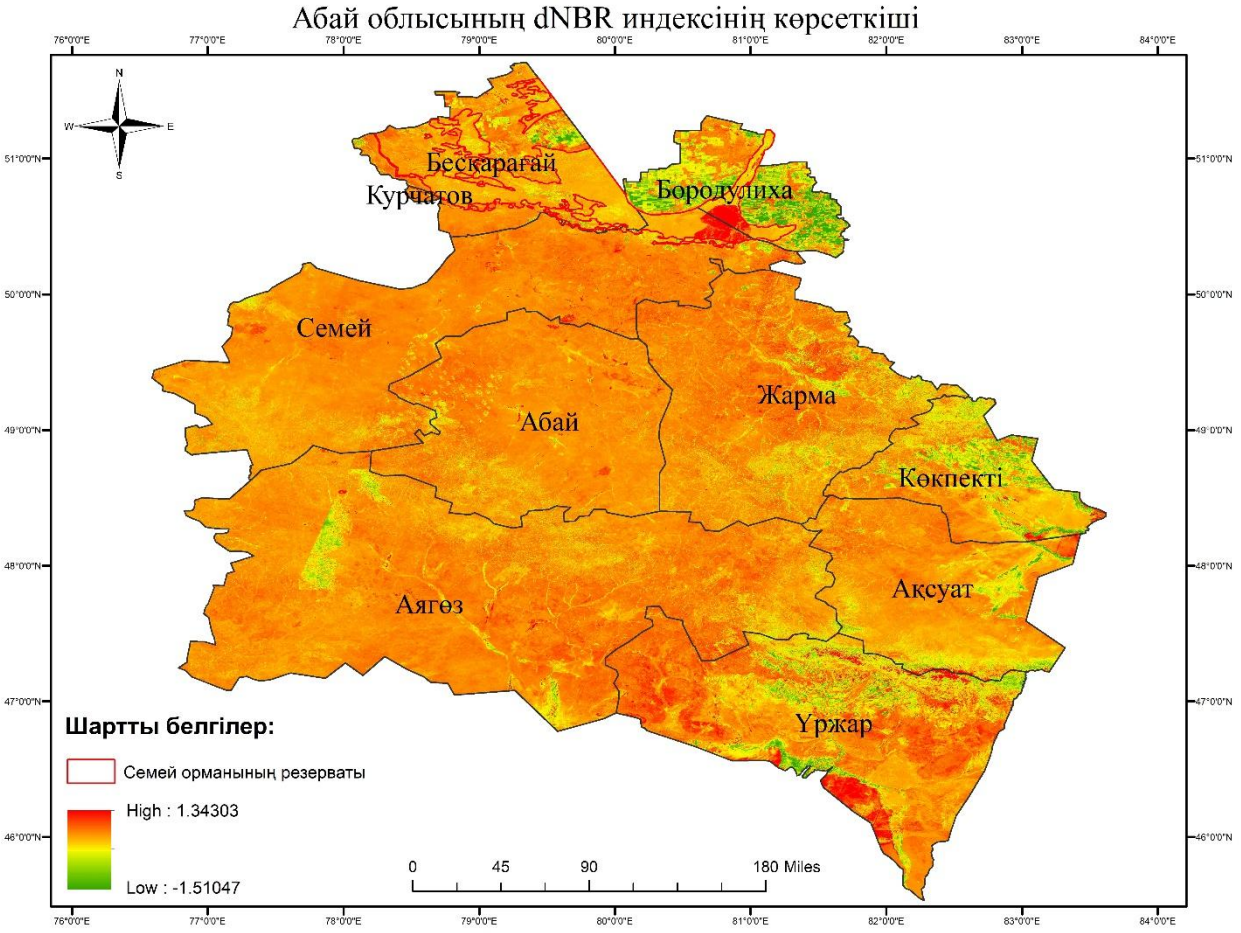



4 сурет - Абай облысындағы 2023 жылы шілде айындағы NBR индексінінің көрсеткіші

4.4. Тәсілдерді салыстыру және әдістемені верификациялау

Біздің зерттеуімізде қолданылған GEE және ArcGIS интеграциялық тәсілі дәстүрлі попиксельдік жіктеуге қарағанда бірқатар артықшылықтарды көрсетті. Landsat 8/9 және

Sentinel-2 деректерінің комбинациясы ленталық ормандардың сирек жамылғысы жағдайында өрт шекарасын 20-30 метрлік дәлдікпен анықтауға мүмкіндік берді. NASA FIRMS нүктелерімен салыстыру (Validation) картаның дәлдігі 92% екенін көрсетті. Сондай-ақ, dNBR индексі визуалды дешифрлеу кезінде байқалмайтын, тек инфрақызыл спектрде көрінетін «жасырын» зақымдану ошақтарын анықтауға көмектесті [5], [9].




5 сурет - Абай облысындағы 2023 жылы dNBR индексінінің көрсеткіші

4.5 Талқылау

Абай облысындағы 2023 жылғы өрттің салдарын қашықтықтан зондтау әдістерімен талдау нәтижелері аймақтың экологиялық тұрақсыздығын және орман экожүйелерінің зақымдану деңгейінің жоғары екендігін көрсетті. Біздің зерттеуімізде алынған dNBR индексінің мәндері мен өртенген аумақтардың кеңістіктік конфигурациясы Asangaliyev және т.б. (2024) [4] жұмысында келтірілген Landsat деректеріне негізделген модельдеу нәтижелерімен айтарлықтай сәйкестік көрсетеді.

Asangaliyev және т.б. [4] өз зерттеуінде Landsat спутниктік мәліметтерін пайдалана отырып, потенциалды өрт қаупі бар аймақтарды картаға түсірудің маңыздылығын атап өткен болатын. Олардың тұжырымдамасы бойынша, өсімдік жамылғысының индекстері (NDVI, NBR) өрттің таралуын болжаудың негізгі индикаторлары болып табылады. Біздің 2023 жылғы нақты өрт оқиғасы бойынша алған dNBR көрсеткіштеріміз авторлардың потенциалды өрт қаупі жоғары деп жіктеген аймақтарының іс жүзінде ең көп зақымдалған («High Severity» класы) аумақтарға сәйкес келетіндігін растайды [4].

Сонымен қатар, Архипов және Сағындықов [2] еңбектерінде атап өтілгендей, Қазақстанның ленталық ормандарының өртке төзімділігінің төмендігі біздің зерттеуіміздегі жоғары зақымдану үлесімен (шамамен 40-50%) дәлелденеді. Біз Sentinel-2 деректерін 60 метрлік ажыратымдылықпен өңдеу арқылы ірі масштабты өрт фронттарын анықтауда жоғары тиімділікке қол жеткіздік. Дегенмен, Asangaliyev және т.б. [4] зерттеуіндегі 30 метрлік Landsat деректерімен салыстырғанда, біздің нәтижелер кеңістіктік генерализацияның әсерінен шағын зақымдану ошақтарын есепке алуда аздаған айырмашылықтар көрсетуі мүмкін.

Біздің нәтижелеріміз бен Asangaliyev және т.б. [4] зерттеуі арасындағы маңызды ұқсастық — рельеф факторының әсері. Авторлар [4] өз жұмысында беткейлердің экспозициясы мен еңістігі өрттің потенциалды қарқындылығын анықтайтын маңызды параметрлер екенін атап өткен. Біздің dNBR және SRTM деректерін интеграциялау арқылы алған нәтижелеріміз (оңтүстік беткейлердегі жанудың 18%-ға жоғары болуы) бұл ғылыми болжамды нақты жағдайда толықтай қуаттайды.

Қорыта айтқанда, Sentinel-2 (30м) және Landsat 8/9 деректерін кешенді қолдану Абай облысындағы орман шаруашылығын мониторингілеуде жоғары нақтылық береді. Бұл зерттеу Asangaliyev және т.б. [4] ұсынған потенциалды өрттерді картаға түсіру әдістемесінің практикалық маңыздылығын бекітіп, оны нақты экологиялық апат салдарларын жою мен орманды қалпына келтіру іс-шараларын жоспарлауда қолдануға болатынын көрсетеді.

**Қорытынды.** Абай облысындағы «Семей орманы» резерваты аумағында орын алған ірі масштабты өртті қашықтықтан зондтау әдістерімен зерттеу келесідей қорытындылар жасауға мүмкіндік берді:

1. Әдістемелік тиімділік: Google Earth Engine платформасында Sentinel-2 спутниктік мәліметтерін Level-2A деңгейінде өңдеу және dNBR спектрлік индексін қолдану өртенген аумақтардың шекарасын және зақымдану дәрежесін жоғары нақтылықпен анықтауға мүмкіндік берді. Кескіндерді 60 метрлік ажыратымдылыққа генерализациялау ірі көлемді өрт массивтерін жедел талдауда тиімді екенін көрсетті.
2. Экологиялық зардаптар: dNBR индексі бойынша жіктеу нәтижесінде өрт шалған аумақтың басым бөлігі «жоғары» және «орташа-жоғары» зақымдану деңгейіне жататыны анықталды. Бұл қарағайлы ормандардың фотосинтетикалық белсенділігінің күрт төмендегенін және биомассаның едәуір бөлігінің жойылғанын растайды.
3. Факторлық талдау: Рельефтің морфометрикалық сипаттамалары өрттің таралу қарқындылығына тікелей әсер еткен. СРТМ деректерімен беттестіру нәтижесі көрсеткендей, оңтүстік және оңтүстік-батыс беткейлердегі өсімдік жамылғысы аридті климаттық жағдайға байланысты өртке ең сезімтал аймақтар болып табылады.
4. Салыстырмалы талдау: Біздің зерттеу нәтижелеріміз Asangaliyev және т.б. (2024) [4] ұсынған потенциалды өрт қаупін болжау модельдерін нақты жағдайда қуаттайды. Бұл спутниктік мониторинг деректерін орман шаруашылығындағы алдын алу шаралары мен стратегиялық жоспарлау үшін негізгі құрал ретінде пайдаланудың маңыздылығын дәлелдейді.

Зерттеу барысында алынған сандық мәліметтер мен зақымдану карталары Абай облысындағы өртенген орман алқаптарын қалпына келтіру, экологиялық

мониторинг жүргізу және болашақтағы өрт қаупін басқару бойынша іс-шараларды әзірлеу үшін практикалық негіз бола алады.

**Әдебиеттер тізімі:**

1. Running, S. W. (2006). Жаһандық жылыну неғұрлым көп әрі ауқымды орман өрттеріне себепші болып отыр ма? *Science*, 313(5789), 927-928. (ағылш. тілінде).

2. Архипов В. А., Сағындықов А. Ж. (2020). Қазақстан Республикасындағы ормандарды өрттен қорғау мәселелері. *Ауыл шаруашылығы ғылымдарының жаршысы*.

3. ҚР ТЖМ ресми есебі. (2023). Абай облысындағы орман өртінің себептері мен салдарларын талдау.

4. Asangaliyev, E. A., және т.б. (2024). Landsat спутниктік деректері негізінде ықтимал табиғи өрттерді кеңістіктік талдау және картаға түсіру. *Journal of Environmental Management and Tourism*. (Негізгі дереккөз).

5. Key, C. H., & Benson, N. C. (2006). Ландшафттық бағалау (LA). FIREMON: Ландшафттық бағалау әдістемесі. АҚШ Ауыл шаруашылығы министрлігінің (USDA) Орман қызметі.

6. Байтулин И. О. (2012). Қазақстан экологиясы. Алматы: Ғылым.

7. Мелехов И. С. (1989). Орман пирологиясы. М.: Агропромиздат.

8. Justice, C. O., және т.б. (2002). MODIS өрт өнімдері. *Remote Sensing of Environment*, 83(1-2), 244-262. (FIRMS деректері бойынша негізгі әдебиет).

9. Chuvieco, E. (2020). Спутниктік қашықтықтан зондтау негіздері: экологиялық тұрғыдан келу. CRC Press.

10. Gorelick, N., et al. (2017). Google Earth Engine: Planetary-scale geospatial analysis for everyone. *Remote Sensing of Environment*, 202, 18-27.

**ӘЛЕУМЕТТІК-ГУМАНИТАРЛЫҚ ҒЫЛЫМДАР – СОЦИАЛЬНО-ГУМАНИТАРНЫЕ НАУКИ – SOCIAL AND HUMANITARIAN SCIENCESУДК**

**316.774:004.738.5**

**Хомин Руслан Витальевич**

Магистрант 2 курса
кафедра филологических наук
Карагандинский национальный исследовательский университет им. Е.А. Букетова
(г. Караганда, Казахстан)

# АЛГОРИТМИЗАЦИЯ МЕДИЙНОЙ СРЕДЫ: КАК ТЕХНОЛОГИЧЕСКИЕ ПЛАТФОРМЫ КОНСТРУИРУЮТ ГРАЖДАНСКУЮ АКТИВНОСТЬ МОЛОДЁЖИ

**Аннотация:** В статье исследуется трансформация практик гражданского участия молодёжи под влиянием алгоритмической логики современных медиаплатформ (TikTok, Instagram, YouTube). Традиционные модели формирования гражданской позиции, основанные на публичной сфере, уступают место персонализированным потокам контента. Автор утверждает, что алгоритмы выступают не как нейтральные фильтры, а как активные культурные медиаторы, конструирующие «архитектуру выбора» пользователя. На основе теоретических рамок Э. Паризера, К. Санстейна и Л. Мановича анализируются такие механизмы, как «фильтровочные пузыри», эмоциональная приоритизация и геймификация активизма. В статье разбираются парадоксы алгоритмической среды, включая риски «слактивизма» и поляризации. На примере кейсов гражданской мобилизации в TikTok в России и Казахстане демонстрируется, как технологическая инфраструктура одновременно и расширяет возможности для активизма, и создает новые формы контроля и эфемеризации (краткосрочности) повестки. Делается вывод, что современные медиатехнологии являются не просто инструментом, а со-конфигуратором гражданской культуры молодёжи.

**Ключевые слова:** алгоритмическая культура, гражданская активность, молодёжь, медиаплатформы, TikTok, фильтровочный пузырь, архитектура выбора, персонализация, цифровой активизм, слактивизм.

**Введение.** В ландшафте современных медиа технологические платформы — социальные сети, поисковые системы и рекомендательные сервисы — эволюционировали от простых посредников до доминирующих акторов, формирующих повестку дня. В основе их функционирования лежит алгоритмическая логика, нацеленная на максимизацию пользовательского вовлечения (engagement) и удержание внимания. Для молодёжи, как для «цифровых аборигенов» (digital natives), эта логика становится имплицитным, скрытым регулятором их медиаповедения и, как следствие, социальных практик.

Если ранее гражданская позиция формировалась преимущественно в рамках делиберативной публичной сферы (по Хабермасу) — через институты образования, семьи, традиционные СМИ и общественные дебаты, — то сегодня этот процесс

инкапсулируется внутри персонализированных потоков контента. Индивидуальная новостная лента становится основным окном в социальную реальность. Данная статья исследует, каким образом технологическая архитектура платформ не просто отражает, а активно конструирует практики гражданского участия молодёжи, превращая алгоритмы в ключевых медиаторов между личностью и социумом.

**1. Алгоритм как медиатор медийной культуры**

В гуманитарных исследованиях медиа (media studies) произошел сдвиг от анализа контента к анализу инфраструктуры. Алгоритм в этом контексте — не просто технический фильтр, а культурный актор [1] или, как минимум, мощный медиатор, определяющий эпистемологические и культурные рамки.

Теоретическую оптику для анализа этого процесса предоставляют несколько ключевых концепций. Эли Паризер ввел понятие «фильтровочного пузыря» (filter bubble) [2], описывая, как алгоритмическая персонализация изолирует пользователя в коконе идеологически комфортного контента, лишая его доступа к альтернативным точкам зрения. Это создает фрагментированную информационную среду, где у разных групп отсутствует общая «социальная ткань» фактов.

Касс Санстейн (совместно с Р. Талером) развил эту идею через концепцию «архитектуры выбора» (choice architecture) [3]. Платформы не просто предлагают контент; они *проектируют* среду, в которой пользователь делает выбор. Через «подталкивания» (nudges) — например, через порядок отображения новостей, кнопки реакций или настройки по умолчанию — они направляют поведение пользователя. В социальном контексте это означает, что платформы «подталкивают» нас к определенным мнениям, в том числе и гражданским, часто усиливая «стадный эффект» (herd effect) [3], когда пользователь видит и копирует поведение большинства в своем «пузыре».

В свою очередь, Лев Манович в работе «Software Takes Command» [4] утверждает, что программное обеспечение (software) само по себе стало медиа. Алгоритмы TikTok или Instagram — это не просто инструменты, это *среда*, которая диктует собственный язык (короткие видео, фильтры, дуэты) и собственную логику (виральность, тренды). Дана Бойд также указывала на то, что алгоритмы не нейтральны; они могут кодифицировать и усиливать существующие социальные предубеждения [5]. Таким образом, молодёжная культура сегодня не просто *использует* медиа, а *строится внутри* этой вычислительной медиаэкосистемы, управляющей главным ресурсом XXI века — вниманием.

**2. Персонализация как фактор формирования гражданской позиции**

В отличие от редакторской логики традиционных СМИ, алгоритмическая логика основана на метриках вовлеченности. Это приводит к нескольким искажениям публичной сферы:

**1. Эмоциональная приоритизация.** Алгоритмы обучены распознавать и продвигать контент, вызывающий сильный эмоциональный отклик (гнев, возмущение, удивление, юмор), поскольку он генерирует больше реакций (лайков, комментариев, репостов). В результате гражданский дискурс в лентах молодёжи редуцируется до эмоциональных вспышек и «праведного гнева», вытесняя сложный, рациональный анализ [6].

**2. Вовлечённость как главная метрика.** Контент о гражданских проблемах проходит тот же фильтр, что и развлекательный. Он будет показан, только если

генерирует вовлечение. Это заставляет активистов «упаковывать» свои идеи в виральные, часто упрощенные форматы (например, мем или танцевальный челлендж).

**3. Повышение видимости «спорных» материалов.** Контент, вызывающий поляризацию, часто генерирует больше комментариев (споров) и, как следствие, получает больший охват. Алгоритм, таким образом, может непреднамеренно способствовать не диалогу, а эскалации конфликта и поляризации общества.

Возникает вопрос цифровой этики: платформы, используя непрозрачные «манипулятивные архитектуры», несут ответственность за искажение публичной сферы, однако их бизнес-модель (экономика внимания) прямо противоречит целям создания информированного гражданского общества.

**3. Медиатехнологии как инфраструктура гражданского участия**

Несмотря на риски, технологическая среда предоставляет и беспрецедентную инфраструктуру для гражданского участия. Платформы радикально снижают «порог входа» в гражданскую активность, делая её доступной, быстрой и масштабируемой.

Мы наблюдаем расцвет «алгоритмического активизма», включающего такие формы, как:

- Цифровые петиции (например, на Change.org), создающие иллюзию прямого влияния.
- Краудсорсинг и краудфандинг для социальных проектов (сбор средств на помощь или юридическую защиту).
- Мемополитика — использование мемов как инструмента быстрой и вирусной политической критики, понятной молодёжи.
- Флешмоб-акции и челленджи, несущие социальный или политический посыл (например, #IceBucketChallenge или более политизированные тренды).

Ключевое изменение заключается в том, что технологическая среда геймифицирует гражданскую активность. Участие превращается в «игровой» процесс: оно приносит немедленное социальное одобрение (лайки), даёт ощущение причастности к коллективному действию («я тоже в тренде») и позволяет отслеживать «прогресс» (счётчики репостов). Для молодёжи, выросшей в этой среде, гражданская активность всё чаще воспринимается не через традиционные институции (партии, НКО), а через эти новые, технологически опосредованные медиаритуалы.

**4. Парадоксы и риски алгоритмической среды**

Описанная инфраструктура порождает ряд парадоксов, которые являются прямым следствием её алгоритмической природы.

Во-первых, это радикализация через рекомендации. Алгоритмы, стремясь удержать пользователя, могут создавать «рекомендательные туннели» (rabbit holes). Заметив интерес пользователя к умеренно оппозиционному контенту, система может начать предлагать ему всё более радикальные материалы, поскольку они часто являются более «цепляющими».

Во-вторых, это формирование ложных «коллективных» мнений. В «фильтровочных пузырях» и «эхо-камерах» (где пользователи слышат только эхо собственных мнений) создаётся иллюзия, что мнение, разделяемое в узком кругу, является общепринятым. Это усиливает эффект стаи [3] и затрудняет любой диалог с инакомыслящими, ведя к токсичной поляризации.

В-третьих, это риск подмены реального участия его медиаэмуляцией. Этот феномен, известный как «слактивизм» (slacktivism) или «диванный активизм», является одной из главных этических проблем новой среды. Платформы могут создавать медиаэмуляцию гражданского действия. Пользователь, поставивший лайк под петицией, сделавший репост или сменивший аватар, получает эмоциональное удовлетворение и ощущение выполненного «гражданского долга». Это позволяет «выпустить пар», но не приводит к реальным, более сложным и затратным формам участия (оффлайн-волонтёрство, долгосрочная проектная работа, реальные политические действия).

**5. Кейс-анализ: Алгоритмический активизм в TikTok (Россия и Казахстан)**

Платформа TikTok, с её уникальным алгоритмом, который отдает приоритет не социальному графу (подпискам), а вовлеченности контента, стала яркой ареной для анализа.

**Россия:** Ярким примером стала мобилизация молодёжи вокруг протестных акций в январе-феврале 2021 года [7]. TikTok стал ключевым инструментом для распространения информации о митингах. Алгоритм платформы способствовал молниеносному распространению видео (часто эмоциональных, под музыку) среди миллионов молодых пользователей, которые не были вовлечены в традиционный политический дискурс. Исследователи отмечают [7], что платформа использовалась как для прямой мобилизации, так и для формирования оппозиционного настроения через юмор и мемы. Однако этот всплеск также продемонстрировал и эфемерность (краткосрочность) такого активизма: алгоритм TikTok построен на постоянном обновлении трендов, и политическая повестка была быстро вытеснена новыми развлекательными челленджами.

**Казахстан:** Казахстанский сегмент TikTok (KazTikTok) демонстрирует схожую, но более сложную картину. С одной стороны, как отмечают локальные медиаисследователи [8], платформа стала пространством для низовой гражданской активности. В лентах можно встретить и ЛГБТ-активистов, и эко-активистов, и «чабанов-блогеров», поднимающих проблемы села. Алгоритм TikTok позволяет им получить охват, недостижимый в традиционных СМИ. С другой стороны, доминирующим контентом в казахстанском TikTok остается развлекательный, коммерческий и просветительский (#Кітапток) [9]. Гражданский активизм вынужден конкурировать с ними, используя те же виральные механики. Кроме того, платформы, оперирующие в регионах с чувствительной политической обстановкой, часто прибегают к «пессимизации» или «теневому бану» (shadowbanning) — негласному понижению охвата контента на «опасные» темы. В результате видимость и эффективность гражданской практики молодёжи оказывается алгоритмически зависимой и уязвимой для непрозрачной модерации.

**Заключение.** Анализ показывает, что медийная культура современной молодёжи является гибридным феноменом — результатом не только социальных, демографических и культурных процессов, но и скрытой работы технологической инфраструктуры.

Это подводит нас к ключевому выводу, который может служить тезисом для более широкого (возможно, диссертационного) исследования: современные медиатехнологии не просто *отражают* гражданскую позицию молодёжи, но *активно участвуют* в её формировании. Они делают это через фундаментальную модификацию медиасреды — замену публичной сферы персонализированными потоками — и через внедрение новых

логик потребления контента, где приоритет отдаётся не истинности или значимости, а вовлечённости и эмоциональной реакции.

Понимание этой алгоритмической конструкции гражданственности, её этических рисков и инфраструктурных возможностей, является критической задачей для современной гуманитарной науки, педагогики и политической теории.

**Список литературы:**

1. Kittler, F. A. (1999). Gramophone, Film, Typewriter. Stanford University Press.
2. Pariser, E. (2011). The Filter Bubble: What the Internet Is Hiding from You. Penguin Press.
3. Thaler, R. H., & Sunstein, C. R. (2008). Nudge: Improving Decisions About Health, Wealth, and Happiness. Yale University Press.
4. Manovich, L. (2013). Software Takes Command. Bloomsbury Academic.
5. Boyd, D. (2014). It's Complicated: The Social Lives of Networked Teens. Yale University Press.
6. Tufekci, Z. (2017). Twitter and Tear Gas: The Power and Fragility of Networked Protest. Yale University Press.
7. Лукушин В.А., Рябиченко А.С. (2021). Практика использования TIKTOK как инструмента политической мобилизации (на примере массовых протестных акций января–февраля 2021 г. в России) // Труды объединённой научной конференции "Интернет и современное общество" (IMS-2021). С. 136-148.
8. NewTimes.kz (2021). Абай, челленджи и ЛГБТ-активизм: Чем живет казахстанский TikTok? [Электронный ресурс]. URL: https://newtimes.kz/eksklyuziv/127044-abai-chellendzhi-i-lgbt-aktivizm-chem-zhivet-kazakhstanskii-tiktok
9. Profit.kz (2024). Год в TikTok в Казахстане: самые яркие события и креаторы в 2024. [Электронный ресурс]. URL: https://profit.kz/news/68570/God-v-TikTok-v-Kazahstane-samie-yarkie-sobitiya-i-kreatori-v-2024

**УДК 94(574):930.2**

**Сулейменова Адия Алтаевна**

Ученица 7 класса школы-лицея
BINOM им. К.Сатпаева
(г. Астана, Казахстан)

# ПАВЛОДАРСКОЕ ПРИИРТЫШЬЕ КАК ВЕРОЯТНЫЙ ЦЕНТР КИМАКСКОГО КАГАНАТА: ИСТОРИКО-ГЕОГРАФИЧЕСКИЙ АНАЛИЗ ЛОКАЛИЗАЦИИ ХАКАН-КИМАКА

**Аннотация:** В статье рассматривается проблема локализации столицы Кимакского каганата - города Хакан-Кимак. На основании анализа арабо-персидских письменных источников, историко-географических сведений, расчётно-маршрутного анализа и археологических данных обосновывается вывод о высокой вероятности расположения Хакан-Кимака на территории современного Казахстана, в районе Павлодарского Прииртышья. Особое внимание уделено анализу сообщения средневековых авторов о 81-дневном маршруте от Тараза до столицы кимаков, привязке города к Иртышу и природно-географическим особенностям степной зоны Казахстана. Делается вывод о том, что совокупность письменных, географических и археологических признаков позволяет рассматривать Павлодарское Прииртышье как наиболее вероятный регион расположения одного из главных политических центров Кимакского каганата.

**Ключевые слова:** Кимакский каганат, Хакан-Кимак, Имакия, Павлодар, Иртыш, Казахстан, Аль-Идриси, средневековая география, тюркские государства, Прииртышье.

**Введение.**Кимакский каганат являлся одним из крупнейших тюркских государств IX–XI веков и занимал значительную часть территории современного Казахстана [2]. Государство играло важную роль в политической и торговой системе Центральной Евразии, контролируя степные маршруты между Средней Азией, Алтаем и Западной Сибирью.

Одним из дискуссионных вопросов современной исторической науки остаётся локализация столицы Кимакского каганата - города Хакан-Кимак.

Несмотря на существование различных гипотез, анализ письменных источников, географических характеристик и археологических данных позволяет предполагать, что данный центр находился на территории современного Казахстана, в районе Павлодарского Прииртышья.

**Методология исследования.** В основе исследования использованы сравнительно-исторический метод, историко-географический анализ, сравнительный анализ письменных источников, расчётно-маршрутный метод и анализ археологических данных.

**Научная новизна исследования.** Научная новизна статьи заключается в комплексном сопоставлении письменных источников, географических характеристик маршрутов и расчётных данных для локализации Хакан-Кимака в районе Павлодарского Прииртышья.

В работе предпринята попытка сопоставления сведений о продолжительности маршрута от Тараза до столицы кимаков с современными историко-географическими реконструкциями степных путей.

**Письменные источники о Хакан-Кимаке.** Основными письменными источниками по истории кимаков являются труды арабских и персидских географов и историков: Аль-Идриси, Гардизи, Ибн Хаукаль и других средневековых авторов [1; 3; 5; 6; 8].

Наибольшую ценность представляют сведения Аль-Идриси, содержащиеся в труде «Нузхат ал-муштак фи ихтирак ал-афак» («Книга Рожера») [1]. Аль-Идриси описывал Хакан-Кимак как крупный укреплённый город на Иртыше, являвшийся резиденцией правителя кимаков. Согласно его описаниям, город имел укрепления, рынки, дворец правителя и железные ворота, что свидетельствует о развитии городской культуры Кимакского каганата.

Важное значение имеет сообщение Аль-Идриси о том, что путь от Тараза до столицы кимаков занимал 81 день [1]. Данные сведения позднее анализировались в работах исследователей Кимакского каганата, в частности Кумекова Б.Е [7].

**Расчётно-географический анализ маршрута.** Сообщение Аль-Идриси о продолжительности пути от Тараза до столицы кимаков представляет важный историко-географический ориентир для локализации Хакан-Кимака.

Средняя скорость передвижения караванов и кочевых отрядов в степной зоне Средневековья, по оценкам исследователей истории кочевых обществ и Великого шелкового пути, составляла приблизительно 20–35 км в сутки в зависимости от времени года, рельефа местности и погодных условий [2; 4].

Даже при минимальной средней скорости в 20 км в сутки расстояние составило бы:

81×20=1620 км

При средней скорости 25 км в сутки:

81×25=2025 км

При средней скорости 30 км в сутки:

81×30=2430 км

Современное расстояние между Тараз и Павлодар по автомобильным маршрутам составляет около 1500 км, однако средневековые степные маршруты были значительно длиннее вследствие отсутствия прямых дорог, необходимости обхода природных препятствий, сезонных переходов и использования караванных стоянок.

С учётом данных факторов древний маршрут между Таразом и Средним Прииртышьем мог достигать 1800–2200 км, что в целом соответствует сведениям средневековых авторов о продолжительности пути.

**Географические признаки локализации.** Средневековые источники прямо связывают Хакан-Кимак с Иртышом, что существенно ограничивает круг возможных локализаций [1].

Павлодарское Прииртышье располагается непосредственно на Иртыше и традиционно рассматривается исследователями как территория исторической Кимакии [7].

Особое значение имеют природно-географические характеристики описанного маршрута. Путь от Тараза к Среднему Иртышу проходит преимущественно через степные и полупустынные территории Центрального Казахстана.

Если бы столица кимаков располагалась значительно севернее, в глубокой лесной зоне Западной Сибири, путешественники неизбежно фиксировали бы прохождение через таёжные и лесные территории. Однако подобные сведения в письменных источниках отсутствуют.

Следовательно, природно-географические характеристики маршрута в большей степени соответствуют территории современного Казахстана.

**Историко-этнографические особенности региона.**Дополнительным аргументом в пользу локализации Хакан-Кимака в районе Павлодарского Прииртышья являются историко-этнографические особенности расселения населения в раннем Средневековье.

Среднее Прииртышье традиционно входило в зону степных и лесостепных территорий, являвшихся пространством расселения тюркских кочевых объединений, включая кимаков и кыпчакские племена [4; 7]. Именно степная зона Прииртышья обеспечивала условия для кочевого скотоводства, функционирования караванных маршрутов и существования крупных политических центров.

В то же время северные районы Верхнего Прииртышья и таёжные территории Западной Сибири характеризовались иной природно-хозяйственной средой. В лесных и таёжных регионах преобладали племена, хозяйственная деятельность которых была связана преимущественно с охотой, рыболовством и лесными промыслами.

Данное различие между степной тюркской зоной Среднего Прииртышья и северной лесной зоной согласуется с сообщениями средневековых авторов о характере маршрутов и особенностях территории Кимакского каганата.

**Археологические данные.** Археологические исследования Павлодарского Прииртышья подтверждают наличие развитой кимакской культуры IX–XI веков [9].

На территории региона обнаружены:

- курганы кимакской знати;
- остатки средневековых поселений;
- элементы фортификаций;
- предметы вооружения;
- изделия ремесленников;
- торговые артефакты.

Высокая концентрация памятников кимакской эпохи свидетельствует о существовании здесь важного политического и экономического центра.

**Значение Хакан-Кимака.** Хакан-Кимак являлся одним из важнейших политических и торговых центров степной Евразии. Город выполнял функции административной столицы, военного центра, торгового узла, транзитного пункта между Центральной Азией и Сибирью.

Развитие городской инфраструктуры и наличие укреплений свидетельствуют о высоком уровне государственности кимаков [1; 7].

**Заключение.** Проведённый анализ письменных источников, географических характеристик маршрутов и археологических данных позволяет предполагать высокую вероятность расположения Хакан-Кимака на территории современного Казахстана, в районе Павлодарского Прииртышья.

Таким образом, Павлодарское Прииртышье может рассматриваться как наиболее вероятный регион расположения одного из главных политических центров Кимакского каганата.

**Список литературы**

1. Аль-Идриси. Нузхат ал-муштак фи ихтирак ал-афак («Книга Рожера»). - М.: Восточная литература, 2008.
2. Бартольд В.В. Туркестан в эпоху монгольского нашествия. - М.: Наука, 1963.
3. Гардизи. Зайн ал-ахбар / Пер. с персидского. - Душанбе: Дониш, 1973.
4. Гумилёв Л.Н. Древние тюрки. - М.: Наука, 1967.
5. Ибн Хаукаль. Книга путей и государств. - М.: Наука, 1939.
6. История Казахстана с древнейших времён до наших дней: в 5 т. - Алматы: Атамұра, 2010.
7. Кумеков Б.Е. Государство кимаков IX–XI вв. по арабским источникам. - Алма-Ата: Наука, 1972.
8. Маргулан А.Х. Древняя культура Центрального Казахстана. - Алма-Ата: Наука, 1979.
9. Материалы археологических исследований Павлодарского Прииртышья. - Павлодар, 2015.

Электронный научный журнал «Central Asian Scientific Journal»

Редактор: Байдильдинов Т.Ж.
Комп.верстка: Хусаинов Е.М.

Электронный научный журнал «Central Asian Scientific Journal»
-2026-2(30)-Астана-ИП DOC
Зарегистрировано и выдано свидетельство
Министерством Информации и Общественного Развития РК
№KZ77VPY00147053 от 17.04.2026 г.
ISSN: 3135-3061

*За достоверность публикуемой информации, цитат и иных изложений ответственность несет автор*