heat equations taking into account the Neumann and Dirichlet boundary conditions, which ensures the accuracy and reliability of modeling. The results of computational experiments demonstrating dynamic changes in temperature fields in 2D space are presented. The main attention is paid to the influence of physical parameters such as thermal conductivity, density and specific heat capacity on temperature distribution. The obtained data can be used to improve energy efficiency and quality of production processes in the food industry.

As a result of the research, a model describing temperature fields was developed in the MATLAB PDE Toolbox. The developed model serves as a basis for further research in the field of digital twins and integration with industrial modeling tools such as SIEMENS NX, as well as PML platforms. During this study, various heat transfer coefficients and boundary conditions were tested, which made it possible to determine the optimal model parameters. The final result, presented at the end of the article, demonstrates a smooth and correct distribution of thermodynamic processes, confirming the effectiveness of the proposed approach. In the future, this approach can be used to create more complex virtual production systems that allow not only to analyze thermal processes, but also to develop intelligent heat treatment control systems, improving the adaptability and efficiency of technological processes.

Key words: *digital twins, heat transfer, MATLAB PDE Toolbox, FEM, heat equation, boundary conditions, numerical modeling, temperature field analysis, energy efficiency, thermal process optimization.*

Авторлар туралы мәліметтер

Қалдыбек Махамбетов* – PhD докторант, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан; e-mail: 1998kaldybek@gmail.com.

Бауыржан Бельгибаев – доцент, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Казахстан; e-mail: bbelgybaev@list.ru.

Nadezda Kunicina – Professor, Riga Technical University, Рига, Латвия; e-mail: Nadezda.Kunicina@rtu.lv.

Сведения об авторах

Калдыбек Махамбетов* – PhD докторант, Казахский национальный университет имени аль-Фараби, Алматы, Казахстан; e-mail: 1998kaldybek@gmail.com.

Бауыржан Бельгибаев – доцент, Казахский национальный университет имени аль-Фараби, Алматы, Казахстан; e-mail: bbelgybaev@list.ru.

Nadezda Kunicina – Professor, Riga Technical University, Рига, Латвия; e-mail: Nadezda.Kunicina@rtu.lv.

Information about the authors

Kaldybek Makhambetov* – PhD student, Al-Farabi Kazakh National University, Almaty, Kazakhstan; e-mail: 1998kaldybek@gmail.com.

Baurzhan Belgibaev – Associate Professor, Al-Farabi Kazakh National University, Almaty, Kazakhstan; e-mail: bbelgybaev@list.ru.

Nadezda Kunicina – Professor, Riga Technical University, Riga, Latvia; e-mail: Nadezda.Kunicina@rtu.lv.

Редакцияға енуі 04.04.2025
Өңдеуден кейін түсуі 22.06.2025
Жариялауға қабылданды 23.06.2025

https://doi.org/10.53360/2788-7995-2025-3(19)-6

МРНТИ: 81.93.29

А.М. Нурушева*, Д.Ж. Сатыбалдина, А.К. Шайханова, А.Р. Кусаинов
Евразийский национальный университет имени Л.Н. Гумилева,
010008, Республика Казахстан, г. Астана, ул. Сатпаева, 2
*e-mail: asselnurusheva7@gmail.com

РАЗРАБОТКА МЕТОДА АНАЛИЗА РИСКОВ КИБЕРБЕЗОПАСНОСТИ НА ПРИМЕРЕ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ТРАНСПОРТНОЙ КОМПАНИИ

Аннотация: *В этом исследовании описана комплексная методология анализа рисков кибербезопасности в критически важных информационных системах транспортной компании с упором на системы диспетчерского управления и сбора данных (Supervisory Control and Data Acquisition, SCADA-системы), платформы управления транспортом и решения по продаже билетов. Предложенный подход оценки рисков соответствует международным стандартам и*

рекомендациям Национального института стандартов и технологий. В структуре используется многоэтапный процесс, включая идентификацию объектов, оценку критичности систем на базе многокритериального метода, определение наличия уязвимостей в системе, влияния угроз, определение вероятности реализации угрозы, оценку риска, определение контрмер и оценка остаточного риска. Исследование случая с участием транспортного оператора демонстрирует эффективность метода, показывая, что SCADA-системы, несмотря на умеренную вероятность атаки, демонстрируют высокие уровни риска из-за серьезных эксплуатационных воздействий, в то время как системы продажи билетов представляют меньшие риски, но все же требуют принятия мер, в частности мониторинга, защиты и контроля. Результаты подчеркивают способность модели более точно расставлять приоритеты в усилиях по смягчению последствий, чем традиционные методы, фиксируя тонкие взаимодействия между вероятностью угрозы и последствиями. Этот подход не только решает текущие проблемы инфраструктуры, но и адаптируется к возникающим угрозам, что делает его масштабируемым решением для защиты критически важных систем.

Ключевые слова: *риск, информационная безопасность, уязвимость, угроза, кибербезопасность, транспортная компания.*

Введение

Современная транспортная инфраструктура все больше зависит от цифровых технологий, включая системы диспетчерского управления и сбора данных (Supervisory Control and Data Acquisition, SCADA-системы), платформы управления транспортом и автоматизированные решения по продаже билетов. Эти компоненты критически важны для обеспечения бесперебойной работы транспортных компаний, однако их интеграция в информационно-коммуникационную инфраструктуру сопровождается значительными рисками кибербезопасности. Угрозы, такие как целевые атаки на SCADA-системы [1], компрометация данных пассажиров [2] и нарушения работы логистических платформ [3], могут привести не только к финансовым потерям, но и к серьезным операционным сбоям, угрожающим общественной безопасности.

Стандартные подходы анализа и оценки рисков обычно основаны на точных пороговых показателях и линейных моделях, это приводит к недостаточному уровню эффективности при условиях высокой неопределенности и динамично меняющихся векторов атак [4]. В частности, они не учитывают качественные экспертные оценки, нелинейные взаимосвязи между факторами риска и изменяющиеся условия эксплуатации критически важных систем [5]. В этой связи актуальной задачей становится разработка новых подходов, способных более точно оценивать и прогнозировать киберриски с учетом нечеткости исходных данных [6].

В данной статье предлагается метод анализа рисков кибербезопасности, основанный на нечеткой логике, который позволяет формализовать экспертные суждения, моделировать сложные зависимости между параметрами угроз и вырабатывать обоснованные решения по управлению рисками. В отличие от классических методов, предлагаемый подход делает акцент на критичности систем, применяет систему нечетких правил для вывода уровней риска [7] и обеспечивает интерпретируемость результатов [8].

Разработанная методология соответствует международным стандартам, таким как ISO/IEC 27005 и рекомендациям лучших практик, и была апробирована на примере транспортной компании. Результаты демонстрируют, что метод позволяет более точно определять приоритеты защиты, выявляя, например, высокий уровень риска SCADA-систем даже при умеренной вероятности атаки.

Исследование вносит вклад в развитие методов кибербезопасности критической инфраструктуры, предлагая адаптивный инструмент для принятия решений. Перспективы дальнейшей работы включают интеграцию машинного обучения для динамического обновления моделей угроз и расширение области применения метода на другие секторы транспортной отрасли и иных критических сегментов.

Методы исследования

В рамках разработки метода анализа рисков кибербезопасности критически важных объектов информационно-коммуникационной инфраструктуры (КВОИКИ) транспортной компании была применена комплексная методология, объединяющая методы многокритериального принятия решений (Multiple-Criteria Decision Analysis, MCDA), нечеткое моделирование, стандарты и лучшие практики информационной безопасности.

На первом этапе проведена инвентаризация ключевых информационных активов компании, включая SCADA-системы управления движением транспорта, системы управления перевозками, платформы продажи билетов, корпоративные web-ресурсы, облачные сервисы, системы мониторинга и защиты информации.

Для ранжирования объектов по степени критичности использован метод анализа иерархий (analytic hierarchy process, AHP) [9], позволяющий учесть экспертные оценки значимости критериев ущерба:

1) Опасность для жизни/здоровья (вес 41.9%),
2) Влияние на экономику страны (вес 25.2%),
3) Зависимость других КВОИКИ (вес 14.4%),
4) Экологический ущерб (вес 9.9%),
5) Социальная значимость (вес 5.1%),
6) Международное влияние (вес 3.5%).

Таблица 1 – Оценка объектов по критериям

Критерий→ Объект ↓	Опасность для жизни/ здоровья	Влияние на экономику страны	Зависимость других КВОИКИ	Экологический ущерб	Социальная значимость	Международное влияние
SCADA-системы	9	7	6	9	8	7
Система «Перевозки»	7	9	5	9	8	9
Система продажи билетов	5	6	2	4	8	7

Далее проведено попарное сравнение критериев, которое выполнялось по шкале Саати (1-9), а согласованность оценок проверялась через индекс согласованности (Consistency Index, CI) и отношение согласованности (Consistency Ratio, CR) (CR = 0.064 < 0.1).

На основе взвешенных сумм определены приоритеты исследуемых объектов по следующей формуле:

Взвешенная сумма уровня критичности = ∑ (Оценка × Вес критерия)

По результатам расчетов был определен ранг систем.

Таблица 2 – Определение оценки объектов по критериям степени критичности при использовании метода анализа иерархий

Критерий	Опасность для жизни/ здоровья	Влияние на экономику страны	Экологический ущерб	Зависимость других КВОИКИ	Социальная значимость	Международное влияние
Опасность для жизни/ здоровья	1	3	5	4	6	7
Влияние на экономику страны	1/3	1	4	3	5	6
Экологический ущерб	1/5	1/4	1	1/2	3	4
Зависимость других КВОИКИ	1/4	1/3	2	1	4	5
Социальная значимость	1/6	1/5	1/3	1/4	1	2
Международное влияние	1/7	1/6	1/4	1/5	1/2	1

Таблица 3 – Определение взвешенной суммы уровня критичности и ранга систем

Объект	Взвешенная сумма уровня критичности	Ранг
SCADA-системы	8.02	1
Система «Перевозки»	7.82	2
Система продажи билетов	5.10	3

Согласно ISO 27005 оценка рисков осуществляется по формуле:

Риск = Вероятность × Влияние

Для учета неопределенности в оценках вероятности и воздействия угроз применена нечеткая логика [10]. Лингвистические переменные (Низкий, Средний, Высокий) формализованы через трапециевидные функции принадлежности:

- Влияние: значение критичности системы линейно нормализовано к шкале 1–3 (например, SCADA-системы – 2.6).
- Вероятность угроз: экспертная оценка по шкале 1–3, где низкая – 1, высокая – 3.

Для исследования была составлена база данных, состоящая из более 40 угроз, включая целевые атаки на системы управления, утечки данных, сбои инфраструктуры, природные катаклизмы и др. Также сформирована база данных из более чем 150 уязвимостей, классифицированная по категориям: Информация, Системы, Персонал, Помещение, Сервис, Оборудование.

Далее в исследовании использовались правила нечеткого вывода (например, «ЕСЛИ Влияние = Высокое И Вероятность = Средняя, ТО Риск = Средний»). Дефаззификация проведена методом центра тяжести (центроид), что позволило получить количественные оценки рисков. Например, для реализации угрозы «DoS-атаки» при уязвимости «Опасная архитектура сети»:

- Риск для SCADA-системы составит 2.6, так как вероятность реализации данной угрозы для изолированной системы низкая и будет равна 1. Соответственно получен низкий риск, несмотря на высокий уровень влияния;
- Риск для Системы «Перевозки» - 5.2 (средний риск);
- Риск для Система продажи билетов - 4.0 (средний риск).

Далее эксперт принимает решение об обработке рисков с учетом условий таблице 4.

Таблица 4 – Варианты обработки риска

Уровень риска	Диапазон	Описание риска, варианты обработки риска
Низкий	1.0 – 3.9	Допустимый, может быть
Средний	4.0 – 6.9	Требует мер по снижению, передаче или отказу от риска
Высокий	7.0 – 9.0	Требует приоритетных мер по снижению, передаче или отказу от риска

Была сформирована база данных с возможными контрмерами. После выбора мер защиты (например, изменение архитектуры сети, внедрение средств защиты от атак, внедрение системы мониторинга, анализа и управления событиями безопасности, резервирование каналов связи и серверов) проведена экспертная оценка их эффективность по шкале от 0 до 1. Остаточный риск рассчитан по формуле:

$$\text{Остаточный риск} = \text{Первоначальный риск} \times (1 - \text{Эффективность мер})$$

Эксперт принимает дальнейшее решение по обработке остаточного риска в соответствии с таблицей 4.

Результаты исследований

В ходе исследования разработан и апробирован метод анализа рисков кибербезопасности критически важных объектов информационно-коммуникационной инфраструктуры транспортной компании.

Наибольшую критичность имеют SCADA-системы (8.02) из-за потенциального воздействия на жизнь/здоровье и зависимость других систем. Система «Перевозки» демонстрирует высокий уровень критичности из-за значительного влияния на экономику страны. Система продажи билетов обладает средним уровнем критичности (5.10), но требует контроля из-за социальной значимости системы для населения.

В результате исследования все остаточные риски переведены в категорию «Низкий», что подтверждает эффективность предложенных контролей и отсутствие необходимости дальнейшего снижения/ передачи риска либо отказа от риска.

К преимуществам предложенного метода можно отнести гибкость в работе с экспертной неопределенностью и динамическими угрозами.

Таким образом, разработанный метод позволяет точно ранжировать критические системы на основе многокритериального анализа, учитывать неопределенность через нечеткие модели, оптимизировать ресурсы киберзащиты за счет приоритизации рисков.

Наличие сформированных баз данных активов, уязвимостей, угроз и контролей позволяет быстро научиться использовать методику и легко проводить оценку рисков информационной безопасности для транспортных компаний.

Применение метода анализа иерархий позволило определить весовые коэффициенты критериев ущерба и рассчитать интегральные оценки критичности для ключевых систем (табл. 1-3). Результаты подтвердили эффективность комбинации AHP и нечеткой логики для анализа рисков в транспортной инфраструктуре. Метод обеспечивает прозрачность принятия решений и соответствует международным стандартам и лучшим практикам. Дальнейшие исследования будут направлены на адаптацию модели для других секторов критической инфраструктуры. Также в последующем планируется внедрение машинного обучения для автоматизации оценки и выбора контролей, интеграция с моделями машинного обучения для прогнозирования угроз.

Обсуждение научных результатов

Полученные результаты демонстрируют несколько ключевых положительных научных и практических аспектов. Разработанный метод сочетает преимущества двух подходов: количественной оценки через AHP, качественного анализа через нечеткую логику.

В отличие от традиционных матричных методов, предлагаемый подход учитывает нелинейные зависимости между факторами риска, позволяет работать с экспертной неопределенностью, обеспечивает более точную градацию уровней риска. Результаты показывают высокую адаптивность метода к специфике транспортной инфраструктуры и возможность тонкой настройки параметров под конкретные объекты. Немаловажным является простота подхода управления рисками и наглядность для лиц, принимающих решения.

Результаты исследования вносят вклад в развитие методов оценки киберрисков и теорию принятия решений в условиях неопределенности.

Проведенное исследование подтвердило эффективность предложенного комбинированного подхода. Полученные результаты имеют как теоретическое значение для развития методов анализа рисков, так и практическую ценность для обеспечения кибербезопасности транспортной инфраструктуры.

Заключение

Проведенное исследование позволило разработать и апробировать комплексный метод анализа рисков кибербезопасности критически важных объектов транспортной инфраструктуры, сочетающий преимущества многокритериального анализа (AHP) и нечеткого моделирования. Разработана адаптивная модель оценки рисков, учитывающая как количественные показатели, так и экспертные мнения. Предложен алгоритм перехода от качественных оценок к количественным показателям риска. Описанный подход позволил установить приоритеты защиты для ключевых систем транспортной компании (SCADA-системы, системы перевозок, системы продажи билетов). Метод может быть адаптирован для других секторов критической инфраструктуры и динамических систем с быстро меняющимися угрозами.

Полученные результаты имеют значительный потенциал для совершенствования систем управления киберрисками в транспортной отрасли. Будущие направления исследований включают интеграцию машинного обучения для обновлений угроз в реальном времени и проверку метода в различных транспортных секторах. Будет проведен анализ возможности автоматизации процесса оценки через интеграцию с системами мониторинга, анализа и управления событиями безопасности.

Список литературы

1. Alanazi M. SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues / M. Alanazi, A. Mahmood, M.J.M. Chowdhury // Computers & Security. – 2023. – Vol. 125.
2. Information Security and Privacy in Railway Transportation: A Systematic Review / P. López-Aguilar et al // Sensors. – 2022. – № 22. – P. 7698. https://doi.org/10.3390/s22207698.
3. Badawi H. Cyber Security Challenges in the Transportation Industry: A Comprehensive Analysis and Recommendations / H. Badawi // Journal of Management and Training for Industries. – 2024. – № 11(2). – P. 16-41.
4. Kalinin M. Cybersecurity Risk Assessment in Smart City Infrastructures / M. Kalinin, V. Krundyshev, P. Zegzhda // Machines. – 2021. – № 9. – P. 78. https://doi.org/10.3390/machines9040078.
5. Cybersecurity Risk Assessments within Critical Infrastructure Social Networks / A. Aktayeva et al // Data. – 2023. – № 8. – P. 156. https://doi.org/10.3390/data8100156.

6. Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things / S. Kerimkhulle et al // Symmetry. – 2023. – № 15. – P. 1958. https://doi.org/10.3390/sym15101958.
7. Cheimonidis P. A Dynamic Risk Assessment and Mitigation Model / P. Cheimonidis, K. Rantos // Appl. Sci. – 2025. – № 15. – P. 2171. https://doi.org/10.3390/app15042171.
8. Merola F. A Risk Assessment Framework Based on Fuzzy Logic for Automotive Systems / F. Merola, C. Bernardeschi, G. Lami // Safety. – 2024. – № 10(2). – P. 41. https://doi.org/10.3390/safety10020041.
9. Saaty T.L. The Analytic Hierarchy Process / T.L. Saaty // The Journal of the Operational Research Society. – 1980. – Vol. 41 Issue 11. – P. 1073-1076.
10. Zadeh L.A. Fuzzy sets / L.A. Zadeh // Information and Control. – 1965. – № 8(3). – P. 338-353.

Информация о финансировании

Работа выполнена в рамках проекта гранатового финансирования Комитета науки Министерства науки и высшего образования Республики Казахстан AP19175746 «Разработка программного инструментария для оценки рисков кибербезопасности систем критической инфраструктуры».

А.М. Нурушева*, Д.Ж. Сатыбалдина, А.Қ. Шайханова, А.Р. Құсайынов
Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
010008, Қазақстан Республикасы, Астана қаласы, Сәтбаев көшесі, 2
*e-mail: asselnurusheva7@gmail.com

КӨЛІК КОМПАНИЯСЫНЫҢ МАҢЫЗДЫ НЫЙМЫСТАРЫНЫҢ МЫСАЛЫН ПАЙДАЛАНУ МЕНЕН КИБЕРҚАУІПСІЗДІК ТӘУЕКЕЛДЕРІН ТАЛДАУ ӘДІСІН ӘЗІРЛЕУ

Осы зерттеу қадағалауды бақылау және деректерді жинау (SCADA) жүйелеріне, көлікті басқару платформаларына және билет сату шешімдеріне баса назар аудара отырып, көлік компаниясының маңызды ақпараттық жүйелеріндегі киберқауіпсіздік тәуекелдерін талдаудың кешенді әдістемесін сипаттайды. Ұсынылған тәуекелді бағалау тәсілі халықаралық стандарттарға және Ұлттық стандарттар мен технологиялар институтының ұсыныстарына сәйкес келеді. Құрылым активтерді сәйкестендіруді, жүйенің критериалдылығын бағалаудың көп критерийін, жүйенің осалдығын бағалауды, қауіп әсерін бағалауды, қауіп ықтималдығын бағалауды, тәуекелді бағалауды, қарсы шараларды анықтауды және қалдық тәуекелді бағалауды қамтитын көп сатылы процесті пайдаланады. Тасымалдау операторының қатысуымен жасалған жағдайлық зерттеу SCADA жүйелерінің орташа шабуыл ықтималдығына қарамастан, ауыр операциялық әсерлерге байланысты жоғары тәуекел деңгейлерін көрсететінін, ал билет сату жүйелері тәуекелдерді төмендететінін, бірақ әлі де бақылау, қорғау және бақылау сияқты шараларды қажет ететінін көрсету арқылы әдістің тиімділігін көрсетеді. Нәтижелер модельдің қауіп ықтималдығы мен әсер ету арасындағы нәзік өзара әрекеттесулерді түсіру арқылы дәстүрлі әдістерге қарағанда жеңілдету әрекеттеріне басымдық беру мүмкіндігін көрсетеді. Бұл тәсіл ағымдағы инфрақұрылымдық мәселелерді қарастырып қана қоймайды, сонымен қатар пайда болатын қауіптерге бейімделіп, оны маңызды жүйелерді қорғау үшін ауқымды шешімге айналдырады.

Түйін сөздер: *тәуекел, ақпараттық қауіпсіздік, осалдық, қауіп, киберқауіпсіздік, көлік компаниясы.*

A. Nurusheva*, D. Satybaldina, A. Shaykhanova, A. Kusainov
L.N. Gumilyov Eurasian National University,
010008, Republic of Kazakhstan, Astana, Satpayev Street, 2
*e-mail: asselnurusheva7@gmail.com

DEVELOPMENT OF A METHOD FOR ANALYZING CYBERSECURITY RISKS USING THE EXAMPLE OF CRITICAL FACILITIES OF A TRANSPORT COMPANY

This study describes a comprehensive methodology for analyzing cybersecurity risks in critical information systems of a transport company, with an emphasis on Supervisory Control And Data Acquisition (SCADA) systems, transport management platforms, and ticketing solutions. The proposed risk assessment approach complies with international standards and recommendations of the National Institute of Standards and Technology. The framework uses a multi-step process including asset identification, multi-criteria system criticality assessment, determination of system vulnerabilities, threat impact, threat likelihood assessment, risk assessment, countermeasure identification, and residual risk assessment. A case study involving a

transportation operator demonstrates the effectiveness of the method by showing that SCADA systems, despite having a moderate attack probability, exhibit high risk levels due to severe operational impacts, while ticketing systems present lower risks but still require measures, such as monitoring, protection, and control. The results highlight the model's ability to more accurately prioritize mitigation efforts than traditional methods by capturing subtle interactions between threat likelihood and impact. This approach not only addresses current infrastructure challenges but also adapts to emerging threats, making it a scalable solution for protecting critical systems.

Key words: *risk, information security, vulnerability, threat, cybersecurity, transportation company.*

Сведения об авторах

Асель Муратовна Нурушева* – PhD, и.о.доцента кафедры информационной безопасности; Евразийский национальный университет имени Л.Н. Гумилева; г. Астана, Казахстан; e-mail: asselnurusheva7@gmail.com. ORCID: https://orcid.org/0000-0001-5407-7191.

Дина Жагыпаровна Сатыбалдина – ассоциированный профессор, кандидат физико-математических наук, директор Научно-исследовательского института информационной безопасности и криптологии при Евразийском национальном университете имени Л.Н. Гумилева; г. Астана, Казахстан; e-mail: satybaldina_dzh@enu.kz. ORCID: https://orcid.org/0000-0003-0291-4685.

Айгуль Кайрулаевна Шайханова – PhD, профессор кафедры информационной безопасности; Евразийский национальный университет имени Л.Н. Гумилева; координатор научных проектов ТОО «WebTotem», г. Астана, Казахстан; e-mail: aigul.shaikhanova@gmail.com. ORCID: https://orcid.org/0000-0001-6006-4813.

Альнур Рамашевич Кусаинов – докторант кафедры информационной безопасности; Евразийский национальный университет имени Л.Н. Гумилева; г. Астана, Казахстан; e-mail: alnur97@mail.ru. ORCID: https://orcid.org/0009-0003-1469-455X.

Авторлар туралы мәліметтер

Асель Муратовна Нурушева* – PhD докторы, ақпараттық қауіпсіздік кафедрасының доцент м.а.; Л.Н. Гумилёв атындағы Еуразия ұлттық университеті; Астана қ., Қазақстан; e-mail: asselnurusheva7@gmail.com. ORCID: https://orcid.org/0000-0001-5407-7191.

Дина Жағыпарқызы Сатыбалдина – доцент, физика-математика ғылымдарының кандидаты, Ақпараттық қауіпсіздік және криптология ғылыми-зерттеу институтының директоры Л.Н. Гумилёв атындағы Еуразия ұлттық университеті; Астана қ., Қазақстанақстан; e-mail: satybaldina_dzh@enu.kz. ORCID: https://orcid.org/0000-0003-0291-4685.

Айгуль Кайрулаевна Шайханова – PhD, ақпараттық қауіпсіздік кафедрасының профессоры; Л.Н. Гумилёв атындағы Еуразия ұлттық университеті; «WebTotem» ЖШС ғылыми жобалардың үйлестірушісі, Астана қ., Қазақстан; e-mail: aigul.shaikhanova@gmail.com. ORCID: https://orcid.org/0000-0001-6006-4813.

Әлнұр Рамашевич Құсайынов – ақпараттық қауіпсіздік кафедрасының докторанты; Л.Н. Гумилёв атындағы Еуразия ұлттық университеті; Астана қ., Қазақстан; e-mail: alnur97@mail.ru. ORCID: https://orcid.org/0009-0003-1469-455X.

Information about the authors

Assel Nurusheva* – PhD, Acting Associate Professor of the Department of Information Security; L.N. Gumilyov Eurasian National University; Astana, Kazakhstan; e-mail: asselnurusheva7@gmail.com. ORCID: https://orcid.org/0000-0001-5407-7191.

Dina Satybaldina – Associate Professor, Candidate of Physical and Mathematical Sciences, Director of the Research Institute of Information Security and Cryptology at L.N. Gumilyov Eurasian National University; Astana, Kazakhstan; e-mail: satybaldina_dzh@enu.kz. ORCID: https://orcid.org/0000-0003-0291-4685.

Aigul Kairulaevna Shaikhanova – PhD, Professor of the Department of Information Security; L.N. Gumilyov Eurasian National University; Coordinator of scientific projects of WebTotem LLP, Astana, Kazakhstan; e-mail: aigul.shaikhanova@gmail.com. ORCID: https://orcid.org/0000-0001-6006-4813.

Alnur Kussainov – PhD student of the Department of Information Security; L.N. Gumilyov Eurasian National University; Astana, Kazakhstan; e-mail: alnur97@mail.ru. ORCID: https://orcid.org/0009-0003-1469-455X.

Поступила в редакцию 11.06.2025
Поступила после доработки 27.06.2025
Принята к публикации 01.08.2025