https://doi.org/10.53360/2788-7995-2025-2(18)-12
МРНТИ: 81.93.29

CC BY 4.0
Check for updates

В.С. Шаров*, Н.Н. Ташатов, А.К. Шайханова
Евразийский национальный университет им. Л.Н. Гумилева,
010000, Республика Казахстан, г. Астана, ул. Сатпаева, 2
*e-mail: vadim.sharov.2025@list.ru

ИССЛЕДОВАНИЕ КЛЮЧЕВЫХ НАПРАВЛЕНИЙ, ПРИНЦИПОВ И МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

Аннотация: *В современном мире технологии развиваются быстро, а угроз в сети становится больше, поэтому защита данных – одна из главных задач. Эта статья представляет обзор ключевых направлений, способов и средств защиты информации в компьютерных сетях. В теоретической части рассматриваются основные способы защиты информации, включая защиту данных с помощью шифрования, системы для выявления атак, способы проверки личности и методы ограничения доступа. Практическая часть статьи содержит количественный анализ научных работ по защите данных в компьютерных сетях с использованием программы Bibliometrix. Полученные результаты позволяют выявить наиболее значимые исследования, авторов и основные тенденции, что помогает лучше понять текущее состояние и перспективы развития этой области. Графики, таблицы и диаграммы в статье помогают визуально представить информацию и выделить наиболее значимые аспекты исследования. На основе проведенного анализа были выделены текущие тенденции и направления в области защиты информации, что помогает лучше понять, как развиваются технологии и какие тренды важны для обеспечения безопасности компьютерных сетей в условиях растущих угроз. Дополнительно рассматриваются вопросы киберугроз и атак на критически важные системы, а также методы их предотвращения.*

Ключевые слова: *Защита информации, компьютерные сети, библиометрический анализ, криптографические методы, обнаружение вторжений, управление доступом.*

Введение

В эпоху цифровых изменений защита информации в сетях становится важной частью информационной среды. Информационные системы постоянно подвергаются рискам. Риск можно определить как возможное событие, способное повлиять на данные компании [1].

Важно не только использовать новые технологии, но и проводить исследования, выявляющие главные тенденции в защите информации. Эта статья посвящена изучению теоретических и практических аспектов безопасности компьютерных сетей, с акцентом на библиометрический анализ научных публикаций через программу bibliometrix. Такой подход позволяет объективно оценить текущее состояние, определить перспективы развития и выделить основные направления будущих исследований.

Актуальность исследования заключается в том, что с каждым годом растет количество киберугроз, и защита информации становится все более важной задачей для всех организаций. Быстрое развитие технологий, использование Интернета в повседневной жизни и переход к цифровым платформам создают новые вызовы для безопасности данных. Поэтому важно не только внедрять новейшие методы защиты, но и понимать, какие тренды и направления становятся ключевыми в области информационной безопасности, чтобы своевременно реагировать на изменения и эффективно защищать информацию от угроз.

Материалы и методы

В данной статье проведен теоретический анализ современных методов защиты информации в компьютерных сетях и библиометрический анализ научных публикаций с использованием программы Bibliometrix.

Теоретическая часть охватывает базовые технологии, включая шифрование, системы обнаружения атак и механизмы контроля доступа. Практическая часть посвящена выявлению ключевых исследований и актуальных трендов в области информационной безопасности на основе библиометрического анализа и визуализации научных направлений.

Полученные результаты

С учетом быстрого роста научной информации и новых методов исследования, библиометрический анализ становится важным инструментом для изучения изменений в научных публикациях, выявления основных направлений и анализа вклада авторов. В этой работе для анализа литературы по теме информационной безопасности в компьютерных сетях будет использован инструмент Bibliometrix.

Динамика публикаций научных материалов за период 2019-2024 годов изображенная на рисунке 1, показывает умеренную вариативность с пиками в 2021 (347 статей) и 2024 (351 статья) годах. В 2020 году наблюдался спад до 317 статей, возможно, связанный с пандемией COVID-19, после чего количество публикаций стабилизировалось в диапазоне 326-351 статьи. Восстановление роста в 2024 году может указывать на завершение долгосрочных проектов и усиление научной активности. В целом, тренд демонстрирует устойчивость научной продуктивности по теме сетевой безопасности с незначительными колебаниями.

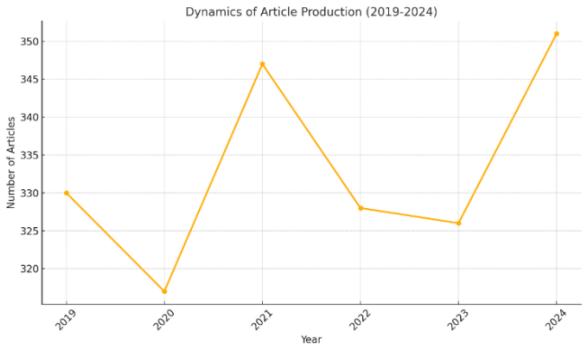

Рисунок 1 – Динамика публикаций научных материалов

Рисунок 2 демонстрирует, что наиболее популярным источником является **IEEE ACCESS**, с большим отрывом имеющий 123 статьи, что указывает на его доминирующую роль в публикационной активности. Второе место занимает **ELECTRONICS (SWITZERLAND)** с 47 статьями, а третье – **SECURITY AND COMMUNICATION NETWORKS** с 44 статьями. Остальные журналы из представленных данных имеют сопоставимые показатели в диапазоне от 31 до 41 статьи, среди которых выделяются **SENSORS** и **COMPUTER NETWORKS**. Эта концентрация публикаций в нескольких ведущих журналах свидетельствует о высокой актуальности и значительном интересе научного сообщества к теме защиты сетевой инфраструктуры.

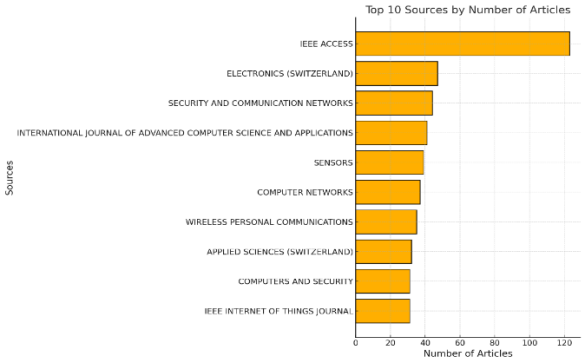

Рисунок 2 – Распределение количества научных материалов по 10 основным источникам

Топ-10 стран по числу публикаций в области сетевой безопасности показанных на рисунке 3 демонстрирует лидирующую роль Китая (1478) и Индии (736), что отражает их значительные инвестиции в исследование современных вызовов киберугроз и защитных технологий. США (277) остаются ведущим центром разработок в кибербезопасности, особенно в прикладных и инновационных направлениях. Южная Корея и Австралия подчеркивают высокий уровень технологий и их применение в защите сетей (рис. 3).

Значительный прогресс Саудовской Аравии (107) и Пакистана (101) указывает на возросшую важность кибербезопасности в Азии и на Ближнем Востоке, что может быть связано с повышенным вниманием к защите критической инфраструктуры и цифровой трансформацией в регионе.

Рисунок 4 показывает, что наиболее исследуемой областью является **«network security»** с 1261 упоминанием, что подчеркивает центральную роль защиты сетей в современной кибербезопасности. Другие популярные направления включают **«internet of things» (269)**, отражающее рост интереса к защите IoT-устройств, и **«security» (255)**, охватывающее общее понятие кибербезопасности.

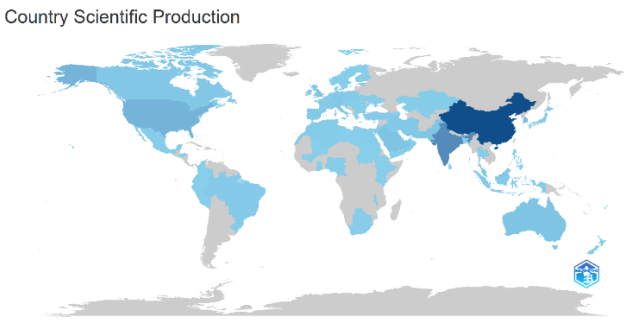

Рисунок 3 – Географическое распределение научных материалов по странам

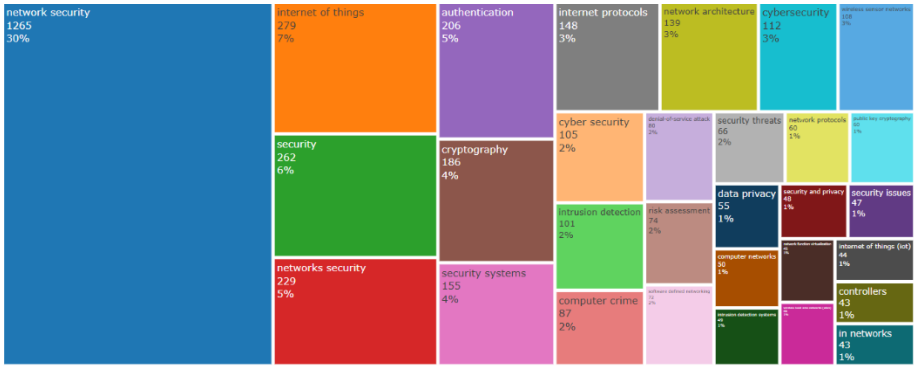

Рисунок 4 – Популярность ключевых направлений в области безопасности компьютерных сетей

Темы, такие как **«authentication» (205)** и **«cryptography» (186)**, фокусируются на методах защиты данных, а **«network architecture» (139)** подчеркивает важность структуры сетей для обеспечения безопасности. Присутствие терминов **«internet protocols» (148)** и **«cybersecurity» (112)** указывает на постоянный интерес к базовым технологиям и стратегическим аспектам защиты.

Эти результаты демонстрируют разнообразие исследуемых направлений, с акцентом на практические и технологические аспекты кибербезопасности, особенно в контексте сетевой защиты и новых вызовов, таких как IoT.

Обсуждение

В современном мире, где компьютерные сети являются основой обмена данными, вопросы их защиты становятся особенно важными. Однако стремительное развитие технологий способствует росту угроз, которые могут нарушить защиту данных, их сохранность и доступность. Основные виды сетевых угроз приведены на рисунке 5.

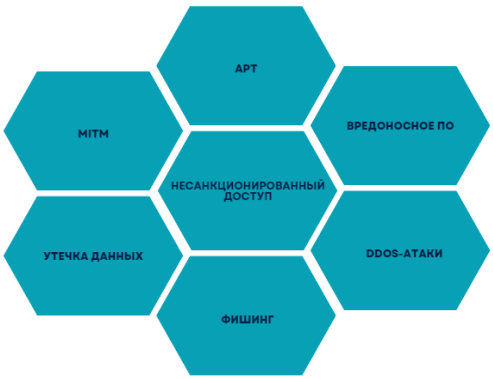

Рисунок 5 – Основные виды сетевых угроз

Один из наиболее распространенных рисков – это попытки несанкционированного проникновения в систему с целью получения данных. Хакеры находят уязвимости в системах аутентификации и контроля доступа, чтобы пробраться в сеть и завладеть конфиденциальными данными.

Зловредные приложения, включая вирусы, трояны, червей и программы-шифровальщики, представляют собой серьезную опасность для компьютерных сетей. Вредоносное ПО постоянно развивается, находя новые уязвимости и атакуя различные организации [2].

Атаки «отказ в обслуживании» нацелены на исчерпание возможностей сетевых ресурсов, что делает сервисы недоступными для пользователей. DDoS-атаки — это разновидность таких атак, когда злоумышленники пытаются отключить сеть и заблокировать доступ [3].

Одной из значительных угроз направленных на пользователей и компании является фишинг. Это поддельные письма, с помощью которых мошенники пытаются завладеть личными данными, такими как пароли или номера банковских карт. Существует и более сложный вариант – целевой фишинг, когда сообщение выглядит так, будто его отправил знакомый человек или надёжная компания [4]. Среди методов социальной инженерии можно выделить атаки в соцсетях, автоматические фальшивые запросы и манипуляции с содержанием информации [5].

Утечка данных – инцидент, в результате которого личная или конфиденциальная информация становится доступной посторонним, что может вызвать серьёзные последствия [6]. Хакеры ищут уязвимости в операционных системах, сетевых протоколах и приложениях. Отсутствие своевременных обновлений делает такие атаки более вероятными.

Один из опасных методов – атака MITM («человек посередине»), когда третье лицо вмешивается в обмен данными между пользователями. Особенно уязвимы для такого перехвата открытые Wi-Fi сети.

Продвинутые устойчивые угрозы (APT) – сложные атаки, нацеленные на продолжительное проникновение в сети предприятий с целью кражи данных. Такие угрозы действуют скрытно: злоумышленник остаётся незамеченным в течение долгого времени [7].

Современные системы защиты испытывают трудности в выявлении APT, так как эти атаки используют продвинутые методы взлома и работают в высоконагруженных сетях с большим объёмом трафика [8].

Основы сетевой безопасности включают ключевые принципы, направленные на защиту информации и предотвращение атак. Фундаментальным принципом защиты данных является триада CIA. Конфиденциальность означает, что доступ к информации имеют только авторизованные пользователи. Целостность гарантирует защищенность данных от несанкционированных правок. Доступность отвечает за бесперебойную работу систем, предотвращая сбои, вызванные, например, DDoS-атаками.

Грамотное управление доступом гарантирует, что пользователи и устройства получают только те данные, которые им необходимы. Этот процесс сопровождается определением личности, подтверждением личности с помощью паролей, биометрии и других методов и авторизацией (разграничение прав на основе заданных правил). Авторизация определяет уровень доступа, опираясь на стратегию, модель и политику управления правами, где учитываются субъект, объект и выполняемые действия [9].

Подход Zero Trust основывается на принципе, что ни один пользователь или устройство, независимо от их местоположения, не должны автоматически получать доверие. Это особенно важно в эпоху облачных технологий и удаленной работы. Внедрение Zero Trust технологии требует кардинального пересмотра подходов к кибербезопасности, особенно для организаций, привыкших полагаться на традиционные модели защиты периметра [10].

Системы мониторинга, такие как IDS и SIEM, играют ключевую роль в защите сетей. SIEM помогает анализировать большие объемы данных, улучшая процесс принятия решений [11]. IDS-системы применяются для обнаружения и предотвращения несанкционированного доступа, неправомерного использования и модификации защищаемой информации в сетях [12].

Шифрование является важнейшим элементом защиты данных, гарантируя их безопасность как при передаче по сети, так и при хранении. Для защиты веб-трафика применяются протоколы SSL/TLS, а криптографические алгоритмы, такие как AES и RSA, препятствуют несанкционированному доступу к конфиденциальной информации.

Межсетевые экраны (firewalls) – это устройства или программы, которые контролируют входящий и исходящий сетевой трафик по заранее установленным правилам безопасности.

В частности, новейшие межсетевые экраны, относящиеся к NGFW (Next-Generation Firewalls), не только фильтруют трафик, но и проверяют содержимое данных, выявляя потенциально вредоносные элементы.

Антивирусные программы защищают конечные устройства, такие как компьютеры и серверы, от вредоносного ПО. Главные функции антивирусных систем для сетей – это обнаружение вирусов, предотвращение их распространения по сети и удаление уже попавших в систему вирусов.

Политики безопасности определяют правила и действия для защиты информации и уменьшения угроз. Это включает разработку норм для контроля доступа, работы с защищаемой информацией, а также использования техники и программного обеспечения. Эффективная настройка и внедрение контроля занимают ключевую роль в обеспечении безопасности в любой организации. Например, политика может требовать обязательного использования двухэтапной проверки для входа в корпоративные ресурсы. Двухфакторная проверка важна для веб-безопасности, поскольку она снижает риски, связанные с утерянными или скомпрометированными паролями.

Обучение сотрудников важно для защиты от атак, связанных с человеческим фактором, например, фишинга или социальной инженерии.

Подход «Defense in Depth» заключается в использовании нескольких уровней защиты для снижения рисков (рис. 6).

Рисунок 6 – Подход Defense in Depth

Целостная стратегия защиты данных включает использование как технических средств, так и организационных мер с учетом роли человека. Он учитывает, что ни одна технология не может полностью защитить без участия людей, и наоборот. Сочетание технологий и человеческого фактора заключается в создании системы, где технические решения дополняются знаниями и действиями сотрудников. Например, даже самый надежный межсетевой экран не предотвратит угрозу, если пользователь случайно откроет доступ злоумышленникам через фишинг. Поэтому необходимо не ограничиваться только новыми технологиями, но и проводить обучение сотрудников, улучшая их знания в области кибербезопасности.

Заключение

Таким образом защита информации включает в себя технические решения, организационные меры и их взаимодействие в рамках комплексной системы. Межсетевые экраны и антивирусы защищают от технических угроз, в то время как политики безопасности и обучение сотрудников помогают минимизировать риски, связанные с влиянием человека. Основным аспектом следует считать сочетание технологий и осведомленности сотрудников, что помогает построить надежную систему защиты от актуальных угроз в сети. Всесторонний подход дает возможность обеспечить многослойную защиту, где каждое решение дополняет другие, создавая стабильную и безопасную инфраструктуру.

Будущее защиты данных связано с сочетанием автоматических решений и участия людей. Хотя технологии, такие как глубокое обучение и алгоритмы анализа данных, помогают оперативно обнаруживать угрозы, основную роль играет осведомленность и подготовка пользователей. Только объединение передовых технологий, правильных процессов и ответственности всех участников поможет создать систему безопасности, которая будет адаптироваться к новым вызовам и защищать данные от сложных кибератак.

Список литературы

1. Alsafwani N. Strategic approaches in network communication and information security risk assessment / N. Alsafwani, Y. Fazea, F. Alnajjar // Information. – 2024. – Vol. 15, № 6. – P. 353.
2. Alharbi F. Empowering network security through advanced analysis of malware samples: Leveraging system metrics and network log data for informed decision-making / F. Alharbi, G.S. Kashyap // International Journal of Network Distributed Computing. – 2024. – Vol. 12. – P. 250-264.
3. Detection and characterization of DDoS attacks using time-based features / J. Halladay et al // IEEE Access. – 2022. – Vol. 10. – P. 49794-49807.
4. Phishing feedback: Just-in-time intervention improves online security / S. Bender et al // Behavioural Public Policy. – 2024. – P. 1-13.
5. Social engineering attacks prevention: A systematic literature review / W/ Syafitri et al // IEEE Access. – 2022. – Vol. 10. – P. 39325-39343.
6. Understanding data breach from a global perspective: Incident visualization and data protection law review / G. Pimenta Rodrigues et al // Data. – 2024. – Vol. 9, № 2. – P. 27.
7. Explainable deep learning approach for advanced persistent threats (APTs) detection in cybersecurity: A review / N.H.A. Mutalib et al // Artificial Intelligence Review. – 2024. – Vol. 57. – P. 297.
8. Threat intelligence sharing community: A countermeasure against advanced persistent threat / S. Chandel et al // IEEE Conference on Multimedia Information Processing and Retrieval (MIPR). – 2019. – P. 353-359.
9. A systematic literature review for authorization and access control: Definitions, strategies, and models / A.K.Y.S. Mohamed et al // International Journal of Web Information Systems. – 2022. – Vol. 18, № 2/3. – P. 156-180.
10. Itodo C. Multivocal literature review on zero-trust security implementation / C. Itodo, M. Ozer // Computers & Security. – 2024. – Vol. 141. – P. 103827.
11. Revolutionizing SIEM security: An innovative correlation engine design for multi-layered attack detection / M. Sheeraz et al // Sensors. – 2024. – Vol. 24, № 15. – P. 4901.
12. Pavithra C. A comprehensive classification approach by integrating principal component analysis and support vector machines for advanced intrusion detection systems / C. Pavithra, M. Saradha // SN COMPUT. SCI. – 2024. – Vol. 5. – P. 996.

В.С. Шаров*, Н.Н. Ташатов, А.К. Шайханова
Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
010000, Қазақстан Республикасы, Астана қаласы, Сәтбаев көшесі, 2
*e-mail: vadim.sharov.2025@list.ru

КОМПЬЮТЕРЛІК ЖЕЛІЛЕРДЕ АҚПАРАТТЫ ҚОРҒАУДЫҢ НЕГІЗГІ БАҒЫТТАРЫН, ҚАҒИДАТТАРЫНЫҢ ЖӘНЕ ӘДІСТЕРІН ЗЕРТТЕУ

Қазіргі әлемде технологиялар қарқынды дамып келеді, ал желідегі қауіп-қатерлер көбейіп жатыр, сондықтан деректерді қорғау – басты міндеттердің бірі. Бұл мақалада компьютерлік желілердегі ақпараттық қауіпсіздіктің негізгі бағыттары, әдістері мен құралдары қарастырылады.Теориялық бөлімде ақпаратты қорғаудың негізгі тәсілдері қарастырылады, оның ішінде деректерді шифрлау, шабуылдарды анықтау жүйелері, тұлғаны растау әдістері және қол жеткізуді шектеу тәсілдері.Мақаланың тәжірибелік бөлімі Bibliometrix бағдарламасын пайдалана отырып, компьютерлік желілердегі деректерді қорғау бойынша ғылыми еңбектердің сандық талдауын қамтиды. Алынған нәтижелер ең маңызды зерттеулерді, авторларды және негізгі үрдістерді анықтауға мүмкіндік береді, бұл осы саланың қазіргі жағдайын және даму болашағын жақсырақ түсінуге көмектеседі. Мақаладағы диаграммалар, кестелер және графиктер ақпаратты көрнекі түрде ұсынуға және зерттеудің ең маңызды аспектілерін бөліп көрсетуге көмектеседі.Жүргізілген талдау негізінде ақпараттық қауіпсіздік саласындағы қазіргі тенденциялар мен бағыттар анықталды, бұл технологиялардың қалай дамып жатқанын және өсіп келе жатқан қауіп-қатерлер жағдайында компьютерлік желілердің қауіпсіздігін қамтамасыз ету үшін қандай трендтердің маңызды екенін түсінуге көмектеседі. Қосымша ретінде, киберқауіптер, сыни маңызды жүйелерге жасалатын шабуылдар және оларды болдырмау әдістері қарастырылады.

Түйін сөздер: *Ақпаратты қорғау, компьютерлік желілер, библиометриялық талдау, криптографиялық әдістер, шабуылдарды анықтау, қолжетімділікті басқару.*

V.S. Sharov*, N.N. Tashatov, A.K. Shaikhanova
L.N. Gumilyov Eurasian National University,
010000, Republic of Kazakhstan, Astana, Satpayev Str., 2
*e-mail: vadim.sharov.2025@list.ru

RESEARCH OF KEY DIRECTIONS, PRINCIPLES, AND METHODS OF INFORMATION PROTECTION IN COMPUTER NETWORKS

In today's world, technology is developing rapidly, and the number of online threats is increasing, making data protection one of the main priorities. This article provides an overview of key areas, methods, and tools for information security in computer networks. The theoretical part examines the main methods of information protection, including data encryption, attack detection systems, identity verification techniques, and access control methods. The practical part of the article includes a quantitative analysis of scientific studies on data protection in computer networks using the Bibliometrix program. The obtained results help identify the most significant studies, authors, and key trends, providing a better understanding of the current state and future prospects of this field. Graphs, tables, and diagrams in the article help visually present information and highlight the most important aspects of the research. Based on the conducted analysis, current trends and directions in information security were identified, helping to understand how technologies are evolving and which trends are crucial for ensuring the security of computer networks in the face of growing threats. Additionally, the article examines issues related to cyber threats, attacks on critical systems, and methods for their prevention.

Key words: *Information security, computer networks, bibliometric analysis, cryptographic methods, intrusion detection, access control.*

Сведения об авторах

Вадим Сергеевич Шаров* – студент магистрант специальности «Системы информационной безопасности», Евразийский Национальный университет имени Л.Н. Гумилева, Республика Казахстан, г. Астана; e-mail: vadim.sharov.2025@list.ru. ORCID: https://orcid.org/0009-0001-9653-5477.

Нурлан Наркенович Ташатов – доцент кафедры информационной безопасности; Евразийский национальный университет имени Л.Н. Гумилева; Республика Казахстан; Республика Казахстан; e-mail: tash.nur@mail.ru. ORCID: https://orcid.org/0000-0002-3271-2163.

Айгуль Кайрулаевна Шайханова – профессор кафедры информационной безопасности; Евразийский национальный университет имени Л.Н. Гумилева; Республика Казахстан; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Авторлар туралы мәліметтер

Вадим Сергеевич Шаров – «Ақпараттық қауіпсіздік жүйелері» мамандығы бойынша магистрант, Еуразия ұлттық университеті Л.Н. Гумилев атындағы, Қазақстан Республикасы, Астана қ.; e-mail: vadim.sharov.2025@list.ru. ORCID: https://orcid.org/0009-0001-9653-5477.

Нурлан Наркенович Ташатов – ақпараттық қауіпсіздік кафедрасының доцент; Л.Н.Гумилёв атындағы Еуразия ұлттық университеті; Қазақстан Республикасы; e-mail: tash.nur@mail.ru. ORCID: https://orcid.org/0000-0002-3271-2163.

Айгуль Кайрулаевна Шайханова – ақпараттық қауіпсіздік кафедрасының профессор; Л.Н.Гумилёв атындағы Еуразия ұлттық университеті; Қазақстан Республикасы; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Information about the author

Vadim Sergeevich Sharov* – Master’s student in the specialty «Information Security Systems», Eurasian National University named after L.N. Gumilyov, Republic of Kazakhstan, Astana, e-mail: vadim.sharov.2025@list.ru.

Nurlan Narkenovich Tashatov – associate professor of the department of Information Security; Eurasian National University named after L.N. Gumilyov; Republic of Kazakhstan; e-mail: tash.nur@mail.ru. ORCID: https://orcid.org/0000-0002-3271-2163.

Aigul Kairulayevna Shaykhanova – professor of the department of Information Security; Eurasian National University named after L.N. Gumilyov; Republic of Kazakhstan; e-mail: shaikhanova_ak@enu.kz. ORCID: https://orcid.org/0000-0001-6006-4813.

Поступила в редакцию 01.04.2025
Поступила после доработки 14.05.2025
Принята к публикации 15.05.2025