**Авторлар туралы мәліметтер**

**Әйгерім Жақыпқызы Жамбулатова*** – магистр, «Математикалық және компьютерлік моделдеу» кафедрасының аға оқытушысы, Л.Н. Гумилев Еуразия ұлттық университеті, Қазақстан; e-mail: aigerimzhambulat@gmail.com. ORCID: https://orcid.org/0009-0000-7749-086X.

**Қилан Әлімхан** – PhD, «Математикалық және компьютерлік моделдеу» кафедрасының аға оқытушысы, Л.Н. Гумилев Еуразия ұлттық университеті, Қазақстан; e-mail: keylan@live.jp. ORCID: https://orcid.org/0000-0003-0766-2229.

**Сведения об авторах**

**Әйгерім Жақыпқызы Жамбулатова*** – магистр, старший преподаватель кафедры «Математическое и компьютерное моделирование», Евразийский национальный университет имени Л.Н. Гумилёва, Казахстан; e-mail: aigerimzhambulat@gmail.com. ORCID: https://orcid.org/0009-0000-7749-086X.

**Қилан Әлімхан** – PhD, профессор кафедры «Математическое и компьютерное моделирование» кафедрасының профессоры, Л.Н. Гумилев Еуразия ұлттық университеті, Қазақстан; e-mail: keylan@live.jp. ORCID: https://orcid.org/0000-0003-0766-2229.

.

**Information about the authors**

**Aigerim Zhambulatova*** – Master's degree, Senior Lecturer of the Department of Mathematical and Computer Modeling, L.N. Gumilyov Eurasian National University, Kazakhstan; e-mail: aigerimzhambulat@gmail.com. ORCID: https://orcid.org/0009-0000-7749-086X.

**Keylan Aimhan** – PhD, Professor of the Department of Mathematical and Computer Modeling, L.N. Gumilyov Eurasian National University, Kazakhstan; e-mail: keylan@live.jp. ORCID: https://orcid.org/0000-0003-0766-2229.

*Редакцияға енуі 22.01.2026*
*Өңдеуден кейін түсуі 03.03.2026*
*Жариялауға қабылданды 10.03.2026*

https://doi.org/10.53360/2788-7995-2026-1(21)-22



IRSTI: 14.35.07

**Y.Sh. Zhursinbek[1], B.Sh. Zhursinbek[1], A.K. Maidanov[*], Sh.Zh. Seilov[1], A.V. Ermakov[2]**
[1]L.N. Gumilyov Eurasian National University,
010000, Republic of Kazakhstan, Astana, Satpayev St. 2,
[2]M.K. Ammosov North-Eastern Federal University,
677000, Russian Federation, Yakutsk, 58 Belinskogo St.
[*]e-mail: makeadil@mail.ru

# IMPLEMENTATION OF THE «IMAGE TO DATA» CONVERTER FOR IMPROVING INFORMATION SECURITY

***Abstract:*** *Enhancing information security can be achieved through a variety of methods, with one notable approach involving the use of specialized hardware and software tools known as the «Image-to-Data» converter. As described by the authors, this device is primarily designed for secure information exchange in scientific research, ensuring data confidentiality and integrity during transfer. Its core principles focus on protecting sensitive information by preventing unauthorized access, making it an essential tool in high-security environments. Although initially developed for scientific purposes, the converter's capabilities are highly adaptable and can be applied to other sectors such as finance, healthcare, and government agencies, where secure communication is vital. By adopting this innovative converter, organizations can significantly strengthen their data protection measures, minimizing risks associated with cyber threats and data breaches. The technology's versatility and robustness facilitate safer data exchange, helping institutions maintain compliance with strict security standards and regulations. Overall, integrating the «Image-to-Data» converter can substantially enhance an organization's security posture, enabling secure, efficient, and versatile information sharing across various fields and industries, thereby supporting the integrity and confidentiality of critical information in an increasingly digital world.*

***Key words:*** *information security, converter, telecommunication network, interface, image, data, tuple.*

**Introduction**

Ensuring the required level of information security is one of the most important tasks faced by telecommunications operators and service providers [1-3]. Addressing this task relies on applying a set of complex procedures that are continually being improved. A common drawback of most information security tools is that their modernization is reactive, responding to newly emerging threats.

The current situation resembles an arms race: offensive tools are typically developed first, followed by defensive measures. A different scenario is observed in the case of burglars attempting to break sophisticated door locks – new locks are developed first, and only then do burglars search for ways to defeat them.

Using this analogy, the purpose of the «Image-to-Data» converter can be viewed as an attempt to place attackers violating information security in a position similar to that of apartment burglars. In other words, the goal is to deprive attackers of the ability to remain on the offensive and, in some cases, to eliminate their ability to cause damage or significantly minimize it.

This paper presents the concept of developing and applying a converter in-tended primarily for applications related to scientific research. The use of the converter does not replace any of the established information security solutions. Instead, the proposed «Image-to-Data» converter should be viewed as an additional means to enhance information security.

**Literature review**

The idea of creating the «Image-to-Data» converter emerged from an interdisciplinary approach [4]. Consider the task of designing an AC power source with high stability in voltage $U$ and frequency $F$ for hypothetical telecommunications equipment. Suppose that when using an external AC power grid, the variations in $U$ (from $U_1$ to $U_2$) and $F$ (from $F_1$ to $F_2$) significantly exceed the permissible limits required for the operation of the equipment: $U_3 \leq U \leq U_4$ and $F_3 \leq F \leq F_4$.

This problem can be solved by using a rectifier, a battery, and an inverter [5]. An example of such a solution is shown in Figure 1. The abbreviations «AC» and «DC» stand for alternating current and direct current, respectively. The rectifier converts AC to DC, enabling the system to store electrical energy efficiently. The battery acts as an energy reservoir, providing power when needed. The inverter then converts DC back to AC for use by various devices. This approach ensures a stable and reliable power supply in the system. Proper calibration of each component is crucial for optimal performance. Additionally, implementing safety mechanisms is essential to prevent overloads and short circuits. Regular maintenance helps identify potential failures before they occur. Using high-quality components can improve the system's overall efficiency and lifespan.

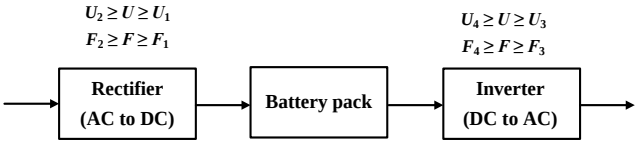


Figure 1 – Example of an AC power source design

Furthermore, integrating smart control systems can optimize energy usage and enhance system responsiveness. Overall, this setup provides a robust solution for managing electrical energy in various applications.

In this example, the values $U_3, U_4, F_3$, and $F_4$ do not depend on $U_1, U_2, F_1$, and $F_2$, respectively. A similar methodological approach was applied in the development of the “Image-to-Data” converter. It should be noted that the use of a battery is not mandatory for achieving the required AC output parameters; rather, it improves the reliability of the power subsystem in the event of a failure of the external AC grid.

**Application Area of the Converter**

It should be emphasized that the initial concept of developing and using the “Image-to-Data” converter was formulated during the design of a telecommunication network for a high-technology company [6]. One of the key aspects considered was the conduct of scientific research. From the perspective of the proposed converter, three features of scientific research are particularly important:

- a small delay in data exchange is generally acceptable and does not significantly exceed the limits established for packet networks [7];
- a researcher receiving information is capable of identifying gross distortions intentionally introduced into the original data;
- the use of neural networks [8] or other artificial intelligence tools [9] may enable the identification of even subtle intentional distortions in the data.

Thus, the original idea limited the application scope of the «Image-to-Data» converter based on these three conditions. In addition, the costs associated with acquiring the required hardware and software should be considered. According to the authors' estimates, these costs are not significant; however, they should be taken into account by specialists planning to use the converter to enhance information security.

**Data Exchange Path Model Using the Converter**

Before describing the model, it is advisable to represent the received information using two tuples: ⟨A, B, C⟩ and ⟨A, B, C, Y, Z⟩. The further discussion is based on another analogy, which relies on the image of an iceberg shown on the left side of Figure 2. It is assumed that the above-water part of the iceberg includes a three-element tuple ⟨A, B, C⟩, which serves to display information on the computer monitor shown in the upper right part of the illustration. The complete five-element tuple ⟨A, B, C, Y, Z⟩, located in the underwater part of the iceberg, is processed by the system unit of the computer shown in the lower right part of Figure 2. The elements $Y$ and $Z$contain service information and malicious objects, respectively.

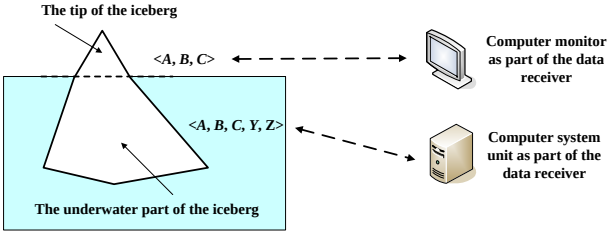


Figure 2 – Representation of received information as two tuples

As noted earlier, a researcher can evaluate the correctness of the received data by analyzing the three-element tuple. This capability was used in the development of the «Image-to-Data» converter. The data exchange path model using the converter is shown in Figure 3. It is assumed that information exchange occurs over an IP network. The application of the converter requires the development of a new interface – UCI (User Converter Interface). The abbreviation «I/D» stands for «Image/Data», while UNI (User Network Interface) is a commonly used term in technical literature [10, 11].

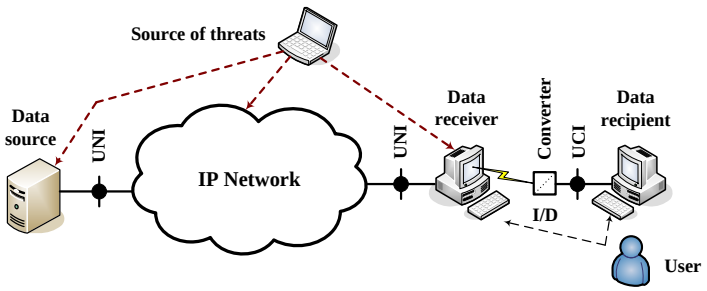


Figure 3 – Information exchange path model using the converter

Although the data receiver and data consumer may be located within the same system unit, the proposed model provides greater clarity. Moreover, separating these elements into different system units enhances the information security of the terminal used by the researcher.

UCI serves to coordinate the terminals referred to as the data receiver and data consumer. The data source and receiver are considered as equipment performing information exchange, whereas the data consumer is an entity capable of correctly interpreting the received information. UNI and UCI are similar in that they are based on the OSI model [12]; their differences are primarily related to the implementation of layers six and seven.

Assume that traditional information security tools estimate the risk of unauthorized access to the data receiver at time $t$ by probability $P(t)$. This probability may increase as new threats emerge. Reducing $P(t)$ typically requires introducing additional protective functions, such as updating firewall software.

By contrast, using the converter significantly reduces the probability $Q(t)$ of unauthorized access to the data consumer terminal, such that $Q(t) \ll P(t)$. The validity of this assertion is the subject of further research outlined later in this paper.

The UCI serves to coordinate the terminals referred to as the data receiver and the data consumer. The data source and data receiver are considered as equipment performing information exchange. The data consumer is an object or subject capable of correctly interpreting the received information. The UNI and UCI are similar in nature, as both are implemented based on the standard OSI (Open Systems Interconnection) model [12]. The differences between them are mainly related to the implementation of the sixth and seventh layers of this model.

Assume that traditional information security tools allow the risk of unauthorized access to the data receiver at time $t$to be estimated by probability $P(t)$. This probability may increase as new types of threats emerge. Reducing the value of $P(t)$ is achieved by introducing additional functional capabilities into protection tools to eliminate newly identified threats. A typical example of such an action is updating firewall software.

As a result of using the converter, the probability $Q(t)$, which determines the risk of unauthorized access to the data consumer terminal at time $t$, is sharply reduced. This fact is expressed by the following inequality: $Q(t) \ll P(t)$

The validity of this assertion is the subject of separate research and is included among the directions for future work formulated at the end of this paper.

If we return to the pair $P(t)$ and $Q(t)$ within the chosen analogy, it can be argued that $Q(t) = 0$. This statement is due to the practical absence of a probabilistic nature in the «Rectifier – Inverter» connection. In this sense, the proposed solution can be considered highly effective. If this assertion appears controversial to the reader, the authors would be grateful for alternative viewpoints.

For the «Image-to-Data» converter, the probabilistic nature of the dependence of the data consumer terminal on external threats cannot be eliminated. In other words, $Q(t) \neq 0$; however, this probability does not differ significantly from zero. Therefore, the proposed solution for improving information security should be considered highly effective, although it cannot eliminate all potential threats. Such threats include various methods of information theft, for example, signal interception resulting from unavoidable electromagnetic emissions.

**Examples of Problems Addressed by the «Image-to-Data» Converter**

First example is related to conducting scientific research in which useful information is presented in the form of numerical data and graphs. Such information may be expressed using the tuple ⟨A, B, C⟩. It is displayed on the monitor of a computer acting as the data receiver. A clear example is the result of an experiment presented on an A4 sheet and, accordingly, on the data receiver's screen in the following form:

- values of variable $x$: 2, 5, 12, 17, 33;
- values of variable $y$ (dependent on $x$): 4, 24, 148, 291, 1078;
- graph of the dependence $y = f(x)$;
- approximation of the obtained dependence $y = f(x)$ in the form $y \approx a + b \cdot x^2$.

Figure 4 shows examples of correct and distorted dependencies of $y$ on $x$. As an intentionally distorted dependency, a linear function is shown. It is assumed that at the initial stage of research, scientific personnel conducting the experiment are able to distinguish the correct function from the distorted one.

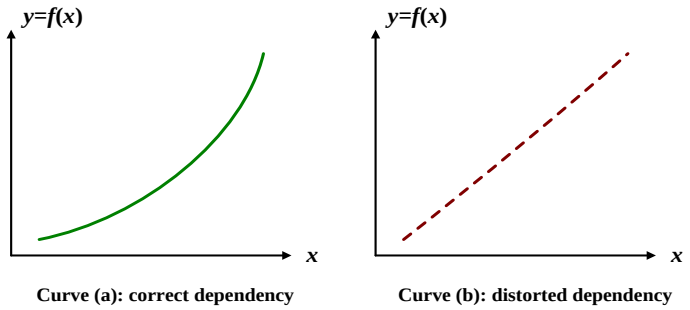


Figure 4 – True and false functions β = f(α)

A distorted dependency may be represented by a curve sufficiently close to the true function. In such cases, it is necessary to use technologies based on neural networks [8], Big Data [13], data mining [14], and pattern recognition [15]. These technologies may serve as useful tools for researchers, helping them verify the obtained results.

In addition, the listed technologies will contribute to reducing the differences between the tuples ⟨A, B, C⟩ and ⟨A_C, B_C, C_C⟩. The subscript «C» in the second tuple indicates that its elements were obtained using the «Image-to-Data» converter. It is obvious that the sets {A} and {A_C}, {B} and {B_C}, {C} and {C_C} will always differ from each other. During the operation of the «Image-to-Data» converter, these differences will be minimized.

The second example concerns the process of controlling the trajectory of an unmanned aerial vehicle (UAV). Let us assume that the UAV is tasked with following an elliptical trajectory to detect potential forest fire sources and illegal logging activities. Figure 5 shows the true and false UAV trajectories. A specialist who formulated the flight task is capable of recognizing a false UAV trajectory caused, for example, by a hacker attack.

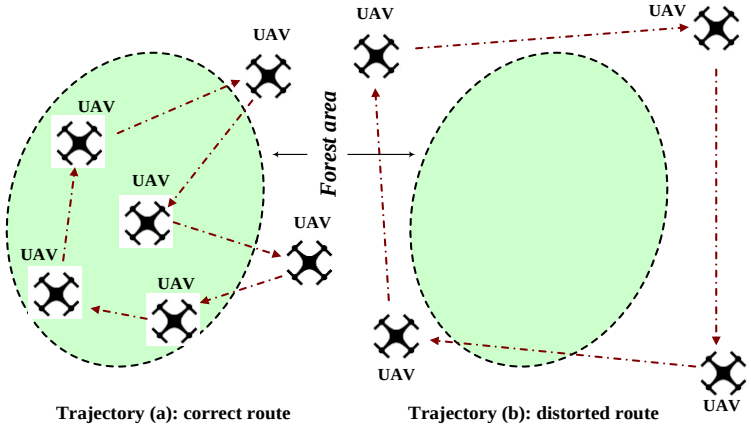


Figure 5 – True and false UAV trajectories

In solving information security problems, an effective tool is the Network of Digital Twins [16]. This network can exchange obtained information with similar or functionally related objects, thereby facilitating the rapid identification of techniques used by attackers. The term «Network of Digital Twins» is not equivalent to the term «Digital Twin Network» introduced by ITU-T Recommendation Y.3090 [17].

A Network of Digital Twins represents a set of objects united by a common purpose. Each such object is an autonomous digital twin [18]. Their interconnection via a telecommunication network enables information exchange that is useful for solving complex problems involving interdisciplinary research aspects. The creation of a Network of Digital Twins requires the development of complex software and the establishment of specialized knowledge bases.

**Future Research Directions**

The proposed method for improving information security is based on the development and subsequent use of an «Image-to-Data» converter as additional hardware and software tools. For this reason, the potential reduction in risk must be weighed against the required investments and the total cost of ownership [19].

As noted above, the use of the «Image-to-Data» converter should be considered an additional measure to improve information security. As a next step, it is planned to analyze the feasibility of applying protective coatings to equipment used for the creation and development of high-technology companies. Such work may be regarded as confirmation of the inequality $Q(t) \ll P(t)$ presented above.

A particularly productive direction for further research is the analysis of the tuple element $Z$, which contains information about malicious software products. Such analysis will make it possible to enhance the level of information security provided by traditional protection tools. Most likely, solving such problems will require interdisciplinary research methods [4].

Another especially important direction for future work is extending the proposed converter to a wider range of applications. The use of quantum computers [20] will enable significant reductions in the additional delay introduced by «Image-to-Data» class converters. This will create a real opportunity to expand the range of information security tasks addressed by the method described in this paper.

**Conclusion**

The application of the «Image-to-Data» converter enables improved information security across a range of critical applications. As experience with such converters accumulates and new technological achievements emerge, the scope of application of the solutions proposed in this paper will expand substantially. At the same time, the installation of the “Image-to-Data” converter does not replace traditional methods of ensuring a specified level of information security but rather complements them with an additional type of hardware-software solution

**References**

1. Andress J. Foundations of Information Security: A Straightforward Introduction / J. Andress. – No Starch Press, 2019. – 248 p.
2. Landoll D.J. Information Security Policies, Procedures, and Standards: A Practitioner's Reference / D.J. Landoll. – Auerbach Publications, 2020. – 240 p.
3. Stamp M. Information Security: Principles and Practice, 3rd Edition / M. Stamp. – Wiley, 2021. – 448 p.
4. Repko A., Szostak R. Interdisciplinary Research: Process and Theory, Third Edition / A. Repko, R. Szostak. – SAGE. – 2017. – 464 p.
5. Maniktala S. Switching Power Supply Design and Optimization, Second Edition 2nd Edition / S. Maniktala. – McGraw Hill, 2013. – 1071 p.
6. Ermakov V. Principles of development of telecommunication system intended for high-technology company / V. Ermakov, N. Sokolov. – Information and Space, 2020. – № 1. – P. 6-11.
7. ITU-T. Network performance objectives for IP-based services. Recommendation Y.1541. – Geneva, 2011. – 66 p.
8. Aggarwal C.C. Neural Networks and Deep Learning / C.C. Aggarwal. – Springer, 2018. – 497 p.
9. Gupta I. Artificial Intelligence and Expert Systems / I. Gupta, G. Nagpal – Mercury Learning and Information, 2020. – 412 p.
10. User Network Interface (UNI) Requirements and Framework. – Metro Ethernet Forum, 2004. – 33 p.
11. ITU, Telecommunication Development Bureau. Telecom Network Planning for Evolving Network Architectures. Reference Manual (Draft version 5.1). – Geneva, 2008. – 448 p.
12. ITU-T. Information technology – open systems interconnection – basic reference model: the basic model. Recommendation X.200. – Geneva, 1994. – 63 p.
13. Erl T. Big Data Fundamentals: Concepts, Drivers & Techniques / T. Erl, W. Khattak, P. Buhler – Prentice Hall, 2015. – 218 p.
14. Han J. Data Mining. Concept and Techniques / J. Han, M. Kamber, J. Pei. – Morgan Kaufmann Publishers, 2011. – 703 p.
15. Bishop C.M. Pattern Recognition and Machine Learning / C.M. Bishop. – Springer, 2016. – 758 p.
16. The Concept of Building a Network of Digital Twins to Increase the Efficiency of Complex Telecommunication Systems / Sh.Zh. Seilov et al // Complexity (Special Issue). – 2021. – Article ID 9480235. – 9 p.

17. ITU-T. Digital twin network – Requirements and architecture. Recommendation Y.3090. – Geneva, 2022. – 26 p.
18. Crespi N. The Digital Twin / N. Crespi, A.T. Drobot, R. Minerva – Springer, 2023. – 1250 p.
19. Economic substantiation of engineering projects in innovation economy / A.V. Babikova et al. – Moscow: INFRA-M, 2024. – 143 p.
20. Majidy S. Building Quantum Computers: A Practical Introductio / S. Majidy, C. Wilson, R. Laflamme. – Cambridge University Press, 2024. – 300 p.

***Acknowledgment***

*This work was supported by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. fund this research AP23488699 «System for Detecting Phytopathogenic In fections in Domestic Fruit Crop Production Using Computer Vision and Artifi cial Olfaction»).*

**Е.Ш. Жүрсінбек[1], Б.Ш. Жүрсінбек[1], А.К. Майданов[1*], Ш.Ж. Сеилов[1], А.В. Ермаков[2]**
[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
010000, Қазақстан Республикасы, Астана қ., Сәтпаев көш., 2
[2]М.К. Аммосов атындағы Солтүстік-Шығыс федералдық университеті,
677000, Ресей Федерациясы, Якутск қ., Белинский көш., 58
e-mail: makeadil@mail.ru

**АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ АРТТЫРУҒА АРНАЛҒАН «IMAGE TO DATA» ТҮРЛЕНДІРГІШІН ІСКЕ АСЫРУ**

*Ақпараттық қауіпсіздікті арттыруға әртүрлі әдістер арқылы қол жеткізуге болады, олардың ішінде ерекше тәсілдердің бірі – «Image-to-Data» деп аталатын мамандандырылған аппараттық-бағдарламалық құралды қолдану. Бұл құрылғы ең алдымен ғылыми зерттеулер аясында ақпарат алмасуды қауіпсіз ұйымдастыруға арналған, яғни деректерді тасымалдау барысында олардың құпиялылығы мен тұтастығын қамтамасыз етуге бағытталған. Оның негізгі қағидаттары құпия ақпаратты рұқсатсыз қол жеткізуден қорғауға негізделген, сондықтан ол жоғары қауіпсіздік талап етілетін ортада маңызды құрал болып табылады.Бастапқыда ғылыми мақсаттарға әзірленгеніне қарамастан, аталған конвертердің мүмкіндіктері кеңейтілген және оны қаржы, денсаулық сақтау, мемлекеттік органдар сияқты қауіпсіз байланыс аса маңызды салаларда да тиімді қолдануға болады. Осы инновациялық конвертерді енгізу арқылы ұйымдар деректерді қорғау деңгейін едәуір күшейтіп, киберқауіптер мен деректердің таралуына байланысты тәуекелдерді азайта алады. Технологияның әмбебаптығы мен сенімділігі ақпарат алмасуды қауіпсіз әрі тиімді ұйымдастыруға мүмкіндік береді, сондай-ақ қатаң қауіпсіздік стандарттары мен нормативтік талаптарға сәйкестікті сақтауға жағдай жасайды. Жалпы алғанда, «Image-to-Data» конвертерін интеграциялау ұйымның ақпараттық қауіпсіздік деңгейін айтарлықтай арттырып, әртүрлі салалар мен индустрияларда маңызды ақпараттың тұтастығы мен құпиялылығын қамтамасыз ете отырып, қауіпсіз әрі тиімді дерек алмасуға мүмкіндік береді.*

***Түйін сөздер:*** *ақпараттық қауіпсіздік, түрлендіргіш, телекоммуникациялық желі, интерфейс, бейне, деректер, кортеж.*

**Е.Ш. Журсинбек[1], Б.Ш. Журсинбек[1], А.К. Майданов[1*], Ш.Ж. Сеилов[1], А.В. Ермаков[2]**
[1]Евразийский национальный университет им. Л.Н. Гумилева,
010000 Республика Казахстан, г. Астана, ул. Сатпаева, 2
[2]Северо-Восточный федеральный университет имени М.К. Аммосова,
677000, Российская Федерация, г. Якутск, ул. Белинского, 58
e-mail: makeadil@mail.ru

**РЕАЛИЗАЦИЯ ПРЕОБРАЗОВАТЕЛЯ «IMAGE TO DATA» ДЛЯ ПОВЫШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

***Аннотация:*** *Повышение уровня информационной безопасности может быть достигнуто различными методами, среди которых особое место занимает применение специализированного аппаратно-программного средства под названием «Image-to-Data». Данное устройство предназначено прежде всего для организации безопасного обмена информацией в рамках научных исследований, обеспечивая конфиденциальность и целостность данных в процессе их передачи. Его основные принципы основаны на защите чувствительной информации от несанкционированного доступа, что делает его важным инструментом в средах с повышенными требованиями к безопасности. Несмотря на то, что изначально конвертер был разработан для научных целей, его*

*функциональные возможности являются расширяемыми, и он может эффективно применяться в таких сферах, как финансы, здравоохранение и государственные органы, где безопасная коммуникация имеет критическое значение. Внедрение данного инновационного решения позволяет организациям существенно усилить уровень защиты данных, минимизируя риски, связанные с киберугрозами и утечками информации. Универсальность и надежность технологии способствуют организации безопасного и эффективного обмена данными, а также обеспечивают соответствие строгим стандартам и нормативным требованиям в области информационной безопасности. В целом интеграция конвертера «Image-to-Data» способна значительно повысить уровень защищенности организации, обеспечивая безопасный, эффективный и гибкий обмен информацией в различных отраслях и поддерживая конфиденциальность и целостность критически важных данных в условиях стремительной цифровизации.*

***Ключевые слова:*** *информационная безопасность, преобразователь, телекоммуникационная сеть, интерфейс, изображение, данные, кортеж.*

**Сведения об авторах**

**Шахмаранович Журсинбек Ерден** – докторант кафедры технологии искуственного интеллекта, Евразийский национальный университет имени Л.Н. Гумилева, Республика Казахстан; e-mail: zhursinbek@gmail.com. ORCID: https://orcid.org/0000-0002-9777-5069.

**Бибинур Шахмарановна Журсинбек** – докторант кафедры компьютерной и программной инженерии, Евразийский национальный университет имени Л.Н. Гумилева, Республика Казахстан; e-mail: zhursinbek99@gmail.com. ORCID: https://orcid.org/0009-0002-4505-470X.

**Адиль Кокенович Майданов*** – преподаватель кафедры компьютерной и программной инженерии Евразийский национальный университет имени Л.Н. Гумилева, магистр, г. Астана, Республика Казахстан; e-mail: makeadil@mail.ru. ORCID: https://orcid.org/0000-0003-2392-5164.

**Шахмаран Журсинбекович Сеилов** – кандидат технических наук, профессор кафедры компьютерной и программной инженерии, Евразийский национальный университет имени Л.Н. Гумилева, Республика Казахстан; e-mail: seilov_shzh@enu.kz. ORCID: https://orcid.org/0000-0001-7057 0461.

**Алексей Валентович Ермаков** – кандидат экономических наук, доцент, Северо-Восточный федеральный университет им. М.К. Аммосова, советник ректора; e-mail: ermakov-it@yandex.ru. ORCID: https://orcid.org/0000-0002-0451-3909.

**Авторлар туралы мәліметтер**

**Ерден Шахмаранұлы Жүрсінбек** – жасанды интеллект технологиялары кафедрасының докторанты, Еуразия ұлттық университеті Л.Н. Гумилев атындағы, Қазақстан Республикасы; e-mail: zhursinbek@gmail.com. ORCID: https://orcid.org/0000-0002-9777-5069.

**Бибінұр Шахмаранқызы Жүрсінбек** – компьютерлік және бағдарламалық инженерия кафедрасының докторанты, Еуразия ұлттық университеті Л.Н. Гумилев атындағы, Қазақстан Республикасы; e-mail: zhursinbek99@gmail.com. ORCID: https://orcid.org/0009-0002-4505-470X.

**Адиль Кокенович Майданов*** – Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Компьютер және Программалық инженерия кафедрасының оқытушысы, магистр, Астана, Қазақстан; e-mail: makeadil@mail.ru. ORCID: https://orcid.org/0000-0003-2392-5164.

**Шахмаран Жүрсінбекұлы Сеилов** – техника ғылымдарының кандидаты, профессор, компьютерлік және бағдарламалық инженерия кафедрасы, Еуразия ұлттық университеті Л.Н. Гумилев атындағы, Қазақстан Республикасы; e-mail: seilov_shzh@enu.kz. ORCID: https://orcid.org/0000-0001-7057-0461.

**Алексей Валентович Ермаков** – экономика ғылымдарының кандидаты, доцент, ректор кеңесшісі, М.К. Аммосов атындағы Солтүстік-Шығыс федералдық университеті, Ресей Федерациясы; e-mail: ermakov-it@yandex.ru. ORCID: https://orcid.org/0000-0002-0451-3909.

**Information about the authors**

**Yerden Zhursinbek** – PhD student, Department of Artificial Intelligence Technologies, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan; e-mail: zhursinbek@gmail.com. ORCID: https://orcid.org/0000-0002-9777-5069.

**Bibinur Zhursinbek** – PhD student, Department of Computer and Software Engineering, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan; e-mail: zhursinbek99@gmail.com. ORCID: https://orcid.org/0009-0002-4505-470X.

**Adil Maidanov*** – Master, Department of Computer and Software Engineering, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan; e-mail: makeadil@mail.ru. ORCID: https://orcid.org/0000-0003-2392-5164.

**Shakhmaran Seilov** – Candidate of Technical Sciences, Professor, Department of Computer and Software Engineering, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan; e-mail: seilov_shzh@enu.kz. ORCID: https://orcid.org/0000-0001-7057-0461.

**Alexey Ermakov** – Candidate of Economic Sciences, Associate Professor, Rector's Advisor, M.K. Ammosov North-Eastern Federal University, Yakutsk, Russia; e-mail: ermakov-it@yandex.ru. ORCID: https://orcid.org/0000-0002-0451-3909.

*Received 16.01.2026*
*Revised 06.03.2026*
*Accepted 10.03.2026*

https://doi.org/10.53360/2788-7995-2026-1(21)-23



IRSTI: 20.53.59

**A. Kenzhebay[1*], A. Tynykulova[2], G. Yensebayeva[1], S. Zhakypbekov[3], K. Bakenova[4]**
[1]Alikhan Bokeikhan University,
070100**,** Republic of Kazakhstan, Abai region, Semey city, Mangilik El str. 11
[2]Astana International University,
010000, Republic of Kazakhstan, Astana, Kabanbay batyr avenue, 8
[3]International Information Technology University,
050016, Republic of Kazakhstan, Almaty, Manas str. 34/1
[4]L.N. Gumilyov Eurasian National University,
010000, Republic of Kazakhstan, Astana city, 2 Satbaev st.
*e-mail: salik2000@icloud.com

# ALGORITHMS FOR SOFTWARE COMPENSATION OF TORSIONAL VIBRATIONS IN H-BOT 3D PRINTERS BASED ON FILTERED B-SPLINES

***Abstract:*** *The rapid development of additive manufacturing technologies imposes increasingly stringent requirements on the positioning accuracy and dynamic stability of motion systems, particularly in printers employing H-bot kinematic architectures, which are prone to torsional vibrations. Such vibrations significantly degrade print quality by inducing trajectory deviations of the print head and cannot be effectively mitigated solely through mechanical reinforcement or conventional control strategies. This study proposes a software-based torsional vibration compensation method founded on the use of filtered B-splines for motion trajectory correction at the planning stage. Unlike existing approaches that rely on rigid digital filtering or real-time adaptive control, the proposed method combines the high approximation capability of B-splines with selective attenuation of spectral components responsible for resonant torsional oscillations.*

*A mathematical model of torsional vibrations in H-bot frame structures is developed, followed by a spectral analysis of their dynamic characteristics to justify the applicability of B-spline-based filtering for identifying and compensating critical frequency components. Numerical simulation results demonstrate a substantial reduction in vibration amplitude and a corresponding decrease in trajectory tracking error of the print head. The practical relevance of the proposed approach lies in its ability to be integrated into standard trajectory planning algorithms without hardware modification, making it applicable to a wide class of H-bot-based additive manufacturing systems.*

***Key words:*** *3D printers; H-shaped kinematics; torsional vibrations; software compensation; filtered B-splines; trajectory correction; spectral analysis; vibrations; print quality; motion planner.*

## Introduction

Additive manufacturing technologies have undergone rapid development in recent years, accompanied by increasing requirements for dimensional accuracy, surface quality, and the dynamic stability of positioning systems. Among the various kinematic architectures used in modern fused deposition modeling (FDM) printers, the H-frame (H-bot) configuration has gained considerable attention due to its compact mechanical structure, reduced moving mass, and capability to achieve high printing speeds [1]. These advantages make the architecture attractive for applications requiring