

УДК 004.65

DOI: [10.26102/2310-6018/2022.39.4.019](https://doi.org/10.26102/2310-6018/2022.39.4.019)

Situation-oriented databases: verifying electronic signatures of heterogeneous documents in a RESTful web service

A.S. Gusarenko 

Ufa University of Science and Technology, Ufa, Russian Federation
gusarenko.as@ugatu.su 

Abstract. When focusing on modern conditions in the field of processing heterogeneous data based on a situation-oriented approach, the task of using information systems with implemented cryptographic technologies during operation arises. One of the examples of such implementation are services and microservices available via the Internet. They provide opportunities to employ their capabilities to verify the authenticity of document enhanced digital signature by means of the published API. Situation-oriented databases (SODB) do not have their own certification authority and encryption-related functionality, but there are opportunities to work with RESTful services by establishing a network connection, thus, there is a research interest in model-oriented processing of heterogeneous documents in cryptographic services and obtaining results from it. To use cryptographic web services in model states, it will be necessary to develop and modify the hierarchical situational model of the SODB in order to enhance it with the ability to work with such services, where authentication of authorization tokens and operating several entry points at the same time are required. The model should also be structured by using specialized elements and methods. The involvement of such services can solve the problem of checking heterogeneous documents: whether they were signed with an enhanced qualified electronic digital signature, the result will be a verification report, the so-called protocol, which is then saved in the database. Such a research objective has not previously been considered from a scientific and technical point of view as part of the SODB project. At the moment, there are opportunities to create tools and methods of the model to solve this problem; the current course design information system based on SODB also exists. By developing the proposed SODB tools, it becomes possible to create applications with the capability to verify heterogeneous documents in cryptographic web services and at the same time avoid laboriousness when creating such applications.


Keywords: situation-oriented database, built-in dynamic model, heterogeneous data sources, JSON, electronic digital signature, verification, RESTful-services.

Acknowledgments: this research is supported by RFBR (grant 19-07-00682); the results of the study, reflecting the structure of the developed software solution, have been obtained as part of the state assignment No. FEUE-2020-0007.

For citation: Gusarenko A.S. Situation-oriented databases: verifying electronic signatures of heterogeneous documents in a RESTful web service. *Modeling, Optimization and Information Technology*. 2022;10(4). Available from: <https://moitvvt.ru/ru/journal/pdf?id=1281> DOI: 10.26102/2310-6018/2022.39.4.019

Ситуационно-ориентированные базы данных: верификация электронных подписей гетерогенных документов в RESTful веб-сервисе

А.С. Гусаренко 

Уфимский университет науки и технологий, Уфа, Российская Федерация
gusarenko.as@ugatu.su 

Резюме. Ориентируясь на современные условия в области обработки гетерогенных данных на

базе ситуационно-ориентированного подхода, возникает задача использования в процессе эксплуатации информационных систем с реализованными криптографическими технологиями. Одним из примеров таких реализаций являются сервисы и микросервисы, доступные через сеть Интернет, они предоставляют возможности за счет опубликованного API пользоваться своими возможностями в целях проверки подлинности усиленной цифровой подписи документа. В ситуационно-ориентированных базах данных (СОБД) нет своего собственного удостоверяющего центра и функциональности, связанной с шифрованием, но есть возможности для работы с RESTful-сервисами за счет установления сетевого подключения. Таким образом, представляется исследовательский интерес к модельно-ориентированной обработке гетерогенных документов в криптографических сервисах и получение из них результатов. Для задействования криптографических веб-сервисов в состояниях модели потребуется проработка и модификация иерархической ситуационной модели СОБД с целью ее обеспечения возможностями работы с такими сервисами, где потребуется проверка подлинности токенов авторизации и работа с несколькими точками входа одновременно. Модель должна быть структурированной также за счет использования специализированных элементов и методов. Задействование таких сервисов может решить задачу проверки гетерогенных документов: вне зависимости от того, были ли они подписаны усиленной квалифицированной электронной цифровой подписью, результатом будет получение отчета о проверке так называемого протокола и сохранение его в базе данных. Такая исследовательская задача ранее не рассматривалась с научно-технических позиций в рамках проекта СОБД, на данный момент существуют возможности для создания средств и методов модели для решения этой задачи и действующая информационная система курсового проектирования, базирующаяся на СОБД. Развивая предложенные средства СОБД, появляется возможность создавать приложения с функциями верификации гетерогенных документов в криптографических веб-сервисах и при этом уменьшать трудоемкость при разработке таких приложений.

Ключевые слова: ситуационно-ориентированная база данных, встроенная динамическая модель, гетерогенные источники документов, JSON, электронная цифровая подпись, верификация, RESTful-сервисы.

Благодарности: работа выполнена при поддержке гранта РФФИ (грант 19-07-00682); результаты исследования, отражающие структуру разрабатываемого программного решения, были получены в рамках государственного задания № ДВУЭ-2020-0007.

Для цитирования: Гусаренко А.С. Ситуационно-ориентированные базы данных: верификация электронных подписей гетерогенных документов в RESTful веб-сервисе. *Моделирование, оптимизация и информационные технологии*. 2022;10(4). Доступно по: <https://moitvivot.ru/ru/journal/pdf?id=1281> DOI: 10.26102/2310-6018/2022.39.4.019 (на англ.).

Introduction

Significant efforts of researchers in the field of security, encryption and cryptography [1] provide information systems with the functionality to sign electronic documents with electronic digital signature certificates [2]. Certifying centers accrediting companies issuing enhanced qualified certificates of electronic signatures, which can be used to sign any text documents from the user's personal file storage, have appeared. Such certificates are issued for both legal entities and individuals. They are used to sign documents and reports are sent to regulatory authorities and other government agencies. It is also possible to exchange documents in electronic document management systems, while documents signed with a qualified electronic signature are recognized by law as legally significant. It should be noted here that web services for signing documents and creating a detached digital signature of a document have already been implemented in the market. In the classic view, a digital signature application consists of an installed cryptographic provider and a desktop application with forms and buttons that help to sign a document. In line with the development of modern technologies, some companies implement the user interface using web technologies, which form a software product

designed as a web system at the final design stage. Web systems also have buttons and controls necessary for the user to upload files for signing or verifying an already signed document. Document management systems additionally provide an opportunity to exchange business letters, documents by coordinating them and signing them in a personal account.

If it concerns a user, and not a corporate application, then all tasks are solved by a cryptographic provider and a desktop program for working with electronic signature certificates; an alternative is a web system. If it is required to bring new functionality to a corporate application, then an integration problem arises since it will require the installation of new components and changing security settings. To solve this problem and facilitate the integration process, certification centers develop their APIs (API – Application Programming Interfaces) which help to provide secure access to their web systems without installing and configuring components via the Internet using HTTP/HTTPS network protocols.

The same problems can arise in document-oriented databases, where documents are contained in heterogeneous data sources or are generated ‘on the fly’ from several documents. Document-oriented storage may not have its own tools for working with an electronic digital signature; therefore, the connection to external RESTful services is required [3]. Here, document-oriented storage means the Situation-Oriented Databases (SODB) project [4], where currently there are no tools for working with electronic signature certificates, but there are heterogeneous document sources, where there are documents signed with an electronic signature that need to be verified. For a corporate system, the option of loading documents with unsigned signatures manually is laborious and cannot be applied, especially if the repository contains a significant number of documents. Under these conditions, it seems possible to use the capabilities of the SODB to work with RESTful services [5]. Since the development of data processing functionality focuses on a hierarchical situational model, this will require the model to be finalized to work with the cryptographic service API. This task is relevant for SODB. In the states of the model, such data processing regarding verification is in demand. All proposed solutions are tested on the current prototype of the educational web-based course design system in the course on databases.

Literature review

Analyzing publications in this subject area, it can be found that recently studies have been carried out on verifying the security of electronic signature protocols [6], and an algorithm has been developed for creating a digital signature with error correction when they are detected [7]. Upon considering publications on data processing in situation-oriented databases, it is evident that the research on generating blank drawings and filling them with information from the database, and the processing of various office documents was also studied [8]. Archives, web services, relational databases and other heterogeneous sources were used in the research [9-10]. These results were reflected in the modifications of the SODB architecture. A course was taken in the direction of the polyglot persistence approach [11-12] based on the capabilities of various services. In the future, this prompted to build a microservice-style architecture [13].

The emerging task of verifying electronic signatures in SODB was not considered at the previous stages of research, but conditions were definitely created for its solution. As part of the microservice style based on the polyglot persistence and situation-oriented approaches, it is already possible to work with external services via the Internet using cURL extension tools from the software development point of view. When objects are prepared with requests sent to the cryptographic service and data for authorization is returned as a response in order to send documents there and request any functions, receive reports on the work. The situation-oriented approach makes it possible to perform operations based on a hierarchical situational model, where these objects are prepared in states and heterogeneous document sources with their

detached signatures are processed. Then, using the mechanism of virtual multi-documents and virtual data arrays [14], documents and signatures are loaded for verification into a cryptographic service. Missing equipment elements, algorithms for such a specific task can be developed and provided in the interpreter and the hierarchical situational model. The task of operating cryptographic services was solved in many information systems. Here we can conclude that the study on this topic is relevant, the interest in tasks of this class during the development of information systems is emphasized.

Verifying electronic signatures of heterogeneous documents in a RESTful web service

Connection to various external services was previously considered in publications on SODB [12, 15]. In this paper, there are differences in that the connection is made to a cryptographic service, and authorization is required. These differences were reflected in the enlarged SODB microservice architecture, which displays the structural elements of the model, as well as the SODB module with the implemented software. The software has distinctive features, expressed in the fact that as part of the SODB architecture, it becomes possible, in accordance with the specifications in the states of the hierarchical situational model, to verify documents in a cryptographic web service using its API. Documents are uploaded to the cryptographic service along with check-out signature files. This will require the introduction of new elements to help structure the model. The proposed vision for the architecture developed and adapted to the verifying the signatures of electronic document tasks is shown in Figure 1, where two structural elements of the documents and signatures entered for setting are added to the left side. A document with associated signatures is located in a virtual data array and is loaded using data processing objects created in the model states. By invoking a pre-programmed cURL [16] extension, the functions for creating and sending an HTTP/HTTPS request are called in the interpreter. At the first stage, a connection is established to the identification service, which, in response to the data sent with the request for identification and the service level, issues an access token and its type.

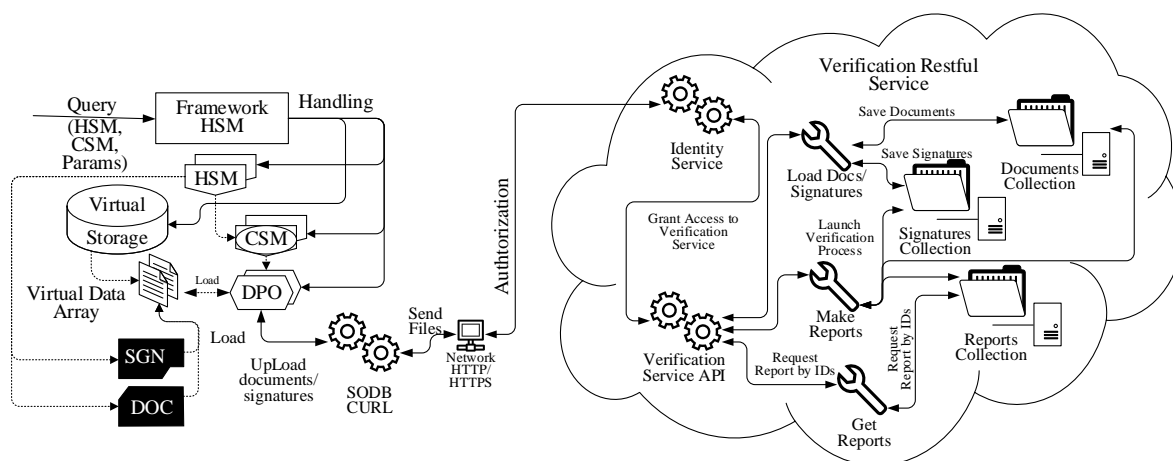


Figure 1 – SODB Architecture for verifying electronic signatures of heterogeneous documents
 Рисунок 1 – Архитектура СОБД для верификации электронных подписей гетерогенных документов

In the future, this response will be an integral part of other requests because the authorization data must be verified for each access to the cryptographic service functions. The next step after obtaining an access token involves downloading documents and their signatures using the implemented Verification Service API. Inside the cryptographic service, the documents and their signatures are recorded in the storage, and in response they are assigned

identifiers. They are included in the response for the SODB if there are no errors that occurred during the upload. The third step begins with obtaining the identifiers of the files uploaded for verification. In the verification state, a function is called that creates a report in the cryptographic service by the same mechanism using the cURL extension. The response of the cryptographic service contains the ID of the report to be requested. At the final stage, a request is sent, where the identifier of the report is indicated, according to which the SODB can receive a pdf-document containing the results of the electronic signature verification process.

SODB virtual multidocuments for working with a cryptographic service. To work with a cryptographic service, it is required to introduce a modified submodel of virtual multidocuments with new parameters introduced to it. Here it is necessary to introduce new attributes of virtual multi-documents to use the group of entry points and specialized options for the content. Virtual multi-documents are divided into two components – for authorization and for sending the contents of multi-documents and performing actions in the web service storage already filled with heterogeneous documents respectively. In one of the states, the specifications of virtual multi-documents are indicated that clearly describe heterogeneous data sources. Figure 2 shows a fragment of the model that describes the model of virtual multi-documents connecting the SODB with the cryptographic web service. The model is designed in the style of structuring through the use of `entry`-elements. This style was described in detail by the authors earlier in their research on the SODB [17]. The fragment of the model from Figure 2 shows the state of the Electronic Signature Verification model with two multi-documents `Identity` and `StampAPI`. The following is a description of the elements of their parameters used in the model, which were not introduced earlier and which are not involved in the processing of heterogeneous data.



Figure 2 – Specifying cryptographic service entry points as virtual multi-documents in the SODB model

Рисунок 2 – Задание точек входа криптографического сервиса в качестве виртуальных мульти-документов в модели СОБД

The Identity multidocument contains the entry point `host = "https://identity.testkontur.ru/connect/token/"` and the tail path `"grant_type=client_credentials&scope=Techno.Stamp"` of the HTTPS request in the first entry-element for obtaining identification data, and the second entry-element contains the authorization type Basic, the content type `Content-Type = "application/x-www-form-urlencoded"` and the secret key (here in Figure 2 its modified random version is shown as an example, the real key is not shown). The key is obtained from the service provider during registration of the client web application. Thus, it can be noted that this Identity multi-document serves for multiple authorization in a cryptographic service since authorization is performed with each request or action in the service.

The second StampAPI multi-document contains an additional but also key entry-point `host = "https://api.testkontur.ru/techno/stamp/v1/"` where documents and signatures are loaded. To load documents, the `LoadDocs` entry-element is provided with the tail contents of the entry point. The next step after the successful upload of documents and signatures is specified in the `MakeReport` multi-document with a different tail of the `reports` address of the entry point responsible for creating a report with the results of the verification procedure. The final step requires the presence of another path `path = "reports/'.$reportid.'/content [3]"` to get the report as a document. Here the `GetReport` entry-element is used, which provides verification results in a pdf-report. The input parameter for receiving a report is the report id, which is written to the `$reportid` variable. The options used for each tail of the entry point address are written to structural entry-elements and can be used to designate the type of content sent to the service. The types of content required to work with the cryptographic service from the example of the model fragment in Figure 2 are as follows:

- `Content -Type = "application/octet-stream";`
- `Content-Type = "application/json";`
- `Content-Type = "application/x-www-form-urlencoded".`

All options are written in their structural entry-elements and can be used in different states under named identifiers `Options1, Options2, Options3`.

Specifications of entry-elements in the SODB model for setting the verification of electronic documents and detached qualified electronic signatures

The doc and sgn-elements for specifying electronic documents and files of detached electronic signatures. The next important issue is the creation of virtual multi-documents provided with files of detached digital signatures. In this case, to specify a signed document, it is possible to use the already known `doc`-element, but a lot of signatures for the document makes its description cumbersome and inconvenient if the document has a lot of signatures. Based on the need for structuring, the `doc` element is modified with additional equipment and a new signature element with the name `sgn` and the graphical representation shown in the example in Figure 3 are introduced into the model. Here in Figure 3, the `sgn`-element named `SignPerson1` denotes the signature of a natural person with the type `type="sig"`, which denotes a detached digital signature. Existing elements do not allow the inclusion of digital signatures in processing and expanding processing methods by including the functionality of cryptographic web services. In this regard, new elements and parameters that did not previously exist in the SODB are introduced. Thus, a model of virtual multi-documents of a higher level of abstraction with the ability to work in a cryptographic web service, which has not been previously studied in SODB, is obtained and analogues of such a model have not been found in

modern conditions of search capabilities of scientific and technical information.



Figure 3 – Fragment of a model with a multi-document that structures the report and its signature with the newly introduced sgn-element

Рисунок 3 – Фрагмент модели с мультидокументом, структурирующим отчет и его подпись с новым введенным элементом sgn

Taking into account the requirements of the cryptographic service, the format="CMS/PKCS #7" parameter is added to the sgn-element. This parameter is important due to the fact that the service checks the signature format since signatures can be written in different formats, but not every service supports them.

In our example in Figure 3, the service supports document files no larger than 20 megabytes and signature formats:

- CMS/PKCS #7;
- CAdES-BES / CAdES-T;
- CAdES-C, CAdES-X Long, CAdES-X Type 1(2), CAdES-X Long Type 1(2), CAdES-A, CAdES-LT.

Data processing object for a multidocument authorization in a cryptographic service. A multi-document requires a data processing object in this case, Figure 4 shows an example of such a dpo-object, which indicates that the src data source named Identity is used.

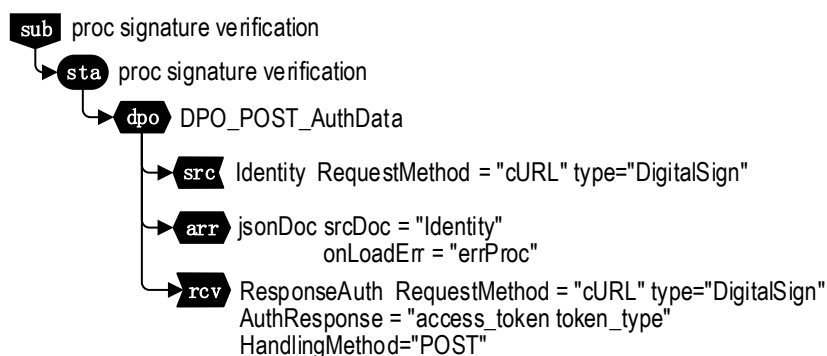


Figure 4 – A fragment of a hierarchical situational model with the state of verification of an electronic signature and a data processing object that solves the authorization task in a cryptographic service
 Рисунок 4 – Фрагмент иерархической ситуационной модели с состоянием верификации электронной подписи и объектом обработки данных, решающим задачу авторизации в криптографическом сервисе

Already existing data processing objects were not previously used for authorization with each call to the cryptographic web service; therefore, it was necessary to refine the model in terms of data processing objects for reuse in the authorization process. Thus, `dpo` have been moved to the scope of research of the SODB with cryptographic services. It is this object using the `cURL` method that sends a request for authorization in a cryptographic service. The request uses data in JSON format, this `arr`-element is specified. Thus, the identification data contained in the multi-document from Figure 2 using the data processing object in JSON format is sent by a request using the `HandlingMethod="POST"` method.

The response of the service is the `token_type` and `access_token` parameters. The first parameter is used to determine the type of token, and the second is an access token that gives access to all subsequent requests access to the functionality of the cryptographic service. For each subsequent request, authorization data is sent in advance, containing exactly the `access_token` token. The data received from the cryptographic service is placed in the `rcv`-receiver specified in the model named `ResponseAuth`.

The `dpo` data processing object in electronic signature verification tasks. In the tasks of verifying electronic documents, it will be necessary to equip the model with a specialized data processing object. By this, we mean its extended capabilities due to working with a multi-document model. A distinctive feature of such an object is its phased work – first with data loading operations, and then operating with loaded documents inside the cryptographic web service storage. Another distinguishing feature is that such a data processing entity uses an external cryptographic web service as a receiver and built-in functions based on multi-document specifications to operate on such a data receiver.

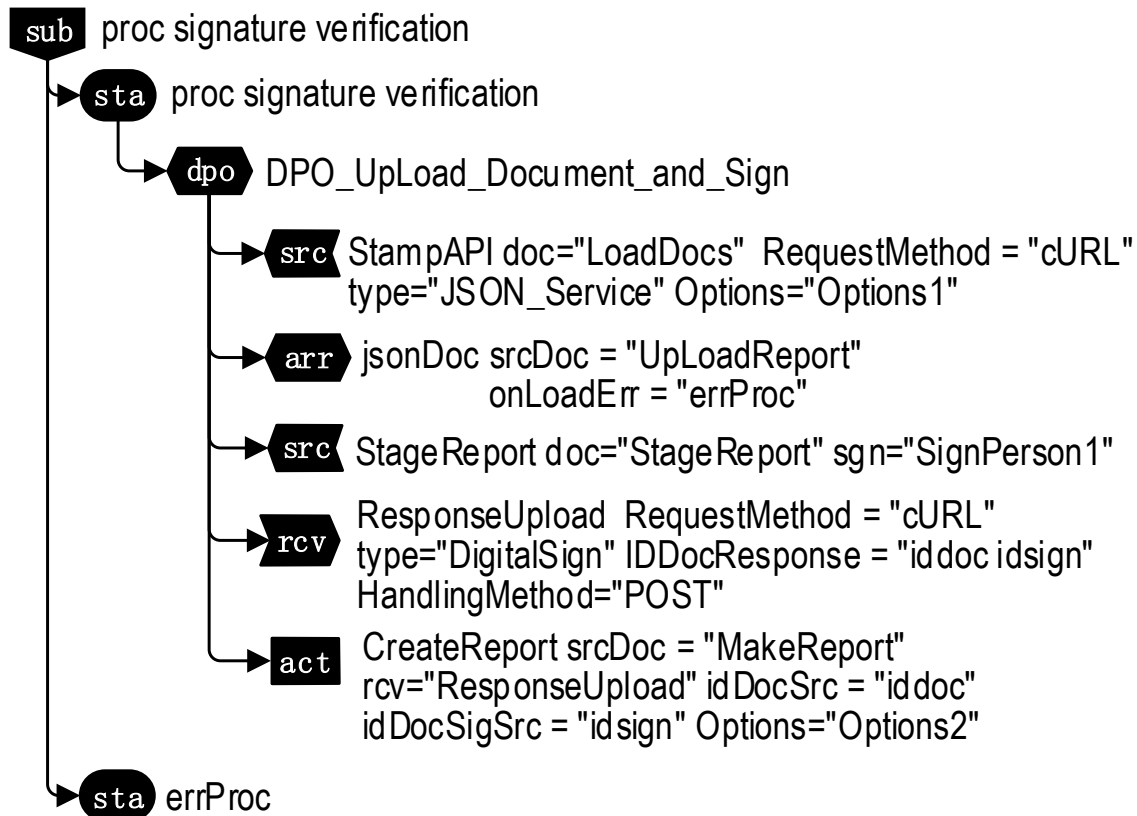


Figure 5 – Fragment of the model with an example of a data processing object at the first stage that loads a document along with a signature, and at the second stage launching the function of creating a report in a cryptographic service

Рисунок 5 – Фрагмент модели с примером объекта обработки данных на первом этапе, загружающего документ вместе с подписью и на втором этапе запускающего функцию создания отчета в криптографическом сервисе

Another key data processing object is a `dpo` named `DPO_Upload_Document_and_Sign`, which provides an extended description of several operations at once using heterogeneous data sources. The first operation concerns the uploading of the original signed document after authorization in the service. Here Figure 5 shows `dpo`-object with the `StampAPI` `src`-source sending the interpreter to the multi-document of the same name. The `doc="LoadDocs"` parameter involves the required document for processing; the source document file is loaded there, and the data processed invariantly [18] is in JSON format with the corresponding content type from the `Options="Options1"` parameter. A document can have several signatures in the model, one of them will be checked, in the figure for a signature, as well as for a multi-document, there is a source `src`-element for each signature. The signature is accessed through the document to which it refers, so the `StageReport` parameter is first specified in the source, this is the document that has this signature, and then the `sgn="SignPerson1"` parameter of the verified signature is specified. The part on uploading documents and signatures to the cryptographic service is limited to these elements and parameters, but there is also a response part, which will also be required later to create a report.

The response part is implemented in the `rcv`-element receiver of the model of the same data processing object. The `rcv`-element named `ResponseUpload` has the key parameter `IDDocResponse="iddoc idsign"`, it will contain the identifiers of the uploaded documents as a response, using these identifiers you can access the service's document store to

trigger the functions of the service. We immediately proceed to the action call – creating a report for uploaded documents and signatures, the figure shows the `act`-element with the name `CreateReport` responsible for actions. This action requires a source - a source multi-document with a specific tail for the entry point to be interpreted, here it is passed as a parameter `srcDoc="MakeReport"`. In response to an action, the SODB receives a result that is also expected in the initiating action, thus requiring the `rcv="ResponseUpload"` receiver element discussed earlier. The received parameters are indicated in the action by variables in the `idDocSrc` and `idDocSigSrc` parameters, and the action request uses the options of the `Options2` multidocument.

Data processing object for obtaining the results of the electronic signature verification process from the cryptographic service. To solve the problem the verification results obtaining of an electronic signature, you will need the `DPO_Download_Report` data processing object from Figure 6 with a fragment of the model.

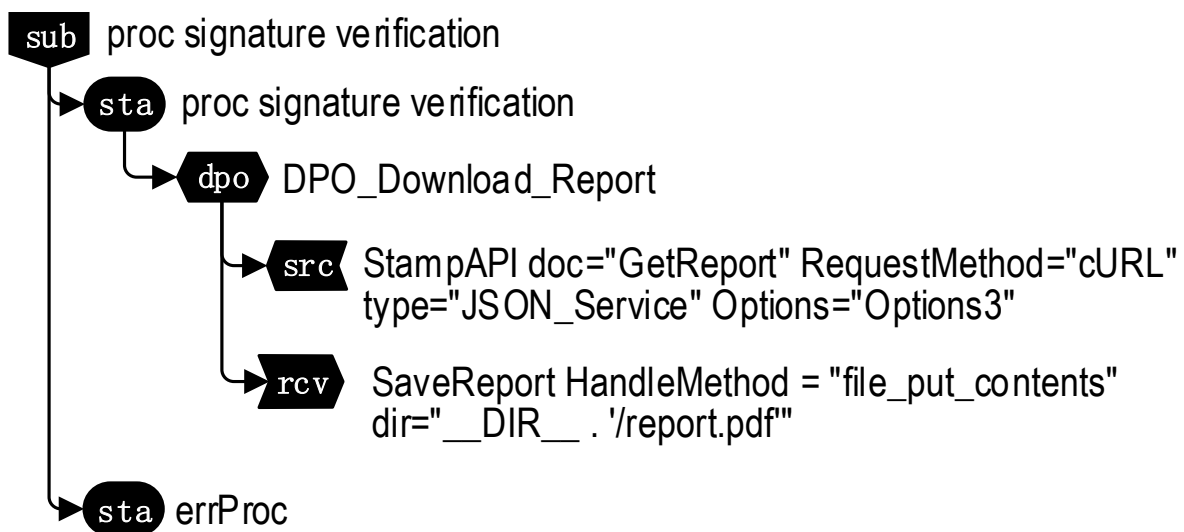


Figure 6 – Fragment of a hierarchical situational model of the SODB for downloading a ready-made report with verification results from a cryptographic service

Рисунок 6 – Фрагмент иерархической ситуационной модели СОБД для скачивания готового отчета с результатами верификации из криптографического сервиса

Here, a data processing object is introduced into the model, characterized in that it is functionally focused only on obtaining verification results and storing them in the internal storage of the SODB. After the execution of the action from the model fragment in Figure 5, reports with verification results are generated in the cryptographic service and stored in the data warehouse. To get them in SODB, the same `StampAPI` source is used, but with `Options3` options in the `Options` parameter. Saving the verification results in the SODB is provided by the `SaveReport` receiver `rcv`-element processing is carried out on the SODB server using the `HandleMethod="file_put_contents"` method to the specified directory `dir="__DIR__ ./report.pdf"`. The `__DIR__` parameter receives the current directory of the calling script, the downloaded report file itself saves the document under the name `report` in `pdf`-format. Further, such a report is provided to the user for display in the personal account.

A practical example of using the proposed model for verifying electronic signatures in SODB

At the Department of Automated Control Systems, the SODB project is being developed within the framework of which the tasks of course design in the discipline "Databases" are being solved [19]. The course design site functions as a research prototype and a real-life application based on the model in Figure 7.

The considered proposals for the process of verification of electronic signatures were implemented in the model shown in Figure 7, here is the part of the model that is directly involved in the verification process, the model of the entire application is much larger. The distinguishing features of this model in comparison with those already available in the SODB is its focus on working with cryptographic web services; previously, such models were not provided. The model is equipped with modified and new elements, as well as parameters for processing heterogeneous data sources present in the SODB. For virtual multi-documents, new structural entry-elements are provided, where it became possible to set entry points with special endings (tails) of the web service, allowing the SODB to perform authorization, upload documents with digital signatures, send requests to create verification reports and receive these reports in order to save them in SODB. Another distinguishing feature of a virtual multi-document is the presence of specialized "options" parameters that provide access to web service functions with different content types. A virtual multi-document specifying a document signed with an electronic digital signature has a new structural element `sgn`, which, unlike entry-elements, makes it possible to specify detached digital signatures. For each signature, a separate `sgn`-element is specified with a format parameter, and there can be such structural elements according to the number of document signatures.

In terms of data processing, the SODB model has distinctive features in `dpo` data processing objects, each of which is modified in accordance with its functional purpose. Introduced `dpo`, which fully provides the first stage of authorization of the verification process and stores authorization data for sending temporary credentials at subsequent stages of verification. Introduced `dpo`, which ensures the loading of the document and its signature, and if successful, performs an action in the document storage of the cryptographic web service to obtain identifiers both after the documents and signatures are loaded, and the report ID after it is created in the storage. Introduced `dpo`, specifying the receiver in the model for downloading and saving a report with verification results in the SODB storage.

To process such a model, the SODB framework is used, which implements the functionality for working with RESTful services and is framed and registered as a SODB module [20].

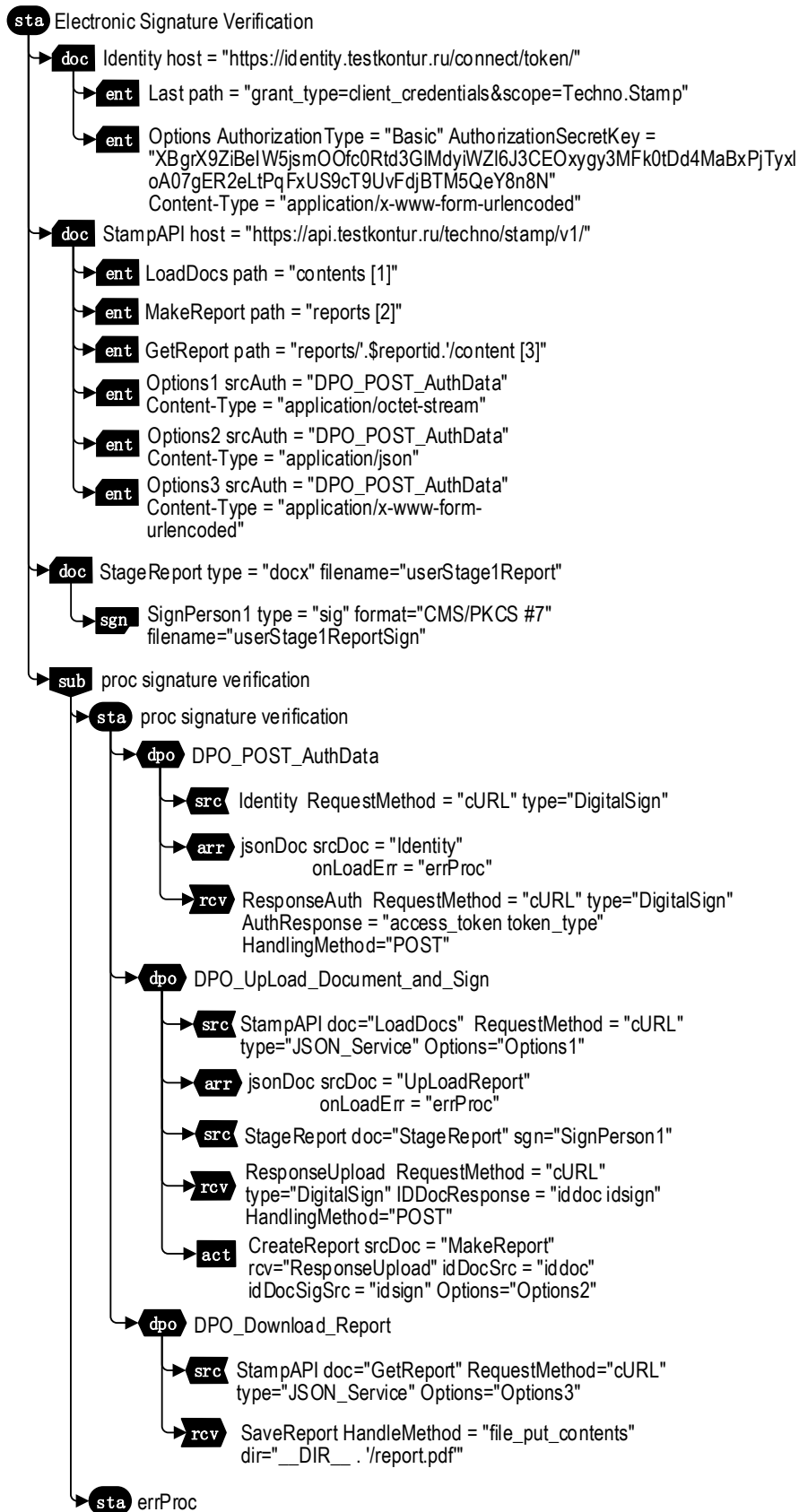


Figure 7 – General view of the hierarchical situational model of SODB for verifying electronic signatures of heterogeneous documents in a RESTful web service

Рисунок 7 – Общий вид иерархической ситуационной модели СОБД для верификации электронных подписей гетерогенных документов в RESTful-сервисе

The screen form with the output of the results of the electronic signature verification process is shown in Figure 8, where there is a protocol in pdf format embedded in the page of the user's personal account of the SODB website. The report confirms that the document was signed by the student of the group (student data has been changed). The following is full information about the certificate of the user who signed the explanatory note of the first stage of course design.

The screenshot displays the website interface for the 'Course Design' project. The main content area shows a PDF report titled 'Протокол проверки электронной подписи' (Protocol of electronic signature verification). The report details include:

- Протокол создан в 19 ноября 2020, 12:31:56 мск
- Подпись подтверждена
- Проверяемые файлы:

| | |
|------------------------------|----------------------------------|
| Исходный документ | Файл подписи |
| Этап_1_КП_Студент_055211.pdf | Этап_1_КП_Студент_055211.pdf.sig |
| Размер 100727 байт | Размер 30918 байт |
- Под документом поставлена 1 подпись:

| | |
|---------------------------------|--------------------------------|
| 1. Сертификат квалифицированный | Область применения сертификата |
| Иванов Иван Иванович | 1.3.6.1.5.5.7.3.2 |
| Иванов Иван Иванович | 1.2.643.2.2.34.6 |
| ИНН: ***** | 1.3.6.1.5.5.7.3.4 |

Figure 8 – Screen form of the "Course Design" website based on the SODB in the ‘Databases’ course. The report displays the results of the electronic signature verification (students' data has been changed)

Рисунок 8 – Экранная форма веб-сайта «Курсового проектирования» на основе СОБД по дисциплине «Базы данных» с отображением отчета результатами верификации электронной подписи (данные студентов изменены)

The developed software [19-20] differs in that it fully implements the multi-document model proposed in this paper for verifying the signatures of electronic documents. The relevance of this software is ensured during testing on real data in the prototype of the SODB used to accompany course design in the discipline "Databases". The work of students is divided into several stages in which database models are created, SODB generates office documents of drawing blanks. After filling out the blank document, the student signs it with an electronic digital signature and uploads the received files of the document and the detached digital signature to the SODB website. In this case, the printing of albums consisting of stages is not provided, this task in modern conditions is an auxiliary mechanism for academic mobility programs, as well as for students who have chosen distance learning in the discipline "Databases".

Conclusion

This article addresses the relevant issue of verifying electronic signatures of electronic documents with the examples of models of the current SODB prototype to support the course design project. This task is relevant in the context of using distant learning technologies and systems using heterogeneous data sources. Manual verification of documents is not possible without performing labor-intensive operations since the service requires the implementation of a client application, knowledge of programming as well as actions aimed at independently uploading documents and signatures to a cryptographic service with preliminary downloading of files to a hard disk. The article considers a model of a high level of abstraction to reduce the

complexity in the process of document verification. All work is transferred inside the system based on SODB, where all information about users and the documents themselves are stored, and routine operations are performed by calling a programmed module built into the SODB interpreter in application model states. The article also discusses the introduced security and new parameters, elements of the model for operating a cryptographic service. Thus, a situation-oriented approach makes it possible to avoid laboriousness while working with remote cryptographic services.

REFERENCES

1. Bartusek J., Carmer B., Malozemoff A.J., Jain A., Jin Z., Lepoint T., et al. Public-key function-private hidden vector encryption (and more). *Lecture Notes in Computer Science*. 2019;11923:489–519. DOI: 10.1007/978-3-030-34618-8_17.
2. Biyashev R.G., Nyssanbayeva S.E. Algorithm for creating a digital signature with error detection and correction. *Cybernetics and Systems Analysis*. 2012;48(4):489–497. DOI: 10.1007/s10559-012-9428-5.
3. Wilde E., Pautasso C. REST: From Research to Practice. Springer Science & Business Media; 2011. 528 p. DOI: 10.1007/978-1-4419-8303-9
4. Mironov V.V., Gusarenko A.S., Tuguzbaev G.A. Extracting semantic information from graphic schemes. *Informatika i avtomatizatsiya = Informatics and Automation*. 2021;20(4):940–970. DOI: 10.15622/IA.20.4.7. (In Russ.).
5. Mironov V.V., Gusarenko A.S., Yusupova N.I. Situation-oriented databases: polyglot persistence based on REST microservices. *Prikladnaya informatika = Applied Informatics*. 2019;14(5):87–97. DOI: 10.24411/1993-8314-2019-10038. (In Russ.).
6. Babenko L.K., Jose A. Sanchez. Verification of the security of the electronic digital signature protocol using AVISPA. *Voprosy kiberbezopasnosti = Cyber security issues*. 2017;20(2):45–52. DOI: 10.21581/2311-3456-2017-2-45-52. (In Russ.).
7. Biyashev R.G., Nyssanbayeva S.E. Algorithm for creating a digital signature with error detection and correction. *Cybernetics and Systems Analysis*. 2012;48(4):489–497. DOI: 10.1007/s10559-012-9428-5.
8. Mironov V.V., Gusarenko A.S., Yusupova N.I. Situation-oriented databases: processing office documents. *Modeling, Optimization and Information Technology*. 2022;10(2). Available from: <https://moitvvt.ru/ru/journal/pdf?id=1187> DOI: 10.26102/2310-6018/2022.37.2.021 (accessed on 25.11.2022).
9. Gusarenko A.S. Improvement of situation-oriented database model for interaction with Mysql. *Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie = Journal of Instrument Engineering*. 2016;59(5):355–363. DOI: 10.17586/0021-3454-2016-59-5-355-363. (In Russ.).
10. Mironov V.V., Gusarenko A.S., Yusupova N.I. Building of virtual multidocuments mapping to real sources of data in situation-oriented databases. *Communications in Computer and Information Science*. 2021;1204:167–178. DOI: 10.1007/978-3-030-78273-3_17.
11. Kolonko M., Mullenbach S., Polyglot Persistence in conceptual modeling for information analysis. In *ACIT'2020: Proc. 10th Int. Conf. on Advanced Computer Information Technologies*. 2020:590–594. DOI: 10.1109/ACIT49673.2020.9208928.
12. Mironov V.V., Gusarenko A.S., Yusupova N.I. Situation-oriented databases: polyglot persistence based on REST microservices. *Prikladnaya informatika = Applied Informatics*. 2019;14(5):87–97. DOI: 10.24411/1993-8314-2019-10038. (In Russ.).
13. Mironov V.V., Gusarenko A.S., Yusupova N.I. Monitoring YouTube video views in the educational environment based on situation-oriented database and RESTful Web Services.

- Sistemnaya inzheneriya i informatsionnye tekhnologii = Systems Engineering and Information Technologies*. 2021;3(1(5)):39–49.
14. Mironov V.V., Gusarenko A.S., Yusupova N.I. The Invariance of the Virtual Data in The Situationally Oriented Database When Displayed on Heterogeneous Data Storages. *Vestnik komp'yuternykh i informatsionnykh tekhnologii = Herald of Computer and Information Technologies*. 2017;(1(151)):29–36. DOI: 10.14489/VKIT.2017.01.PP.029-036. (In Russ.).
 15. Gusarenko A.S., Mironov V.V., Yusupova N.I. Stream processing of large documents in situationally oriented databases. In *ITIDS'2018: Proceedings of the 6-th International Conference Information Technologies for Intelligent Decision Making Support*. Ufa, USATU; P. 7–12. (In Russ.).
 16. Gusarenko A.S. Certificate of state registration of the computer program No. 2022617505. Situational database modules for extracting large documents and archives from RESTful services of heterogeneous data stores. 2022. (In Russ.).
 17. Mironov V.V., Gusarenko A.S., Yusupova N.I. Structuring Virtual Multi-Documents in Situationally-Oriented Databases by Means of Entry-Elements. *Informatika i avtomatizatsiya (Trudy SPIIRAN) = Informatics and Automation (SPIIRAS Proceedings)*. 2017;53(4):225–243. DOI: 10.15622/sp.53.11. (In Russ.).
 18. Mironov V., Gusarenko A., Yusupova N. Stream documents processing invariance in situation-oriented databases. In: *7th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS'2019)*. Atlantis Press; 2019:309–315. DOI: 10.2991/itids-19.2019.55.
 19. "Databases" course project. Available from: <http://hsm.ugatu.su/artem/dbproj/> (accessed on 20.10.2022) (In Russ.).
 20. Gusarenko A.S. Certificate of state registration of the computer program No. 2022615538. Microservice for verifying qualified electronic signatures of documents in situation-oriented databases. 2022. (In Russ.).

СПИСОК ИСТОЧНИКОВ

1. Bartusek J., Carmer B., Malozemoff A.J., Jain A., Jin Z., Lepoint T., et al. Public-key function-private hidden vector encryption (and more). *Lecture Notes in Computer Science*. 2019;11923:489–519. DOI: 10.1007/978-3-030-34618-8_17.
2. Biyashev R.G., Nyssanbayeva S.E. Algorithm for creating a digital signature with error detection and correction. *Cybernetics and Systems Analysis*. 2012;48(4):489–497. DOI: 10.1007/s10559-012-9428-5.
3. Wilde E., Pautasso C. REST: From Research to Practice. Springer Science & Business Media; 2011. 528 p. DOI: 10.1007/978-1-4419-8303-9
4. Миронов В.В., Гусаренко А.С., Тугузбаев Г.А. Извлечение семантической информации из графических схем. *Информатика и автоматизация*. 2021;20(4):940–970. DOI: 10.15622/IA.20.4.7.
5. Миронов В.В., Гусаренко А.С., Юсупова Н.И. Ситуационно-ориентированные базы данных: polyglot persistence на основе REST-микросервисов. *Прикладная информатика*. 2019;14(5):87–97. DOI: 10.24411/1993-8314-2019-10038.
6. Бабенко Л.К., Санчес Россель Х.А. Верификация безопасности протокола электронной цифровой подписи с помощью AVISPA. *Вопросы кибербезопасности*. 2017;20(2):45–52. DOI: 10.21581/2311-3456-2017-2-45-52.
7. Biyashev R.G., Nyssanbayeva S.E. Algorithm for creating a digital signature with error detection and correction. *Cybernetics and Systems Analysis*. 2012;48(4):489–497. DOI: 10.1007/s10559-012-9428-5.

8. Mironov V.V., Gusarenko A.S., Yusupova N.I. Situation-oriented databases: processing office documents. *Modeling, Optimization and Information Technology*. 2022;10(2). Available from: <https://moitvvt.ru/ru/journal/pdf?id=1187> DOI: 10.26102/2310-6018/2022.37.2.021 (accessed on 25.11.2022).
9. Гусаренко А.С. Усовершенствование модели ситуационно-ориентированной базы данных для взаимодействия с MySQL. *Известия высших учебных заведений Приборостроение*. 2016;59(5):355–363. DOI: 10.17586/0021-3454-2016-59-5-355-363.
10. Mironov V.V., Gusarenko A.S., Yusupova N.I. Building of virtual multidocuments mapping to real sources of data in situation-oriented databases. *Communications in Computer and Information Science*. 2021;1204:167–178. DOI: 10.1007/978-3-030-78273-3_17.
11. Kolonko M., Mullenbach S., Polyglot Persistence in conceptual modeling for information analysis. In *ACIT'2020: Proc. 10th Int. Conf. on Advanced Computer Information Technologies*. 2020:590–594. DOI: 10.1109/ACIT49673.2020.9208928.
12. Миронов В.В., Гусаренко А.С., Юсупова Н.И. Ситуационно-ориентированные базы данных: polyglot persistence на основе REST-микросервисов. *Прикладная информатика*. 2019;14(5):87–97. DOI: 10.24411/1993-8314-2019-10038.
13. Mironov V.V., Gusarenko A.S., Yusupova N.I. Monitoring YouTube video views in the educational environment based on situation-oriented database and RESTful Web Services. *Sistemnaya inzheneriya i informatsionnye tekhnologii = Systems Engineering and Information Technologies*. 2021;3(1(5)):39–49.
14. Миронов В.В., Гусаренко А.С., Юсупова Н.И. Инвариантность виртуальных данных в ситуационно-ориентированной базе данных при отображении на разнородные хранилища. *Вестник компьютерных и информационных технологий*. 2017;(1(151)):29–36. DOI: 10.14489/VKIT.2017.01.PP.029-036.
15. Гусаренко А.С., Миронов В.В., Юсупова Н.И. Поточковая обработка больших документов в ситуационно-ориентированных базах данных. В *ITIDS'2018: Труды 6-ой международной конференции по Информационным технологиями интеллектуальной поддержки принятия решений*. Уфа, Россия: УГАТУ; С. 7–12.
16. Гусаренко А.С. Свидетельство о государственной регистрации программы для ЭВМ № 2022617505. Модули ситуационно-ориентированной базы данных для извлечения больших документов и архивов из RESTful-сервисов гетерогенных хранилищ данных. 2022.
17. Миронов В.В., Гусаренко А.С., Юсупова Н.И. Структурирование виртуальных мультидокументов в ситуационно-ориентированных базах данных с помощью entry-элементов. *Информатика и автоматизация (Труды СПИИРАН)*. 2017;53(4):225–243. DOI: 10.15622/sp.53.11.
18. Mironov V., Gusarenko A., Yusupova N. Stream documents processing invariance in situation-oriented databases. In: *7th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS'2019)*. Atlantis Press; 2019:309–315. DOI: 10.2991/itids-19.2019.55.
19. Курсовой проект «Базы данных». Доступно по: <http://hsm.ugatu.ru/artem/dbproj/> (дата обращения: 20.10.2022).
20. Гусаренко А.С. Свидетельство о государственной регистрации программы для ЭВМ № 2022615538. Микросервис верификации квалифицированных электронных подписей документов в ситуационно-ориентированных базах данных. 2022.

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Гусаренко Артем Сергеевич, кандидат технических наук, доцент кафедры Автоматизированных систем управления, Уфимского университета науки и технологий, Уфа, Российская Федерация.
e-mail: gusarenko.as@ugatu.su
ORCID: [0000-0003-4132-6106](https://orcid.org/0000-0003-4132-6106)

Artem Sergeevich Gusarenko, Candidate of Technical Sciences, Associate Professor at the Department of Automated Control Systems, Ufa University of Science and Technology, Ufa, Russian Federation.

Статья поступила в редакцию 05.12.2022; одобрена после рецензирования 19.12.2022; принята к публикации 28.12.2022.

The article was submitted 05.12.2022; approved after reviewing 19.12.2022; accepted for publication 28.12.2022.