IRSTI 81.93.29

Software implementation of two-factor authentication to ensure security when accessing an information system

Ussatova O.A., Al-Farabi Kazakh National University,
Almaty, Kazakhstan, E-mail: olgaussatova@gmail.com
Nyssanbayeva S.E., Institute of Information and Computational Technologies,
Almaty, Kazakhstan, E-mail: sultasha1@mail.ru
Wojcik W., Lublin University of Technology,
Lublin, Poland, E-mail: waldemar.wojcik@pollub.pl

The article describes methods for applying two-factor authentication (2FA). An example of two-factor authentication using mobile devices as identifiers and the generation of a temporary password based on the hash function of encryption standards is considered. For an automated control system, a two-factor authentication model and a sequential algorithm for generating a temporary password using mathematical functions have been developed. Mathematical function is selected from the array of functions. To protect the opening of a one-time password, a secret string is read, consisting of a sequence of characters that will be generated randomly. Implemented software implementation on the Node.js software platform using the JavaScript programming language, as well as frameworks and connected system libraries. A document-based database management system with open source MongoDB, using for storing and processing information. The analysis of the software implementation of the proposed algorithm.

Key words:two-factor authentication, data security, one-time password (OTP) generation, security methods, mobile application, smartphone.

Ақпараттық жүйеге қол жеткізу кезінде қауіпсіздікті қамтамасыз ету үшін екі факторлы аутентификацияны бағдарламалық қамтамасыз ету

Усатова О.А., әл-Фараби атындағы Қазақ ұлттық университеті,
Алматы қ., Қазақстан Республикасы, olgaussatova@gmail.com
Нысанбаева С.Е., Ақпараттық және есептеу іштехнологиялар институты,
Алматы қ., Қазақстан Республикасы, sultasha1@mail.ru
Войцик В., Люблин техникалық университеті,
Люблин қ., Польша, waldemar.wojcik@pollub.pl

Мақалада автоматтандырылған басқару жүйесіндегі екінші факторға негізделген түпнұсқаландыруды қолдану әдістері сипатталған. Ұялы құрылғыларды идентификаторлар ретінде пайдалану негізінде екі факторлы түпнұсқаландырудың мысалы, сондай-ақ, шифрлау стандарттарының хэш функциясына негізделген уақытша құпия сөзді генерациялау мысалы қарастырылады. Автоматтандырылған басқару жүйесі үшін екі факторлы аутентификациялау моделі жасалды. Математикалық функцияларды пайдалана отырып, уақытша құпия сөзді генерациялау үшін дәйекті алгоритм сипатталады.Математикалық функция функциялардың массивінен таңдалады. Бір мәртелік парольдің ашылуын қорғау үшін құпия жолды оқып, кездейсоқ пайда болатын таңбалар тізбегінен тұратын оқылады. Node.js бағдарламалық платформасының бағдарламалық жасақтамасы JavaScript бағдарламалау тілінің көмегімен, сондай-ақ шеңберлер мен қосылған жүйелік кітапханалар арқылы жүзеге асырылды. Ақпаратты сақтау және өңдеу үшін Open source MongoDB бар құжатқа негізделген дерекқорды басқару жүйесі қолданылады. Ұсынылған алгоритмді бағдарламалық қамтамасыз етуді талдау.

Түйін сөздер:екі факторлы түпнұсқалық растама, деректерді қорғау, бір жолғы парольді генерациялау, қауіпсіздік әдістері, мобильді қосымша, смартфон.

Программная реализация двухфакторной аутентификации для обеспечения безопасности при доступе к информационной системе

Усатова О.А., Казахский национальный университет имени аль-Фараби,
г. Алматы, Республика Казахстан, E-mail: olgaussatova@gmail.com
Нысанбаева С.Е., Институт информационных и вычислительных технологий
г. Алматы, Республика Казахстан, E-mail: sultasha1@mail.ru
Войцик В., Люблинский технологический университет,
г. Люблин, Польша, E-mail: waldemar.wojcik@pollub.pl

В статье описаны методы применения аутентификации на основе второго фактора. Рассмотрен пример двухфакторной аутентификации с использованием мобильных устройств в качестве идентификаторов и генерации временного пароля на основе хеш-функции стандартов шифрования. Для автоматизированной системы управления разработаны модель двухфакторной аутентификации и последовательный алгоритм генерации временного пароля с использованием математических функций. Математическая функция выбирается из массива функций. Для защиты вскрытия одноразового пароля считывается секретная строка, состоящая из последовательности символов, которая будет генерироваться случайным образом. Осуществлена программная реализации напрограммной платформе Node.js с использованием языка программирования JavaScript, а так же фреймворков и подключенных системных библиотек. Использована документоориентированная система управления базами данных с открытым исходным кодом MongoDB, для хранения и обработки информации. Проведен анализ программной реализации предложенного алгоритма.

Ключевые слова: двухфакторная аутентификация, безопасность данных, генерация одноразового пароля, методы безопасности, мобильное приложение, смартфон.

1 Introduction

Crimes increasing in the digital environment and cases of Internet hackers is one of the trends in today's world. For many users, online security, the safety of usernames, usernames and passwords is crucial. This article discusses a two-factor authentication model based on a mobile application and an authentication program. Two-factor authentication, also known as 2FA, has become relevant in the current digital age. When choosing two different channels for authentication, it becomes possible to protect user logins from remote attacks, the purpose of which is to use other people's personal or identification data [1]. Two-factor authentication is an additional layer of security, which is called "multifactor authentication." 2FA requires not only input an user name and password, but also the use of such information that only the author knows or which will immediately be available only for the author [2].Such information may include what you know (for example, a unique username and password), belongs to you (for example, a smartphone with an application to confirm the authentication request) or part of you (for example, biometric data - fingerprint or scan retina). So, the first factor may be a password, and the second factor is what is sent via the app or notification to your smartphone for confirmation. In the modern world, more than 5 billion mobile devices are used, and using the phone as an authentication tool helps to quickly solve the problem of enhanced protection, reduction of additional costs and delivery delays. The problem of information leakage is related to the modern world and the usingof information protection serves as an additional barrier for intruders. Two-factor authentication methods are considered as mechanisms for enhancing the strength of authenticators [3-5]. Two-factor protection is a fairly reliable barrier, seriously complicating access to other people's data

and to some extent leveling the disadvantages of classic password protection. This article describes the results obtained when developing a two-factor authentication model based on an application using a smartphone:
- analysis of security procedures and information leakage;
- developed a two-factor authentication model based on a smartphone;
-an algorithm for an authenticator application using a smartphone for two-factor authentication has been developed and implemented in software.

2 Literature review

According to a study of Verizon's Data Security Incidents Report (DBIR) in 2018, 95 percent of violations involve the use of stolen personal data [6]. Standard security procedures, especially online, require simple input of a username and password, and criminals can easily take possession of personal user data — personal and financial information — in order to use it further to commit fraud, mainly in the financial sector.
According to SearchInform, in 2018, 66 percent of Russian companies and 70 percent of foreign companies faced information leaks (Figure 1) [7].

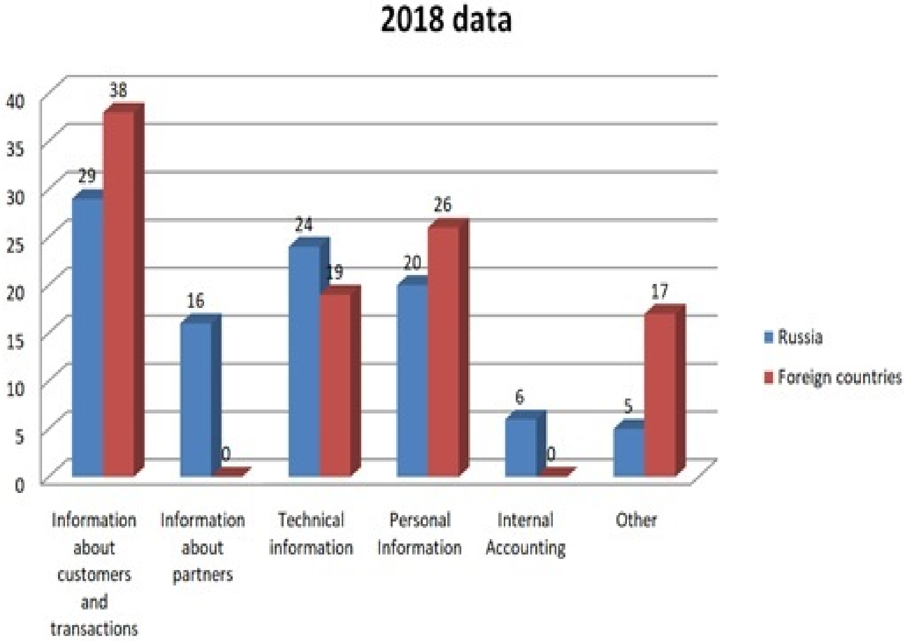

Figure 1: Data on information leaks for 2018

As can be seen from the above data, this problem is relevant for the whole world. A large percentage of leakage accounted for customer and transaction information, technical information, as well as personal data. Unfortunately, some companies hide the incident and do not make any notifications about information leaks in their companies. Thus, the problem arises of protecting confidential information from malicious attacks. One of the means of protecting information is password protection using the second factor. Two-factor authentication from

Infobip solves this problem with the help of SMS messages sent to a mobile phone and Voice technologies [8]. Using SMS as the second authorization factor is not the safest solution. There can be only one phone number, and therefore we will have one confirming device: -if you are in the area of uncertain reception, SMS - the message from the service may not come;
-the number can be stolen along with the phone or try to make a duplicate of it for authorization instead of you;
-there may be problems with authorization when traveling abroad, for example, SMS - a message comes for a long time, roaming does not work or you decide to use local instead of a native card.
All these inconveniences can be forgotten when using special services and applications that may be the second factor of authorization. The proposed authentication method is an application authenticator, which runs on a mobile device associated with the server. The mobile device in the proposed method will be connected to the server by the unique MAC address of the phone. The MAC Address (Media Access Control) is the device ID for the Wi-Fi network. MAC - address will identify the user in this system. This type of authentication is the most secure, convenient and cost effective to use. When authorization is required in the service, not only a login and password is entered, but also a 6-digit one-time confirmation password generated on the server. The validity period determines the period of activity of a one-time password after its generation. Password can be confirmed in the specified time frame. Upon expiration of the one-time password and its verification will become impossible. When theold password is canceled, you must request a new one-time password. Verification attempts represent the total number of password verification requests at a predefined time interval. If re-confirmation of the password is requested before the expiration of the time interval, verification will become impossible. It is necessary that the predefined time interval for confirmation expires, and the attempt to confirm the password can be made again. The length of the acknowledgment interval represents a predefined time interval in which several confirmation attempts cannot be made. The password is generated automatically when the program is started and is valid for 20 seconds from the moment of creation.

3 Material and methods

The proposed authentication method is implemented using a client-server network architecture. This is a client-server application developed on the Node.js software platform using the JavaScript programming language, as well as frameworks and connected system libraries. Node.js is a server platform for working with JavaScript through the V8 engine. JavaScript performs the action on the client, and the node performs on the server. For the JavaScript language, the jQuery framework, is a library with ready-made visual effects, AJAX requests and other useful things. The framework defines the rules for constructing the architecture of the application by defining at the initial stage of development the default behavior - “framework”, which will need to be expanded and modified according to the specified requirements. To implement the application, you need a smartphone that will display the generated one-time password to identify the user in the system. The application is designed for the Android operating system. According to statistics, the Android OS uses 85.9 percent of users [9], which determined its choice for the implementation of the proposed method. The scheme of the method is attached to Figure 2.

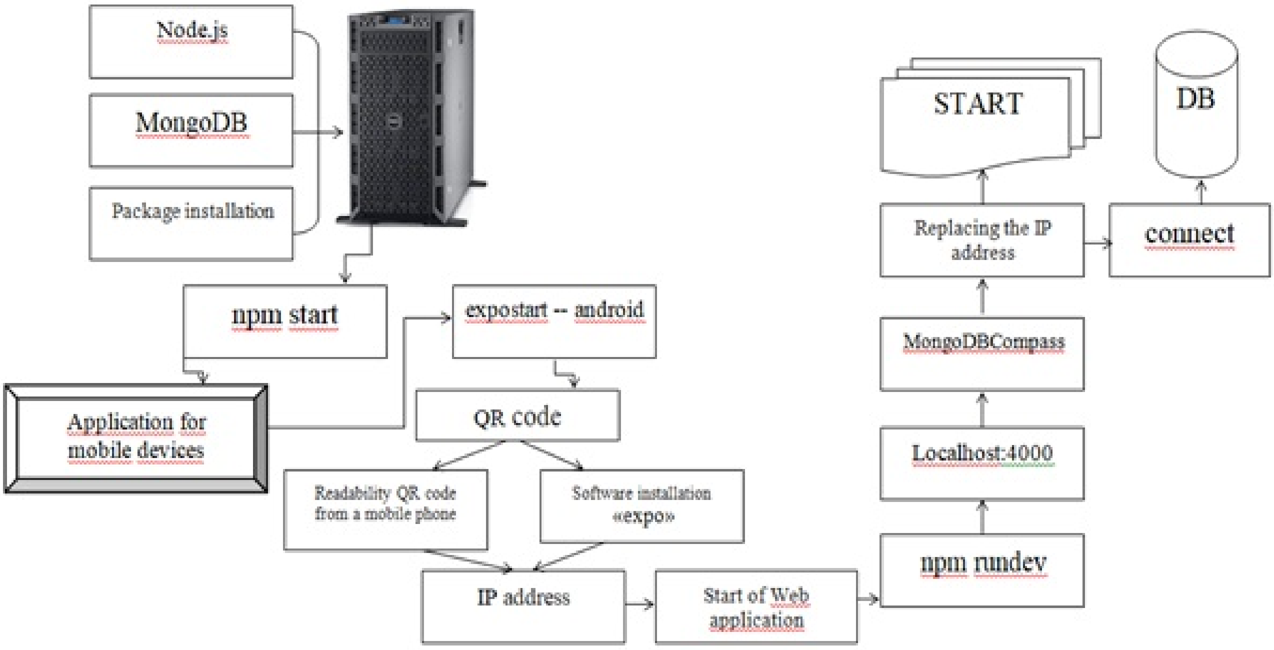

Figure 2: Scheme of implementation of the proposed two-factor authentication system

The developed model is based on two types of two-factor authentication: an authenticator application and input verification with using a smartphone. Node.js are used to implement the system. This software platform is responsible for writing the server part in the programming language JavaScrript. Together with it comes the package manager npm, which is used to install various libraries and frameworks.Additionally, you need to install MongoDB - a document-based open-source database management system that does not require a description of the table schema. When complex queries occur, they are usually solved on the application side, which makes it easier to work with data and links to them. The use of this database management system (DBMS) is due to the fact that rather simple scalability is built into this system using sharding technology, which makes the partitioning (partitioning) of the database into separate parts so that each of them can be transferred to a separate server [10].

The advantage of using MongoDB DBMS is:
- increase the speed of development;
- there is no need to synchronize the schema in the database and application;
- understandable path to scalability;
- simplicity of prescribed solutions.

To work with Mongo, a “data” folder is created on the “C” drive, and the “db” folder is created in it. To install the packages required to run certain parts of the project (“Server”, “devschacht”, “dip”), open the console in the folder with the package.json file and run the “npm install” command in it. After installing all the packages, the project is launching for execution in parts. In the beginning, the “Server” starts. To do this, go to the folder, open the

console and execute the "npm start" command. After starting, the message "server started" appears. Next, the mobile application is launched via the "devschacht" folder, in which the console opens and the "expostart - android" command is launched. After launch, a QR code will appear in the console. Also, a tab with system information and a QR code will open in the browser. The field with the IP address above the QR code must be remembered. For successful work, replace the IP addresses in the code with the one written in the tab in the following files:
Dip—> src—> server.js (line 79)
Server—> index.js (line 225)
Devschacht—> App.js (line 17)
In order for the mobile application to work, it is necessary to read the QR code, which can be performed using the installed scanner on the mobile device by default or installing additional software "EXPO". To start the smartphone and personal computer, the local network is configured so that they are in the same network. Then the web site starts, the console opens, and the npm rundev command is executed. For the operation of the web application, the port 4000 is "localhost: 4000". To view the contents of the database, you need to install MongoDBCompass and make connections by clicking the "connect" button. After saving all changes to the settings, the main parts of the system are restarted, which means the completion of the formation of the 2FA system for use.

4 Results and discussions

Consider an example of the proposed information protection system using a combination of two factors: permanent and temporary passwords [11]. The user chooses a permanent password (the first factor) himself and uses it when registering an account (account). Before authorization must be registered in the application. After that, the application starts to enter user data (login and password), which must correspond to the registered data. Then you need to enter the application on your smartphone and enter the initial data to generate a temporary password. A one-time or temporary password (the second factor) is generated on the server according to the proposed algorithm [8] and is valid for a specific length of time for one authentication session. The advantage of a one-time password is that the password is not reused. Thus, an attacker who intercepted data from a successful authentication session cannot use the copied password to gain access to the protected system. The generation of a temporary password is possible online. To obtain a temporary password, additional software is used (Figure 1). The software sends a request to the authorization server to generate a temporary password. This temporary password is generated on the server and displayed to the user in additional software on the smartphone. This temporary password has a short duration of 20 seconds. The temporary password is generated based on the result of the selected trigonometric function, which has a number of variable parameters. The trigonometric function is combined into a table, the dimension of 256x256 is a multiple of degree two. The choice of this function and its initial parameters is based on the result of the hash function of the SHA256 standards [12,13]. This is a cryptographic hash function developed by the US National Security Agency [14].The purpose of the hash function is the transformation (or hashing) of an arbitrary set of elements in the data into a fixed-length value. This value will

characterize the set of source data without the possibility of extraction. The input string for the hash function is a combination of user credentials, the current Greenwich Mean Time, and an additional secret string. The result of the hash function is divided into individual numbers, which will be the indices for selecting the function and its initial data. The secret string is a required field that will be randomly selected from the array. The secret line at each input is named, which makes it much more difficult to open the initial input line, which allows you to further strengthen the protection. The initial data for the input string will be the following values:
- Login: olga
- Password: pass17word
- Current moment: 2019 02 21, 11:54:25
- Secret line: salt
The input line will look like:
olgapass17word20190221115425salt
The result of the SHA256 hash function is as follows:
2AA878BD4D10F5861B9A2096DCC22222E5C0EB6766A1079581EDA00C0C27B99B
The first symbols of the result are used to select a mathematical function. Then the index of the function in the table with the size of 256x256 will be the following (42, 168), as the decimal representation of the hexadecimal numbers 2A, A8. By this index, the function will be selected and its parameters will be determined. Two hexadecimal numbers from the end of the hash function are used as initial parameters, and a hexadecimal number from position 10 is used as the "x" value. Based on the results of the calculation, the numbers after the comma are taken from the 5th position and the length in 6 digits. Then the temporary password will be the number that must be entered into the application (Figure 3).

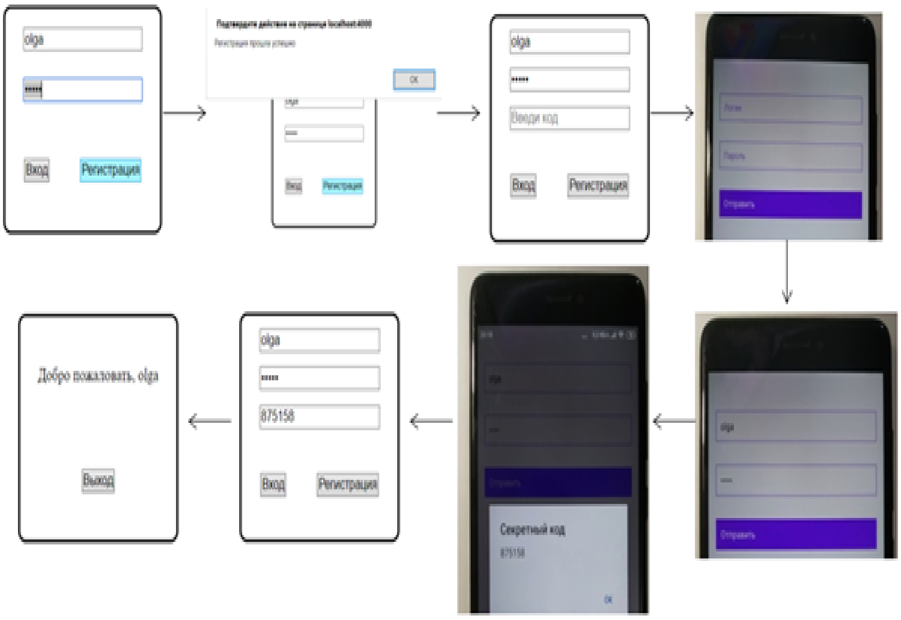

Figure 3: Software implementation

Consider the effect of generating a temporary password on the software implementation of information security tools based on two-factor authentication. For assessment of the sgenirovanny temporary password, different input data that show efficiency of realization of an algorithm were taken. Table1 shows the results of the study of the generation of a temporary password according to the algorithm described above.

Table 1: Generating a temporary password using this algorithm

Input data	Mathematical function	Hash - value	Password generated
login1 pas123 2019325132850 secret	((Math.pow(Math.cos (Math.pow(x,2)),3) + Math.tan(c) * Math.pow (Math.sin(Math.PI * p1),4)) /Math.sqrt(p2))	320943960B 777D0654539D 97B00565B950CBD77B 4B5F93BBDDA EA31F82C59427	432027
login1 pas123 2019325133815 secret	((y * Math.pow(Math.sin (p1),2) + 4 * Math.pow (Math.tan(x),4)) * c)	16C645887AB 5726CA912041FC 3AE3339A03B 0223603A4D4C81F 42942ED0510C3	578476
user123 password456 201932513328 wer	(Math.sqrt(a) * Math.sin(b + Math.PI/y))	5617AB08E76F 629353D8BD6579365 CA712D459D5B982 BF9D43DC4CBDB4 CFF1EC	839447
pinokio qwert 201932513346 asdf	((c * Math.pow(Math.sin(x),3) + 3 * Math.pow(Math.cos(x), 2))/p2)	33CADE53484F221 3E2266390588E381 468B61D831ABCCF F36A23770814411952	586576
new poiuyt 2019325133620 confidentially	((Math.pow(Math.cos(Math. pow(x,2)),3) + Math.tan(c) * Math.pow(Math.sin(Math.PI * p1),4))/Math.sqrt(p2))	6EEF6A6F907ACC FF8278BFE986A54 F9354A214A40C8D 7906C6DDFC294C1D7EFB	417266

The analysis of the work showed that the software implementation corresponds to the described model and algorithm. The developed client-server application works correctly, the generated one-time password is not repeated and changes even when entering duplicate data. The proposed two-factor authentication method can, is an additional means of protecting information stored in the system.

5 Conclusion

The use of two-factor authentication allows you to enhance the protection of information. The proposed algorithm will eliminate the existing disadvantage of using two-factor authentication based on SMS - messages, since the proposed method uses two types of two-factor authentication: the authenticator application and input verification using a smartphone based on the client-server application. The software implementation of the proposed method shows that the considered algorithm works correctly and corresponds to described above.

References

[1] Wang D., Wang P., Ma C., Chen Z., "Robust smart card based password authentication scheme against smart card loss problem. Cryptology ePrint Archive" , *IEEE transactions on dependable and secure computing* 15(2018): 708-722.

[2] Wang D., He D., Wang P., Chu C.H., "Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment." , *IEEE Trans. Depend. Secur. Comput.* 4(2015): 428-442.

[3] Amin R., Islam S., Khan M. K., Karati A., Giri D., Kumari S., "A two-factor rsa-based robust authentication system for multiserver environments." , *Security and Communication Networks.* vol. 2017, Article ID 5989151, (2017): 15.

[4] Han L. et al., "An efficient and secure two-factor authentication scheme using elliptic curve cryptosystems." , *Peer-to-Peer Networking and Application.* vol. 11(12), (2016): 11.

[5] Xie Q., Wong D. S., Wang G., Tan X., Chen K., Fang L., "Provably secure dynamic id-based anonymous two-factor authenticated key exchange protocol with extended security model." , *IEEE Transactions on Information Forensics and Security.* vol. 12, (2017): 1382-1392.

[6] "Data Breach Investigations Report 2018."last accessed January 10, 2019, https: www.verizonenterprise.com-resources-reports-rp-DBIR-2018-Report-execsummary-en-xg.pdf.

[7] "Providing information security."last accessed January 25, 2019, https: searchinform.ru.

[8] "Two-factor authentication."last accessed January 10, 2019, https: www. infobip.com-ru-glossariy-dvukhfaktornaya - autentifikatsiya.

[9] "iOS and Android already occupy 99.9 of the market for mobile operating systems."last accessed January 27, 2019, https: www.ixbt. com-news-2018-02-24-ios-android-99-9.html.

[10] "MySQL and MongoDB - when and what is better to use."last accessed February 02, 2019, https: habr.com-ru-post-322532.

[11] Nyssanbayeva S. , Ussatova O., "Dvuhfaktornaja autentifikacija v avtomatizirovannoj sisteme upravlenija,"["Two-factor authentication in the automated control system"], [the III International scientific conference "Information Science and Applied Mathematics"] , *DAN USSR* vol. 2, no 2 (2018): 239-242.

[12] "National Institute of Standards and Technology (NIST)."last accessed January 10, 2019, https: www.nist.gov.

[13] "FIPS 140-2 standard and self-encryption technology."last accessed January 10, 2019, https: www.seagate.com-files- www-content -solutions-content -security-and-encryption -id - docs - faq-fips-sed-lr- mb-605-2-1302-ru.pdf.

[14] "National Security Agency ."last accessed January 10, 2019, https: www. cryptomuseum.com-intel-nsa-index.htm.