SATBAYEV UNIVERSITY

Computing & Engineering

Volume 2 (2024), Issue 1, 7-13

https://doi.org/10.51301/ce.2024.i1.02

Research and development of a multi-factor authentication system for a document management system

A. Akhmetova*

Satbayev University, Almaty, Kazakhstan

**Corresponding author: akhmetova.aidanaa@gmail.com*

Abstract. The article discusses the development and research of a multi-factor authentication (MFA) system for document management systems. Attacks that threaten document management systems are described, and methods for developing an MFA system to prevent these attacks are proposed. A comparative analysis of multifactor authentication with other authentication systems has been carried out, as well as methods for developing multifactor authentication have been investigated. Two popular types of multifactor authentication that can be used in the document management system were compared. To verify the developed MFA system, it is necessary to conduct testing and audit. Conducting research ensures high security for the document management system, compliance with regulatory requirements, and vulnerability prevention.

Keywords: *multifactor authentication, accessibility, workflow, integration, password, biometrics, encryption, protocol*.

1. Кіріспе

Қазіргі кезде құжат айналымы жүйесі іс жүзінде әрбір ұйымның ажырамас бөлігіне айналды. Бүгінгі құжат айналымы – кәсіпорынның ақпараттық технология инфрақұрылымының маңызды құрамдас бөлігі. Бұл жұмыста үнемі қолданылатын құжаттардың саны күн сайын тез өсіп келе жатқандығына байланысты. Олардың барлығын жедел және сапалы өңдеу қажет. Құжат айналымы жүйесі – құжаттарды, сондай-ақ кәсіпорынның ұйымдастырушылық процестерімен байланысты құрылымдалмаған контентті жинақтауға, сақтауға, басқаруға және жеткізуге арналған стратегияларды, әдістер мен құралдарды қамтитын жүйе [1]. Электронды құжат айналымы жүйелері құжаттардың кәсіпорын ішінде және сыртында ақпараттық және коммуникациялық технологиялар негізінде қатаң реттелген және формалды бақылаудағы қозғалысын қамтамасыз етеді [2]. Электронды құжат айналымы жүйесінде құжаттармен жұмыс істеудің толық циклін орындауға болады: құру, өңдеу, жіберу, танысу, үйлестіру, құжаттар бойынша тапсырма беру, олардың орындалуын бақылау, құжаттарға қол қою (электрондық цифрлық қолтаңба арқылы), тіркеу, мұрағатқа тапсыру, сақтау (әртүрлі форматтарда: мәтіндік, графикалық) және берілген мерзім бойы пайдалану немесе жою [2]. Құжат айналымы жүйесіне арналған көп факторлы аутентификация жүйесін әзірлеу қосымша қорғаныс қабатын қосады, бұл пайдаланушылардан қол жеткізгенге дейін бірнеше тексеру формаларын ұсынуды талап етеді. Бұл ұрланған немесе әлсіз құпия сөздердің салдарынан рұқсатсыз кіру қаупін азайтады. Көп факторлы аутентификация рұқсат етілмеген адамдардың құпия ақпаратқа қол жеткізу мүмкіндігін айтарлықтай төмендетеді [3].

Құжат айналымы жүйесінде бірнеше аутентификация деңгейлерін пайдалану арқылы, тіпті бір элемент бүлінген немесе өшірілген болса да, пайдаланушы тіркелгісі қауіпсіз болып қалады. Құжат айналымы жүйесіне арналған көп факторлы аутентификация жүйесін тестілеу жүйенің қаншалықты жақсы жұмыс істейтінін және құпия ақпаратты қорғайтынын көрсетеді [3].

Құжат айналымы жүйесіне қауіп төндіретін шабуылдар

Құжаттарды басқарудың заманауи жүйесі көбінесе іздеудің кешенді мүмкіндіктерін, метадеректерді белгілеуді, қол жетімділікті бақылауды және файлдарды қорғауға арналған сенімді қауіпсіздік процестерін ұсынады [4]. Құжат айналымын енгізудің мақсаты – бірнеше пайдаланушылардың бірыңғай өзара байланысты деректер базасымен бірлескен жұмысы кезінде кәсіпорынды басқарудың және оның жұмыс істеуінің тиімді ортасын құру [5].

Құжаттарды басқару жүйесіне әртүрлі қауіптер төнуі мүмкін. Қауіптер рұқсатсыз қол жетімділікке, деректерді жоюға және өзгертуге, құпиялылыққа, тұтастыққа қауіп төндіруге бағытталады. Құжаттарды басқару жүйесінің жеткілікті деңгейде қорғалмауы салмақты салдарларға алып келуі мүмкін, мысалы, құпия деректердің таралуы, серіктестер мен клиенттердің сенімінің бұзылуы, қаржылық шығындар және беделдің жоғалуы [6].

Құжаттарды басқару жүйесіне арналған негізгі қауіптер 1-кестеде көрсетілген. Құжаттарды басқару жүйесіне арналған негізгі қауіптер [7] дереккөзіне негізделген.

Кесте 1. Құжаттарды басқару жүйесіне арналған негізгі қауіптер [7]

Қауіптер	Сипаттама	Мақсат
Тұтастыққа қауіп	Деректердің бүлінуі, жойылуы немесе бұрмалануы	Қасақана немесе қасақана емес түрде деректерге зиян тигізу
Құпиялылыққа	Құпия ақпараттардың	Қасақана түрде ұрлық,

қауіп	рұқсатсыз қол жетімділігі, таратылуы	ақпаратты ұрлау, құпия деректерді жариялау
Жүйенің жұмыс қабілеттілігіне қауіп	Жүйенің бұзылуы немесе тоқтатылуы	Қасақана шабуылдар жасау, аппаратық, бағдарламалық жасақтамаларды бұзу
Авторлық құқықты дәлелдеуге қауіп	Құжат айналымында ЭЦҚ қолданылмаған жағдайда, нақты бір пайдаланушының осы құжатты жасағанын дәлелдей алмауы	Құжат айналымының заңды тұрғыдағы маңыздылығын бұзу
Қол жетімділікке қауіп	Дерекқорға қол жеткізудің шектеулігі немесе мүмкін болмауы	Ақпаратқа, дерекқорға немесе жүйеге қол жеткізуді бұзу, тоқтату немесе шектеу

Құжат айналымы жүйесінде ақпараттың қауіпсіздігін қамтамасыз ету және рұқсатсыз әрекеттерден қорғау үшін арнайы механизмдер қолданылады. Бұл қауіптерден қорғауды кез келген құжат айналымы жүйесі белгілі бір деңгейде жүзеге асыруы тиіс [7]. Жүйенің сенімді жұмысын қамтамасыз ету үшін бірнеше міндетті талаптар орындалуы қажет. Осы қауіптерді жеңу үшін құжат айналымы жүйесінде қолданылуы керек механизмдер:

- жүйеде айналымдағы электрондық құжаттардың мазмұнын үшінші тұлғалардың рұқсатсыз қарауынан қорғау. Құжат айналымы жүйесінде айналымдағы электрондық құжаттардың мазмұнын үшінші тұлғалардың рұқсатсыз қарауынан қорғау қажет. Бұл деректердің құпиялылығын сақтаудың негізгі шарты болып табылады.

- электрондық құжаттардың жіберушілерін біржақты сәйкестендіру. Жүйеде электронды құжаттарды жіберушілерді біржақты анықтап, олардың заңдылығын тексеру маңызды. Бұл процесс әрбір қатысушының жеке сәйкестендіру мәліметтері арқылы жүзеге асады.

- электрондық құжаттарды рұқсатсыз өзгерістерден қорғау. Құжаттардың тұтастығын сақтау және оларды рұқсатсыз өзгертулерден қорғау жүйенің сенімділігін арттырады. Бұл мақсатта деректерді шифрлау және электрондық цифрлық қолтаңба қолданылады.

- қақтығыс жағдайларын дұрыс шешу. Электрондық құжат айналымы жүйесінің қатысушылары арасында туындайтын қақтығыс жағдайларын реттеу үшін арнайы регламенттер мен ережелер белгіленуі қажет. Бұл құжат алмасудың тәртібін нақтылап, түсініспеушіліктерді болдырмауға көмектеседі.

Алғашқы үш мәселе ақпаратты криптографиялық қорғау құралдарын қолдану арқылы шешілсе, соңғы мәселе электрондық құжаттармен алмасу тәртібін жүйе қатысушылары арасында регламенттеу арқылы шешіледі.

Құжат айналымы жүйелерінде ақпаратқа рұқсатсыз қол жеткізуден қорғау талаптарына сәйкестік үшін, криптографиялық қорғау құралдары қолданылған жағдайда, ақпаратты сақтау және өңдеу кезінде келесі негізгі қорғау механизмдері қарастырылуы тиіс:

- пайдаланушылар мен қолжетімділік субъектілерін сәйкестендіру және аутентификациялау. Әрбір пайдаланушы жүйеге кірген кезде, оның жеке деректері (логин, құпия сөз, биометриялық мәліметтер) арқылы тексеріледі.

- қол жетімділікті басқару. Құжаттарға тек белгіленген рұқсаттары бар пайдаланушылардың ғана қол жеткізуін қамтамасыз ету. Қол жетімділікті шектеу жүйенің қауіпсіздігін күшейтеді.

- деректерді шифрлау құралдары мен электрондық цифрлық қолтаңбаны қолдану. Шифрлау құралдары құжаттардың құпиялылығын қамтамасыз етеді, ал электрондық цифрлық қолтаңба деректердің тұтастығын сақтайды және жіберушіні растайды.

Бұл критерийлер электрондық құжат айналымы жүйелері үшін ақпаратты қорғаудың негізгі бағалау критерийлері болып табылады [7].

Қауіпсіздікті қамтамасыз ету үшін әртүрлі аутентификация әдістері қолданылады. Олар пайдаланушылардың жүйеге кіру құқығын анықтау үшін әртүрлі факторларды пайдаланады. 2-кестеде бір реттік кіру, екі факторлы, көп факторлы аутентификация түрлері салыстырылып, олардың артықшылықтары мен кемшіліктері қарастырылған. Салыстырмалы талдау [8] дереккөзіне негізделген.

Кесте 2. Салыстырмалы талдау [8]

Параметр	Бір реттік кіру	Көп факторлы аутентификация	Екі факторлы аутентификация
Аутентификация факторы	1(мысалы құпия сөз)	2 немесе одан да көп (құпия сөз + SMS)	2 (мысалы құпия сөз және саусақ ізі)
Қауіпсіздік деңгейі	Орташа	Жоғары	Жоғары
Ыңғайлылық	Өте жоғары	Орташа	Жоғары
Іске асыру қиындығы	Жоғары	Орташа	Төмен
Қолданылуы	Корпоративтік орта, бұлтты сервистер, қызметкерлерге арналған порталдар	Банктер жүйесі, корпоративтік желілер	Онлайн-банкинг, бағдарламалар

2. Зерттеу әдістері мен материалдары

Көп факторлы аутентификация (MFA) – бұл компьютерлік жүйелерде пайдаланушылардың тіркелгі деректерін қорғау үшін бір құпия сөзбен шектелмей, бірнеше тәуелсіз тексеру әдісін қолдануды білдіреді. Бұл әдіс құжаттарды басқару жүйесінде, сондай-ақ кез келген басқа ақпараттық жүйелерде деректер қауіпсіздігін қамтамасыз етудің негізгі құралдарының бірі.

Көп факторлы аутентификация төмендегі элементтер арқылы жүзеге асады:

1) білімге негізделген фактор;

Білімге негізделген фактор – пайдаланушы тек өзі білетін ақпаратты енгізу арқылы аутентификациядан өтетін қауіпсіздік деңгейі. Бұл фактор аутентификацияның ең кең таралған түрі болып табылады және жиі қолданылады. Мысалы, құпия сөз, PIN-код, құпия сұрақтар.

Артықшылықтары:

- жүзеге асыру оңай,
- кез келген жүйеде қолдану ыңғайлы,
- пайдаланушыға таныс әдіс.

Кемшіліктері:

- құпия сөздерді ұмыту қаупі бар,
- құпия сөздерді фишинг немесе хакерлік шабуылдар арқылы оңай ұрлауға болады,
- пайдаланушылар жиі әлсіз құпия сөздерді таңдайды.

2) иемденуге негізделген фактор;

Иемденуге негізделген фактор – аутентификация кезінде пайдаланушының қолында (немесе иелігінде)

болуы тиіс нақты затты немесе құрылғыны қолдануға негізделеді. Жүйеге кіру үшін, әдетте, пайдаланушыға бір реттік кодтар немесе арнайы токендер беріледі. Мысалы, смартфондағы бір реттік кодтар, аппараттық токендер, SMS арқылы жіберілетін кодтар.

Артықшылықтары:

- құпия сөз ұрланған жағдайда да, қосымша құрылғысыз жүйеге кіру мүмкін емес,

- орнату және пайдалану салыстырмалы түрде оңай.

Кемшіліктері:

- смартфон немесе аппараттық токен ұрланса, аутентификация қиындайды,

- кейде желіге тәуелді (SMS-код алу үшін байланыс қажет).

3) биометриялық фактор;

Биометриялық фактор – пайдаланушының физиологиялық немесе мінез-құлықтық ерекшеліктеріне сүйенеді. Биометриялық деректер әдетте адамға ғана тән және оны көшіріп алу қиын. Мысалы, саусақ іздері, бет-әлпетті тану, көз торын сканерлеу.

Артықшылықтары:

- жоғары деңгейдегі қауіпсіздік,

- қолдануға ыңғайлы.

Кемшіліктері:

- биометриялық деректер бұзылған жағдайда, оларды ауыстыру қиын,

- жабдыққа қосымша шығын керек,

- кейде жарық, тазалық секілді сыртқы факторлар аутентификацияны қиындатуы мүмкін.

Көп факторлы аутентификация компьютерлік жүйеде аутентификация үшін құпия сөзден бөлек қорғанысты қолдануды білдіреді. Құжаттарды басқару жүйесінде болсын, кез келген жүйелерде қолданушылардың тіркелгі ақпараттарын қорғау үшін сенімді құпия сөзге қосымша ретінде көп факторлы аутентификацияны қолданған дұрыс. Көп факторлы аутентификация (MFA) жүйенің қауіпсіздігін арттырады, себебі қол жетімділікті беру алдында пайдаланушыдан бірнеше тексеру формасын талап етеді, бұл рұқсатсыз қол жеткізу қаупін айтарлықтай төмендетеді [9].

Көп факторлы аутентификация жүйесін әзірлеу әдістері

Құжат айналымы жүйесі үшін көп факторлы аутентификацияны әзірлеу бірнеше кезеңдерден тұрады. Бұл әдістер жүйенің қауіпсіздігін қамтамасыз етіп, құжаттардың тұтастығы мен құпиялылығын сақтауға бағытталған. Құжаттарды басқару жүйесіне арналған көп факторлы аутентификация жүйесін әзірлеу аутентификация түрін таңдау, басқа жүйелермен байланысын қалыптастыру секілді комплекстік шаралардан тұрады. Сонымен қатар, қолданушыларға қолданғанда ыңғайлы және жоғары қауіпсіздікті қамтамасыз ете білуі қажет.

Жүйені әзірлеу мен енгізудің негізгі қадамдары мен ерекшеліктері

1. Жүйе талаптарын анықтау

Көп факторлы аутентификацияны құжаттарды басқару жүйесіне енгізу үшін ең алдымен жүйеге қойылатын талаптарды анықтау қажет. Бұл кезеңде құжат айналымының ерекшеліктері, пайдаланушылар саны, олардың рөлі мен жүйеге қол жеткізу құқықтары ескеріледі. Сонымен қатар, жүйеге төнетін қауіптер мен осалдықтар анықталып, оларды шешуге бағытталған қорғаныс шаралары жоспарланады. Жүйенің талаптары анықтағанда, ескерілуі тиіс факторлар:

- құжат айналымының масштабы, яғни жергілікті немесе бұлтты қызмет негізінде, пайдаланушылардың рөлдері және оларың жүйеге қатынасу деңгейі,

- пайдаланушылардың аутентификация процесіне ыңғайлылығын қамтамасыз ету,

- құжаттардың қауіпсіздігін қамтамасыз ету мақсатында шифрлауды және хаттамаларды қолдану,

- қауіпсіздікті арттыру мақсатында жүйені жаңарту қажеттілігі.

2. Аутентификация факторларын таңдау

Көп факторлы аутентификация жүйесін құру барысында бірнеше факторды қолдану қажет. Құжаттарды басқару жүйесіне арналған көп факторлы аутентификация жүйесін әзірлеудің негізгі кезеңдері мен әдістері:

- ең алдымен, құжаттарды басқару жүйесіне сай келетін аутентификация

жүйесін анықтау. Құпия ақпараттармен жиі жұмыс жасайтындықтан ақпараттардың жоғары қауіпсіздігін қамтамасыз ететін факторларды таңдаған дұрыс. Факторлар ретінде қарайтынымыз:

1) құпия сөз. Басқа факторлармен байланысу кезіндегі негізгі фактор.

Пайдаланушылардың жүйеге кіруін қамтамасыз ететін кең таралған әдіс, бірақ ол жалғыз қолданылса көптеген шабуылдарға осал болып келуі мүмкін.

2) биометрия. Қауіпсіздікті күшейту үшін қолданылатын екінші негізгі фактор. Саусақ іздері. Бет-әлпет немесе көз торын тану арқылы жоғары деңгейдегі қауіпсіздікті қамтамасыз етеді.

3) аппараттық токендер. Құжаттарды басқару жүйесіне кіру үшін бір реттік кодтар немесе физикалық токендер [10]. Бір реттік кодтарды немесе физикалық құрылғыларды қолдану қосымша қорғаныс қабатын жасайды.

4) SMS немесе электрондық пошта арқылы кодтар. Қолдануға ыңғайлы және жиі қолданылатын әдіс, бірақ желіге тәуелді.

Факторларды таңдағанда жүйенің қауіпсіздігін арттырып қана қоймай, пайдаланушыларға ыңғайлылықты қамтамасыз ету де маңызды.

- көп факторлы аутентификация жүйесінің құрылымын жасау. Атап айтқанда, жүйеге кіру процесін жеңілдету үшін бірлік аутентификация жүйесімен байланысу.

- арнайы сенімді және стандартталған аутентификация протоколдарын таңдау іске асыру кезінде оң әсерін тигізеді.

- аутентификация факторларын байланыстыру. Мысалы, құпия сөздер немесе бір реттік құпия сөздер, биометриялық аутентификация және тағы басқа.

- қауіпсіздік және қауіптерді басқара алу. Әртүрлі шабуылдарға қарсы қорғаныс шараларын ұйымдастырып, тұрақты болу.

Қауіпсіздікті күшейту шаралары:

1) деректерді шифрлау;

Деректерді шифрлау – ақпаратты қорғаудың маңызды ісі. Бұл тәсіл деректерді шифрланған форматта сақтап, рұқсатсыз қол жеткізу жағдайында оны оқылмайтындай етеді. Деректерді шифрлау үшін заманауи алгоритмдер (AES, RSA) қолданылады.

2) қолданушылардың белсенділіктеріне мониторинг және күмәнді қимылдарды бұғаттау;

Пайдаланушылардың жүйеде жүргізген әрекеттерін бақылау және күмәнді белсенділіктерді анықтау. Мысалы, әдеттегіден тыс уақытта кіру әрекеті немесе бірнеше рет қате пароль енгізу сияқты оқиғаларды автоматты түрде бұғаттау.

3) әлеуметтік инженерия шабуылынан қорғаныс;

Қызметкерлерді әлеуметтік инженерия әдістеріне қатысты оқыту. Зиянкестердің әлеуметтік инженерияны пайдаланып, құпия ақпараттарды алуға тырысатынын түсіндіру және осындай шабуылдардан қалай қорғану керектігі туралы нұсқаулар беру.

- осалдықтарға тестілеу және тексеріс жүргізу. Құжаттарды басқару жүйесіне және көп факторлы аутентификацияға тексеріс жүргізу осалдықтардың анықталуы үшін маңызды. Соның ішінде:

- жүйеге тұрақты түрде қауіпсіздік аудитін жүргізу,

- тестілік шабуылдар арқылы жүйенің осалдықтарын анықтау,

- жаңа осалдықтарды анықтау үшін жүйені үнемі жаңартып отыру.

- қызметкерлерге үйрету сабақтарын жүргізу. Яғни, қауіпсіздік жүйелерін және аутентификациямен жұмыс жасау тәртіптерін үйрету. Соның ішінде:

- қызметкерлерді жүйеде қауіпсіз жұмыс жасауға оқыту,

- құпия ақпараттарды қорғау және күдікті жағдайларды хабарлау тәртіптері туралы тренингтер өткізу,

- пайдаланушыларға күшті пароль жасау, фишинг хаттарды тану сияқты қауіпсіздік негіздерін түсіндіру.

3. Интеграция;

Жаңа жүйені қолданыстағы құжат айналымы жүйесімен біріктіру маңызды қадам болып табылады. Бұл кезеңде интеграция құралдары мен хаттамалары қолданылады. Жүйенің барлық компоненттері үйлесімді жұмыс істеуі үшін, пайдаланушыларға ыңғайлы интерфейстер жасалып, процестер оңтайландырылуы тиіс. Интеграцияда маңызды болып табылатын факторлар:

- жүйе архитектурасының үйлесімділігі,

- заманауи API және SDK құралдарын пайдалану арқылы интеграцияны жеңілдету,

- қауіпсіздік хаттамаларын қолдану (SSL/TLS) деректердің шифрлануын қамтамасыз етеді.

Жүйенің сенімділігін арттыру және қауіпсіздік деңгейін көтеру үшін интеграция барысында заманауи технологиялар қолданылып, барлық компоненттердің біртұтас жұмыс істеуі қамтамасыз етіледі.

4. Пайдаланушылар тәжірибесін оңтайландыру;

Жүйе тек қауіпсіз ғана емес, қолданушылар үшін ыңғайлы болуы да маңызды. Сондықтан интерфейсті интуитивті етіп жобалау және қолданушыларға аутентификация процесін түсінікті ету керек.

Пайдаланушылардың қанағаттануын арттыру үшін:

- қосымша қадамдарды барынша азайту,

- тек қажетті аутентификация әдістерін пайдалану,

- қолданушыларды оқыту және қажетті нұсқаулықтар беру.

5. Прототипті тестілеу;

Әзірленген жүйенің қауіпсіздігі мен тиімділігін тексеру үшін тестілеу жүргізіледі. Бұл кезеңде жүйенің осалдықтары анықталып, оларды жою бойынша тиісті шаралар қабылданады. Прототипті тестілеу барысында пайдаланушылардың жүйемен өзара әрекеттесуі де бағаланады.

Тестілеудің негізгі бағыттары:

- жүйенің жұмыс тұрақтылығы,

- пайдаланушылардың кері байланысын жинау,

- осалдықтарды түзету.

6. Құралдар мен технологиялар;

Көп факторлы аутентификацияны әзірлеу үшін заманауи бағдарламалық құралдар мен технологиялар пайдаланылады. Мысалы, қауіпсіздік хаттамалары, API және SDK интерфейстері, шифрлау құралдары. Бұл құралдар жүйенің жұмысын оңтайландыруға және оның қауіпсіздігін арттыруға көмектеседі.

3. Зерттеу нәтижелері және оларды талқылау

Қауіпсіздікті қамтамасыз ету үшін әртүрлі аутентификация әдістері қолданылатындығын атап өттік. Сонымен, бір реттік кіру, екі факторлы аутентификация, көп факторлы аутентификация әдістерінің 2-кестеде көрсетілген салыстырмалы талдаудың нәтижесі бойынша:

- бір реттік кіру жүйесі жылдам әрі ыңғайлы болғанымен, қауіпсіздік деңгейі орташа.

Бұл әдіс қарапайым қолданушылар үшін тиімді болуы мүмкін, бірақ ақпараттың қауіпсіздігін қамтамасыз ету үшін жеткіліксіз.

- көп факторлы аутентификация жоғары қауіпсіздікті қамтамасыз етеді, себебі бірнеше тексеру әдісін қолданады. Бұл әдіс өте сенімді және рұқсатсыз кіру қаупін айтарлықтай төмендетеді, бірақ оны іске асыру кейбір техникалық қиындықтарды талап етеді.

- екі факторлы аутентификация қауіпсіздікті қамтамасыз етеді және көбінесе күнделікті қолдануға ыңғайлы болып табылады, әсіресе онлайн-банкинг және қосымшаларда. Бірақ көп факторлы аутентификациядан төменірек деңгейде, себебі ол тек екі тексеру әдісін қолданады.

Microsoft бұлттық сервистері күн сайын 300 миллионға жуық жалған тіркелгі кіру құрылғыларын тіркейді [11]. Көп факторлы аутентификация есептік жазбаларды шабуыл түрлерінен қорғау арқылы қауіпсіздікті айтарлықтай жақсарта алады. Microsoft мамандарының айтуы бойынша көп факторлы аутентификацияны іске қосқан пайдаланушылар автоматты шабуылдардың 99.9%-ын бұғаттайды [11].

Көп факторлы аутентификация қауіпсіздік тұрғысынан ең жақсы таңдау болып табылады, және құжаттарды басқару жүйесінің қауіпсіздік деңгейін арттырып, қосымша қорғаныс механизмдерін қосады.

Құжаттарды басқару жүйесінің көп факторлы аутентификация жүйесін әзірлеу үшін тек аутентификациялық факторларды ескеру жеткіліксіз. Аутентификациялық факторлармен қатар тиімді интеграция факторларын да қарастырған жөн. Теориялық аспектілермен қатар көп факторлы аутентификация жүйесін нақты жағдайларда қолдану қажет. Құжаттарды басқару жүйесіне ең қолайлы аутентификация әдісін таңдауда, әртүрлі көп факторлы аутентификация түрлерінің ерекшеліктерін салыстыру өте маңызды. Осы мақсатта, құжаттарды басқару жүйесінде қолдануға болатын екі танымал көп факторлы аутентификация түрін қарастырамыз: құпия сөз +

қосымша аутентификатор + биометрия және құпия сөз + SMS/Email-код + биометрия.

- құпия сөз – пайдаланушының тұлғасын растау үшін қолданылатын фактор. Бұл ең кең тараған аутентификациялық әдіс, мұнда пайдаланушы жүйеге кіру үшін алдын ала орнатылған құпия сөзді енгізеді.

- биометрия – жеке тұлғаны тексеру үшін саусақ іздері немесе көз қабағын сканерлеу үшін қолданылатын фактор. Адамның физикалық немесе мінез-құлық ерекшеліктерін анықтап, тұлғаны растау әдісі [12].

- қосымша аутентификатор – пайдаланушылардың тұлғасын растайтын қосымша қауіпсіздік факторы. Мұнда пайдаланушыға қосымша қауіпсіздік деңгейін қамтамасыз ететін құралдар, мысалы, Google Authenticator немесе Authy сияқты мобильді қосымшалар ұсынылады.

- SMS/Email-код– құрылғыға немесе почтаға жіберілетін бір реттік қолданылатын код.

Бұл код тек белгілі бір уақыт аралығында жарамды болады және пайдаланушы оны өз құрылғысына немесе почта арқылы алады [12].

Қауіпсіздік деңгейі бойынша**:**

- құпия сөз + қосымша аутентификатор + биометрия ең қауіпсіз әдістердің бірі болып саналады. Себебі, әрбір аутентификация факторы белгілі бір көлемде рұқсатсыз кіру қаупін төмендетеді. Зиянкес пайдаланушының құпия сөзіне қол жеткізіп, қосымша-аутентификаторға қауіп төндірсе де биометрия жоғары қауіпсіздік деңгейін қамтамасыз етеді.

- құпия сөз + SMS/Email-код + биометрия қауіпсіз, бірақ толықтай емес әдістердің бірі болып саналады. Себебі, биометрия қаншалықты жоғары қауіпсіздік деңгейін қамтамасыз етсе де, пайдаланушылардың SMS/Email-код ақпараттары фишинг, әлеуметтік инженерия және тағы сол сияқты шабуылдарға осал болып келеді.

Құпия сөз + қосымша аутентификатор + биометрия әдісі Құпия сөз + SMS/Email-код + биометрия әдісіне қарағанда қауіпсіз болып саналады.

Ыңғайлылық деңгейі бойынша:

- құпия сөз + қосымша аутентификатор + биометрия пайдаланушылар үшін біршама ыңғайсыз болуы мүмкін, себебі ол қосымша-аутентификатор қолданбасымен биометрияны пайдалануды қажет етеді. Кейбір пайдаланушылар егерде оларға үнемі құпия сөзді енгізіп, биометриялық аутентификацияны растау қажет болған жағдайда оның құрылымына кіре алады.

- құпия сөз + SMS/Email-код + биометрия пайдаланушылар үшін ыңғайлы нұсқа, себебі көптеген пайдаланушылар SMS немесе растау хаттарын алады. Аутентификация процесі оңайырақ көрінеді, өйткені қосымша-аутентификатор қолданбасы қажет емес және кодтар жиі автоматты түрде келеді.

Құпия сөз + SMS/Email-код + биометрия әдісі көптеген қолданушылар үшін ыңғайлы.

Тұрақтылық деңгейі бойынша:

- құпия сөз + қосымша аутентификатор + биометрия Негізінен алғанда тұрақты, бірақ қосымша аутентификатормен немесе биометриямен мәселелер туындауы мүмкін. Себебі, қосымша аутентификатор немесе биометрия әрқашан дұрыс жұмысты қамтамасыз етпейді, әсіресе ескі құрылғыларда.

- құпия сөз + SMS/Email-код + биометрия тұрақты әдіс, бірақ ұялы байланыс сапасы мен SMS / Email қолжетімділігіне тәуелді болуы мүмкін. Егер сымсыз желі қосылған болса, код уақытында келмеуі мүмкін.

Екі әдіс те тұрақты, бірақ, Құпия сөз + SMS/Email-код+биометрия әдісінде SMS/Email-код желілік мәселелерге осал болып келуі мүмкін.

Шығындар факторы бойынша:

- құпия сөз + қосымша аутентификатор + биометрия Қосымша аутентификатор қолданбасын орнату және пайдалану жиі тегін. Алайда, егер биометрияға арналған қатты құрылғы қолданылса (мысалы, саусақ ізі сенсоры), бұл жабдықтың қосымша шығындарына әкелуі мүмкін.

- құпия сөз + SMS/Email-код + биометрия SMS-кодтар ұялы байланыс шығындарын немесе хабарлама жіберу қызметтерін қамтуы мүмкін. Дегенмен, бұл шешім құрылғыға немесе қолданбаға қосымша шығындарды қажет етпейді, бұл оны биометриялық жабдықты пайдаланбайтын ұйымдар үшін тиімдірек етеді.

Құпия сөз + SMS/Email-код + биометрия әдісін қолдану әдетте арзанырақ,

бірақ шығындар ауқымды көлемде ескерілуі мүмкін.

Сенімділік деңгейі бойынша:

- құпия сөз + қосымша аутентификатор + биометрия Бұзуды қиындататын әртүрлі факторлардың арқасында өте жоғары сенімділікке ие. Факторлардың бірі бұзылса да, қалғандары әлі де қорғауды қамтамасыз етеді.

- құпия сөз + SMS/Email-код + биометрия тұрақты шабуылдар болуы мүмкін SMS және email арналарының осалдығына байланысты сенімділік біршама төмен.

Құпия сөз + қосымша аутентификатор + биометрия әдісі жоғарғы сенімділік деңгейіне ие.

Осылайша, таңдау әдісі басымдықтарға байланысты: егер растаудың қол жетімділігі мен құны маңызды болса, Құпия сөз + SMS/Email-код + биометрия әдісін таңдаған дұрыс, бірақ егер басты басымдық жоғары қауіпсіздік болса, онда Құпия сөз + қосымша аутентификатор + биометрия әдісін таңдаған жөн.

Көп факторлы аутентификация жүйесі құжат айналымы жүйелерінен бөлек басқа салаларда да қолданылады. Бұл жүйе қаржы секторында, медицинада, мемлекеттік органдарда құпия ақпараттардың қауіпсіздігін қамтамасыз ету мақсатында қолданылады. Мысалы, медициналық ұйымдарда пациенттердің деректерін қорғау үшін, ал мемлекеттік секторда құпия мемлекеттік құжаттарды сақтау үшін қолданылады.

Жүйе енгізілгеннен кейін оның тиімділігін бағалау үшін қосымша тестілеу жұмыстары жүргізіледі. Бұл кезеңде пайдаланушылардың кері байланысы жинақталып, жүйенің өнімділігі мен қауіпсіздігі бағаланады.

Жүйенің қауіпсіздігін арттыру және заманауи қауіптерге төзімділігін қамтамасыз ету үшін оны жетілдіру жұмыстары үздіксіз жүргізілуі тиіс. Бұл процесс жүйені тұрақты түрде жаңартып, оның жұмыс істеу тиімділігін арттыруға бағытталады.

Жетілдіру бағыттары:

- жасанды интеллект – шабуылдарды болжау және оларды алдын-ала анықтауда маңызды рөл атқарады. Бұл технология пайдаланушылардың әдеттегі әрекеттерін бақылап, күдікті белсенділікті автоматты түрде анықтауға мүмкіндік береді.

- машиналық оқыту – жүйенің қауіп-қатерлерге жауап беру қабілетін арттыратын технология. Ол

шабуылдардың жаңа түрлерін анықтап, олардың алдын алу үшін жүйені автоматты түрде бейімдеуге көмектеседі.

- қолданушылардың кері байланысын ескеру – пайдаланушылардан алынған кері байланыс жүйені жетілдіруде маңызды рөл атқарады. Бұл процесс интерфейсті оңтайландыруға, аутентификация қадамдарын жеңілдетуге және жаңа функционалдарды енгізуге көмектеседі.

Жүйені жетілдіру үшін жұмыстар жасау жүйені тиімдірек етуде өз үлесін қосады. Құжат айналымы жүйесі үшін көп факторлы аутентификацияны әзірлеу осы қадамдарды іске асыру арқылы жүзеге асады. Бұл жүйе құжаттардың қауіпсіздігін қамтамасыз етудің маңызды құралы болып табылады. Әзірленген әдістер мен технологиялар жүйенің тиімділігін арттырып, оны заманауи қауіптерге төзімді етеді.

4. Қорытынды

Мақалада құжаттарды басқару жүйесінің көп факторлы аутентификация жүйесін әзірлеу және зерттеу мәселелері қарастырылды. Құжаттарды басқару жүйесіне қауіп төндіретін шабуылдар сипатталды. Шабуылдардан қорғаныс шаралары да талданды. Көп факторлы аутентификация жүйесінің басқа аутентификация жүйелерімен салыстырмалы талдауы келтірілді. Салыстырмалы талдау нәтижесі бойынша көп факторлы аутентификация жоғары қауіпсіздікті қамтамасыз етеді.

Сонымен қатар, аутентификация жүйесін әзірлеу кезеңдері анықталып, әр кезеңге сипаттама беріліп, маңыздылығы көрсетілді. Құжаттарды басқару жүйесінде қолдануға болатын екі танымал көп факторлы аутентификация түрі құпия сөз + қосымша аутентификатор + биометрия және құпия сөз + SMS/Email-код + биометрия салыстырмалы талдау жүргізіліп, олардың артықшылықтары мен кемшіліктері көрсетілді.

Құжаттарды басқару жүйесінде ақпараттардың қауіпсіздігін қамтамасыз ету үшін әрдайым сенімді, шабуылдарға осал емес, қауіпсіздікті толық қамтамасыз ететін аутентификация факторын, яғни, көп факторлы аутентификацияны қолданған дұрыс екендігі анықталды. Құжаттардың құпиялылығын, тұтастығын, қол жетімділігін сақтаумен қатар бұл әдіс рұқсатсыз кіру шабуылының мүмкіндігін азайтады. Жүйенің өнімділігі мен қауіпсіздігін арттыру үшін алдағы уақытта жасанды интеллект және машиналық оқыту технологияларын интеграциялау ұсынылады. Интерфейсті жетілдіру және аутентификация процесін қарапайым ету құжат айналымы жүйесінде пайдаланушылардың тәжірибесін оңтайландыруға көмектеседі.

References / Әдебиеттер

[1] OOO Analitika SNG. (2023). Sistema dokumentooborota. *Retrieved from:* https://xn--90afdtkhdeabaxvge.net/sed/novosti_i_press-relizi/sistema_dokumentooborota.html

[2] Zharkov, A.A. (2020). Sistema vozvrata dokumentooborota. Tekst nauchnyh statej po special'nosti «Komp'juternye i informacionnye nauki». *Retrieved from:* https://cyberleninka.ru/article/n/sistema-elektronnogo-dokumentooborota

[3] DMS Technology. (2023). Password Protection Made Better with Multifactor Authentication. *Retrieved from*: https://dmstechnology.com/multifactor-authentication/

[4] Babelforce. (2023). What is a Document Management System (DMS)? *Retrieved from*: https://www.babelforce.com/blog/explainer/what-is-a-document-management-system-dms/#:~:text=A%20document%20management%20system%20is,security%20processes%20to%20protect%20files

[5] Redakcija «KORUS Konsalting». (2024). DMS sistema: kljuch k jeffektivnomu upravleniju dokumentami v sovremennom biznese. *Retrieved from*: https://korusconsulting.ru/infohub/dms-sistemy-upravlenie-dokumentami/

[6] Astral Soft. (2023). Bezopasnost' jelektronnogo dokumentooborota. *Retrieved from*: https://astral.ru/info/elektronnyy-dokumentooborot/bezopasnost-elektronnogo-dokumentooborota/

[7] RusNauka. (2016). Analiz ugroz informacii sistem jelektronnogo dokumentooborota. *Retrieved from*: https://www.rusnauka.com/45_PWMN_2016/Informatica/4_219982.doc.htm

[8] LogicMonitor. (2023). What are the different types of authentication? LogicMonitor Blog. *Retrieved from*: https://www.logicmonitor.com/blog/what-are-the-different-types-of-authentication

[9] Dimka, D. (2024). Osobennosti sistemy upravlenija juridicheskimi dokumentami. Upravlenie juridicheskimi dokumentami. *Retrieved from*: https://lexworkplace.com/features-of-a-legal-document-management-system/

[10] Nadejkina, V. S. & Lagutkina, T. V. (2022). Analiz sposobov realizacii sistemy mnogofaktornoj autentifikacii. *Nauchnyj rezul'tat. Informacionnye tehnologii, 7 (4), 59-66*

[11] TAdviser. (2024). Mnogofaktornaja (dvuhfaktornaja) autentifikacija. *Retrieved from*: https://www.tadviser.ru/index.php

[12] StrongDM. (2023). Multi-factor authentication types. *Retrieved from*: https://www.strongdm.com/blog/multi-factor-authentication-types

Құжаттарды басқару жүйесінің көп факторлы аутентификация жүйесін әзірлеу және зерттеу

А. Ахметова*

Satbayev University, Алматы, Қазақстан

**Корреспонденция үшін автор: akhmetova.aidanaa@gmail.com*

Аңдатпа. Мақалада құжаттарды басқару жүйесінің көп факторлы аутентификация жүйесін әзірлеу және зерттеу мәселелері қарастырылған. Құжаттарды басқару жүйесіне қауіп төндіретін шабуылдар сипатталған. Шабуылдардың

алдын алу мақсатында құжаттарды басқару жүйесіне көп факторлы аутентификация жүйесін әзірлеу әдістері көрсетілген. Көп факторлы аутентификация жүйесінің басқа аутентификация жүйелерімен салыстырмалы талдауы, сонымен қатар көп факторлы аутентификация жүйесін әзірлеу әдістері қарастырылған. Құжаттарды басқару жүйесінде қолдануға болатын екі танымал көп факторлы аутентификация түрлері салыстырылды. Әзірленген көп факторлы аутентификация жүйесін зерттеу тестілеу жүйесін және аудит жүргізуді талап етеді. Зерттеу жүргізу құжаттарды басқару жүйесі үшін жоғары қауіпсіздікті, нормативтік талаптарға сай болуды, осалдықтардың алдын алуды қамтамасыз етеді.

Негізгі сөздер: *көп факторлы аутентификация, қол жетімділік, құжат айналымы, интеграция, құпия сөз, биометрия, шифрлау, хаттама*.

Исследование и разработка системы многофакторной аутентификации для системы документооборота

А. Ахметова*

Satbayev University, Алматы, Казахстан

**Автор для корреспонденции: akhmetova.aidanaa@gmail.com*

Аннотация. В статье рассматриваются вопросы разработки и исследования системы многофакторной аутентификации (MFA) для систем управления документами. Описаны атаки, угрожающие системам управления документами, и предложены методы разработки системы MFA с целью предотвращения этих атак. Проведен сравнительный анализ многофакторной аутентификации с другими системами аутентификации, а также исследованы методы разработки многофакторной аутентификации. Были сравнены два популярных типа многофакторной аутентификации, которые можно использовать в системе управление документооборота. Для проверки разработанной системы MFA необходимо провести тестирование и аудит. Проведение исследования обеспечивает высокую безопасность для системы управления документами, соответствие нормативным требованиям и предотвращение уязвимостей.

Ключевые слова: *многофакторная аутентификация, доступность, документооборот, интеграция, пароль, биометрия, шифрование, протокол*.

Received: 17 November 2023
Accepted: 16 March 2024
Available online: 31 March 2024