МРНТИ 20.53.17
УДК 004.056.55:343.982.34(574)
https://doi.org/10.47533/2024.1606-146X.53

Б. А. КАЗАНГАПОВА, А. А.ШАЙКУЛОВА*, А. Ж. МОЛДАКАЛЫКОВА, А. Т. ИСКАКОВА

Алматы технологиялық университеті, Алматы, Қазақстан
**E-mail:shaikulova_ak_al@mail.ru*

ЭЛЕКТРОНДЫҚ ҚҰЖАТ АЙНАЛЫМЫН ҚОРҒАУДЫҢ ТИІМДІЛІГІН АРТТЫРУДЫҢ НЕГІЗГІ ЖОЛДАРЫ

Казангапова Баян Алькеновна – т.ғ.к., «Ақпараттық жүйелер» кафедрасының қауымдастырылған профессоры, Алматы технологиялық университеті, Алматы, Қазақстан;

E-mail: kbayana@mail.ru https://orcid.org/0000-0002-5196-8885

Шайкулова Актоты Алиевна – т.ғ.к., «Ақпараттық жүйелер» кафедрасының қауымдастырылған профессоры, Алматы технологиялық университеті, Алматы, Қазақстан;

E-mail: Shaikulova_Ak_Al@mail.ru https://orcid.org/0000-0001-6121-123X

МолдакалыковаАйгульЖоямергеновна–«Ақпараттықжүйелер»кафедрасының сеньор-лекторы, Алматы технологиялық университеті, Алматы, Қазақстан;

E-mail: aigul_atu@mail.ru https://orcid.org/ 0000-0003-0656-9065

Искакова Айнур Тлеубаевна – «Ақпараттық жүйелер» кафедрасының сеньор-лекторы, Алматы технологиялық университеті, Алматы, Қазақстан;

E-mail: iskakova.1977@mail.ru https://orcid.org/0000-0001-6841-9244

Ақпараттық ресурстар мен ақпараттық жүйелер қазіргі заманғы кәсіпорындардың барлық салаларында бірқатар негізгі қорғалатын элементтерге жатады [11-15]. Бүгінгі таңда осы элементтерге теріс ақпараттық әсер ету құралдары белсенді дамып келеді, Оларға қарсы тұру кең ауқымды зерттеулер мен тиісті тұжырымдамаларды, ақпараттық қауіпсіздікті қамтамасыз ету құралдары, әдістері мен әдістемелерін құру саласындағы нақты жұмыстарды ұйымдастыру бағдарламаларын әзірлеуді талап етеді. Цифрлық құжаттарды авторизацияланған, бірақ жосықсыз пайдаланушылардың заңсыз таратуы ұйымдардың құпиялылығына өсіп келе жатқан қауіп болып табылады, оны тек шифрлау әдістерін қолданатын құжаттарды басқару жүйесі толығымен жеңе алмайды. Бұл мәселе рұқсат етілмеген пайдаланушылардың цифрлық құжатқа қол жеткізуімен бірге туындайды.

Бұл мақалада цифрлық құжаттарды осы екі қауіптен қорғау үшін қарсы шара ретінде цифрлық құжаттың өмірлік циклінің белгілі бір кезеңдерінде шифрлау және саусақ іздерін алу әдістерін мұқият біріктіретін жаңа тәсіл ұсынылады. Осы сценарий аясында толық талдау жүргізілді, онда негізгі құрамдас элементтер, олардың өзара әрекеттесуі, деректер ағыны және қауіпсіздікті қамтамасыз ету қызметтері анықталды. Бұл қорғаныс жүйесі қауіпсіздіктің жеткілікті деңгейіне кепілдік береді, өйткені ол стандартты криптографиялық алгоритмдерді және кілттердің ұсынылған өлшемдерін қолданады.

Бұл тәсілдің мақсаты-пайдаланушының құпиялылығы, тұтастығы, аутентификациясы, қол сұғылмаушылығы және қадағалауы сияқты ақпараттық қауіпсіздік қызметтерін қамтамасыз ету, осылайша олардың өмірлік циклі бойына цифрлық құжаттарды қорғау.

Түйін сөздер: *электрондық құжат айналымы жүйелері, ақпараттық қауіпсіздік, тиімділік критерийлері, ақпараттық қауіпсіздік қатерлері, дактилоскопия.*

Б. А. КАЗАНГАПОВА, А. А.ШАЙКУЛОВА*, А. Ж. МОЛДАКАЛЫКОВА, А. Т. ИСКАКОВА

Алматинский технологический университет, Алматы, Казахстан
E-mail:shaikulova_ak_al@mail.ru

ОСНОВНЫЕ ПУТИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Казангапова Баян Алькеновна – к.т.н., ассоциированный профессор кафедры «Информационные системы», Алматинский технологический университет, Алматы, Казахстан;

E-mail: kbayana@mail.ru https://orcid.org/0000-0002-5196-8885

Шайкулова Актоты Алиевна – к.т.н., ассоцированный профессор кафедры «Информационные системы», Алматинский технологический университет, Алматы, Казахстан;

E-mail: Shaikulova_Ak_Al@mail.ru https://orcid.org/0000-0001-6121-123X;

Молдакалыкова Айгуль Жоямергеновна сеньор-лектор кафедры «Информационные системы», Алматинский технологический университет, Алматы, Казахстан;

E-mail: aigul_atu@mail.ru https://orcid.org/ 0000-0003-0656-9065

Искакова Айнур Тлеубаевна – сеньор-лектор кафедры «Информационные системы», Алматинский технологический университет, Алматы, Казахстан;

E-mail: iskakova.1977@mail.ru https://orcid.org/0000-0001-6841-9244

Информационные ресурсы и информационные системы относятся к ряду основных защищаемых элементов во всех сферах жизнедеятельности современных предприятий [11-15]. Сегодня активно развиваются средства негативного информационного воздействия на эти элементы, противодействие которым требует широких разноплановых исследований и разработок соответствующих концепций, программ организации конкретных работ в области создания средств, методов и методик обеспечения информационной безопасности. Незаконное распространение цифровых документов авторизованными, но недобросовестными пользователями представляет собой растущую угрозу конфиденциальности организаций, с которой не может полностью справиться система управления документами, использующая только методы шифрования. Эта проблема возникает вместе с доступом к цифровому документу неавторизованных пользователей.

В данной статье в качестве контрмеры для защиты цифровых документов от этих двух угроз предлагается новый подход, который тщательно объединяет методы шифрования и снятия отпечатков пальцев на определенных этапах жизненного цикла цифрового документа. В рамках этого сценария был проведен полный анализ, в котором были определены основные составные элементы, их взаимодействие, поток данных и предоставление услуг по обеспечению безопасности. Данная система защиты гарантирует достаточный уровень безопасности, так как в ней используются стандартные криптографические алгоритмы и рекомендуемые размеры ключей.

Цель этого подхода-обеспечить такие услуги информационной безопасности, как конфиденциальность, целостность, аутентификация, неотказуемость и отслеживание пользователя, тем самым защищая цифровые документы на протяжении всего их жизненного цикла.

Ключевые слова: *системы электронного документооборота, информационная безопасность, критерии эффективности, угрозы информационной безопасности, дактилоскопия.*

B. KAZANGAPOVA, A. SHAIKHULOVA*, A. MOLDAKALYKOVA, A. ISKAKOVA

[1]Almaty Technological University, Almaty, Kazakhstan
**E-mail: shaikulova_ak_al@mail.ru*

THE MAIN WAYS TO IMPROVE THE EFFECTIVENESS OF ELECTRONIC DOCUMENT MANAGEMENT PROTECTION

Kazangapova Bayan Alkenovna – PhD, Associate Professor, Department of Information Systems, Almaty Technological University, Almaty, Kazakhstan;

E-mail: kbayana@mail.ru https://orcid.org/0000-0002-5196-8885

Shaikulova Aktoty Alievna – Candidate of Technical Sciences, Associate Professor of the Department of Information Systems, Almaty Technological University, Almaty, Kazakhstan

E-mail: Shaikulova_Ak_Al@mail.ru https://orcid.org/0000-0001-6121-123X

Moldakalykova Aigul Zhoyamergenovna – senior lecturer of the Department of "Information Systems", Almaty Technological University, Almaty, Kazakhstan;

E-mail: aigul_atu@mail.ru https://orcid.org/ 0000-0003-0656-9065

Iskakova Ainur Tleubaevna – senior lecturer of the Department of "Information Systems", Almaty Technological University, Almaty, Kazakhstan;

E-mail: iskakova.1977@mail.ru https://orcid.org/0000-0001-6841-9244

Abstract. Information resources and information systems are among the main protected elements in all spheres of life of modern enterprises [11-15]. Today, the means of negative information impact on these elements are actively developing, the counteraction of which requires extensive diverse research and development of relevant concepts, programs for organizing specific work in the field of creating tools, methods and techniques for ensuring information security. Illegal distribution of digital documents by authorized but unscrupulous users is a growing threat to the confidentiality of organizations, which a document management system using only encryption methods cannot fully cope with. This problem occurs together with access to a digital document by unauthorized users.

In this article, as a countermeasure to protect digital documents from these two threats, a new approach is proposed that carefully combines encryption and fingerprinting methods at certain stages of the digital document lifecycle. Within this scenario, a full analysis was carried out, in which the main constituent elements, their interaction, data flow and the provision of security services were identified. This protection system guarantees a sufficient level of security, since it uses standard cryptographic algorithms and recommended key sizes.

The purpose of this approach is to provide information security services such as confidentiality, integrity, authentication, non-repudiation and user tracking, thereby protecting digital documents throughout their entire life cycle.

Keywords: *electronic document management systems, information security, performance criteria, threats to information security, fingerprinting.*

Кіріспе. Ақпараттық ресурстар мен ақпараттық жүйелер қазіргі заманғы компаниялардың өмірінің барлық салаларында қорғалатын бірқатар негізгі элементтердің бөлігі болып табылады. Бүгінгі таңда теріс ақпараттық әсер ету

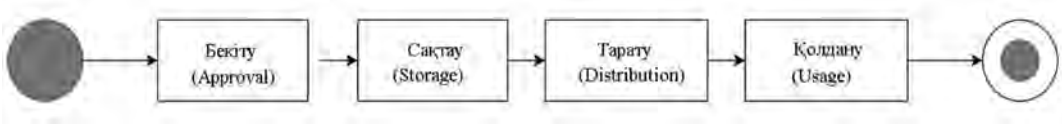
құралдары белсенді түрде әзірленуде және оларға қарсы тұру ақпараттық қауіпсіздікті қамтамасыз ету үшін құралдарды, әдістер мен технологияларды құру саласында нақты жұмысты ұйымдастыру үшін ауқымды және алуан түрлі зерттеулерді, өзара байланысты концепцияларды, жоспарларды әзірлеуді талап етеді [7]. Заманауи құрылым мен жүйенің жұмыс істеуін құру және ұйымдастыру, ең алдымен, оның сыртқы ортамен ақпараттық өзара әрекеттесуін қамтамасыз етуді талап етеді. Мұндай өзара әрекеттесу мүмкіндігінше сенімді және қауіпсіз болуы керек, бірақ ақпаратқа төнетін қауіптердің жыл сайын ауқымы кеңейіп, түрі де алуан түрлі болуда, оған дәлел: 2022 жылы бүкіл әлем бойынша инциденттер саны 2021 жылмен салыстырғанда 21%-ға өсті. Ұйымдарға жасалған шабуылдарда шабуылдаушылардың құпия ақпаратты ұрлауы 47%-ды, жеке тұлғаларға жасалған шабуылдарда құпия ақпаратқа қол сұғуы – 64%-ды құраған. Бұл жөнінде Positive Technologies зерттеулері нақты дәлел келтірген. Сарапшылар ұйымдар арасында мемлекеттік органдар (17%), медициналық мекемелер (9%) және өнеркәсіп (9%)шабуылдардың құрбаны болғанын анықтады. Көптеген жағдайларда шабуылдаушылар зиянды бағдарламалық жасақтаманы (54%), әлеуметтік инженерияны (43%) қолданған және осалдықтарды (34%)пайдаланған. Сарапшылар мұндай шабуылдар 2023 жылы жалғасады деп күтеді. Олар интернет қызметтерін ұсынатын және онлайн төлем мүмкіндігін ұсынатын компаниялар үшін ерекше қауіп төндіреді[16].

«Касперский Зертханасының» ақпараты бойынша, Қазақстан ірі ұйымдар да, үжеке қолданушылары да ұшыраған кибершабуылдар саны бойынша әлемде жетінші орынға ие болды, деп хабарлайды Zakon.kz.

Мамандар 2022 жылдың бірінші тоқсанын 2023 жылдың ұқсас кезеңімен салыстыра келе, Қазақстандағы фишингтік шабуылдар санының 12% - ға өскенін атап өтті. Бұл ретте корпоративтік сектордағы фишингтік шабуылдар саны 120% - ға өскен. 2023 жылдың бірінші тоқсанында елде бопсалау бағдарламаларына тап болған ұйымдардың саны негізінен 2022 жылдың төртінші тоқсанымен салыстырғанда 17% – ға төмендеген (егер бизнеске жасалған шабуылдарды қарастыратын болсақ) [17].

Әдістер. Ұсынылған тәсіл белгілі бір сценарийге бағытталған, әдетте цифрлық құжаттарды пайдаланушылар әртүрлі кезеңдерде - құрудан, цифрландырудан, сақтаудан бастап пайдалануға дейін әртүрлі рөлдермен басқаратын ұйымдарда кездеседі [4].

Бұл жұмыста физикалық немесе қағаз құжаттары цифрланған және цифрлық кескін ретінде сақталған нақты ұйымдар мен кәсіпорындарда жиі кездесетін сценарий қарастырылады. Бұл әдетте қолмен жазылған қолтаңбаларды, мақұлдау мөрлерін немесе құжаттың мазмұнын растайтын кез келген басқа таңбаны сақтау үшін жасалады. Физикалық құжаттарды сканерлеу және оларды цифрлық кескін ретінде сақтау процесі жергілікті желі контекстінде жиі қолданылатын құжаттың белгілі бір өмірлік циклін анықтайтын Document Imaging (DI) ретінде танымал. Құжаттың өмірлік циклі 1-суретте көрсетілген және [3]-те жақсы құжатталған.



Сурет 1 – Құжаттардың өмірлік циклінің кезеңдері.

DI үшін құжаттың өмірлік циклі физикалық құжат жасалған және тексерілген сәттен басталады. Құжат бекітілгеннен кейін ол цифрландырылады және алынған цифрлық кескін ЭҚЖ-да мұрағаттауға дайын, бұл бекіту кезеңі (Approval) болып табылады.

Осы кезеңнен бастап ЭлҚ өзгертілмеуі тиіс. Әрі қарай, ЭлҚ сақтау кезеңі (Storage) үшін ЭҚЖ-ға жіберіледі, онда таңбаларды оптикалық тану құралдары мәтінді шығарып, оны индекстейді. Соңында, ЭлҚ тарату кезеңіне (Distribution) дайын, ол қол жетімді және оны пайдалану кезеңінде (Usage) авторизацияланған пайдаланушылар қолдана алады. Әдетте, цифрлық құжаттарға қол жетімділік бұрын ҚБЖ-ға тіркелген пайдаланушылармен шектеледі, бұл рұқсатсыз кіруге жол бермейді. Құжаттарды бекіту және оларға қол жеткізу ұйымның аумақтары бойынша сегменттелуі мүмкін, осылайша құжаттар тек пайдаланушылардың ішкі жиынына қол жетімді болады. Пайдаланушыларды ЭҚЖ-дағы рөлдері бойынша категориялау арқылы пайдаланушылардың әртүрлі типтерін аймақтарға бөлуге болады:

1) Цифрлық құжаттарды мақұлдайтын және жүктейтін рецензенттер. Рецензенттер мен ЭҚЖ арасындағы барлық операциялардың түпнұсқалығы мен құпиялылығына кепілдік беріледі.

2) Цифрлық құжаттарға қол жеткізетін тұтынушылар (пайдаланушылар), цифрлық құжаттарды пайдалана алады. Тұтынушылар мен DMS арасындағы барлық операциялар кепілдендірілген және құпия болып табылады.

3) Аудиторлар-кез-келген цифрлық құжатқа шектеусіз қол жеткізе алатын тұтынушылардың ерекше түрі және авторлық қызметтерден бас тартуды талап ете отырып, нақты цифрлық құжатты мақұлдаған рецензенттердің жеке басын растайды.

4) Құжатты таратқан пайдаланушының/пайдаланушылардың жеке басын анықтайтын әкімшілер. Пайдаланушы-әкімшілер цифрлық құжаттарды жою немесе жүйе пайдаланушыларын қосу/жою сияқты арнайы өкілеттіктерге ие.

Ұсынылған ЭҚҚЖ-да пайдалану сценарийлері 1-кестеде сипатталған. №1 жағдайда қауіпсіздікті ескеру қажет, өйткені аутентификация үшін пайдаланушылар ұсынатын тіркелу деректері транзит кезінде қорғалуы керек. №2, №3, №4 және №5 -ті қолданудың қосымша нұсқалары жүйе мен агент арасындағы қорғалған байланысқа сүйенуі мүмкін, бірақ бұл міндетті емес, өйткені бұл жағдайда берілетін деректердің мағынасы жоқ десе де болады.

Кесте 1 – Ұсынылған ЭҚҚЖ-дағы пайдалану сценарийлері

Пайдалану жағдайының идентификаторы	Жағдайдың сипаттамасы	Жауапты тұлға	Өмірлік циклдің кезеңдері
№1	Жүйеге кіру	Пайдаланушы	Алдын ала кезең
№2	Жүйеден шығу	Пайдаланушы	Соңғы кезең
№3	Пайдаланушыны тіркеу	Әкімші	Алдын ала кезең
№4	Пайдаланушыны жою	Әкімші	Алдын ала кезең
№5	Электрондық құжатты жою	Әкімші	Сақтау
№6	Электрондық құжатты жүктеу	Рецензент	Бекіту
№7	Жеке департаменттің электрондық құжатын жүктеу	Пайдаланушы	Тарату
№8	Барлық департаменттің электрондық құжатын жүктеу	Аудитор	Тарату
№9	Рецензенттің мақұлдауын растау	Аудитор	Сақтау
№10	Заңсыз көшірмелерді тарататын пайдаланушыларды анықтау	Әкімші	Қолдану

Алайда, № 6 - №10 жағдайлар үшін қауіпсіздік міндетті талап болып табылады. 2-кестеде осы пайдалану жағдайларында ұсынылатын қауіпсіздік қызметтері, сондай-ақ оларды модельдеу және енгізу кезінде қарастырылған қауіпсіздік әдістері көрсетілген.

Кесте 2 – Қажетті қауіпсіздік қызметтері мен әдістерін пайдалану

Өмірлік циклдің кезеңдері	Қажетті қауіпсіздік қызметі	Әдістер
Бекіту және Тарату	Шынайылық	Асимметриялық криптография, Цифрлық сертификаттар, Электрондық цифрлық қолтаңба
Бекіту, сақтау және Тарату	Құпиялылық	Симметриялық және асимметриялық шифрлау
Бекіту, сақтау және Тарату	Тұтастық	Хэш функциялары және цифрлық қолтаңбалар
Сақтау	Бас тарту емес (ауытқу емес) *Non-repudiation	Электрондық цифрлық қолтаңба
Сақтау	Қол жеткізуді басқару	Рөлге негізделген қол жеткізуді басқару, қол жеткізуді міндетті басқару (ҚМБ)
Қолдану	Пайдаланушыларды бақылау	Дактилоскопия (Саусақ ізі)

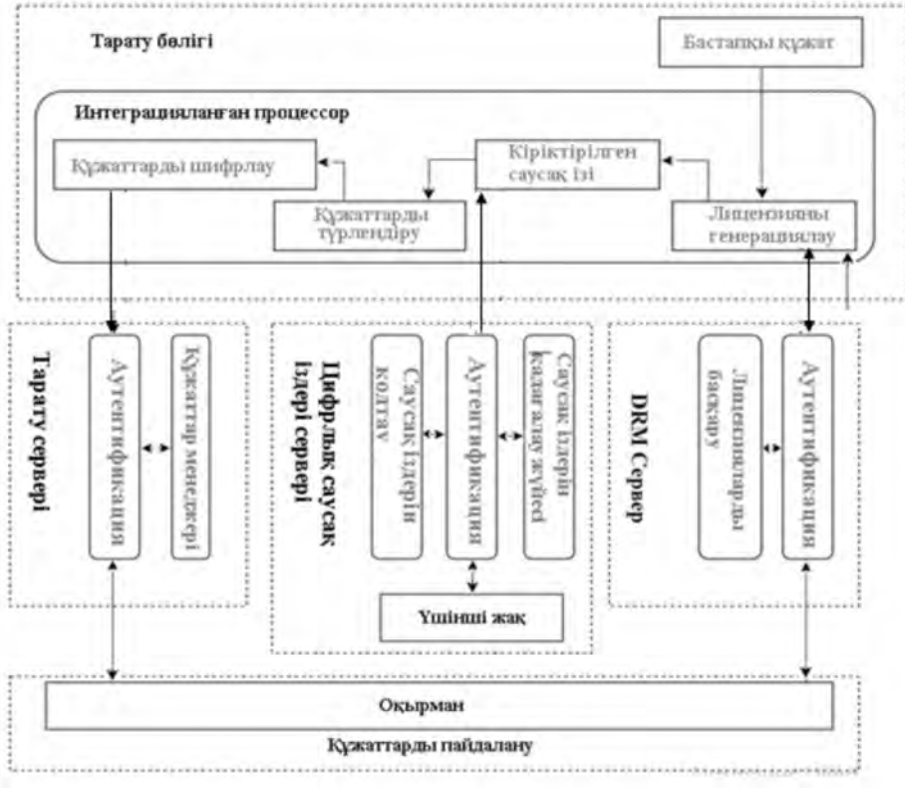
№6-да рецензент бекіту кезеңінде цифрлық құжаттарды жүйеге жүктеу кезінде түпнұсқалықты, құпиялылықты және тұтастықты қамтамасыз етуі тиіс. Ол үшін рецензент цифрлық құжатқа қол қояды және құжатты және оның қолтаңбасын шифрлау арқылы жүйеге қауіпсіз түрде жүктейді. Сонымен қатар, рецензент мақұлдау операциясына қатысты деректерге цифрлық қолтаңба береді. Бұл ақпаратты аудитор № 9-да рецензенттің әрекеттерін ескере отырып растау және қауіпсіздікті қамтамасыз ету үшін қолдана алады. №7 және № 8 тарату сатысында жүзеге асырылады. Бұл жағдайда тұтынушылар немесе аудиторлар цифрлық құжаттарды жүктеген уақытта қауіпсіздік, шынайылық, құпиялылық және тұтастық қызметтерін қамтамасыз етуі қажет. Цифрлық құжат және оның қолтаңбасы жүйеден шифрланған түрде алынады. Содан кейін Тұтынушы немесе Аудитор құжат мазмұнын локальды түрде кері шифрлайды және құжаттың цифрлық қолтаңбасының түпнұсқалығын тексереді. № 9-ды сақтау кезеңінде аудитор орындайды. Кез келген уақытта, аудитор рецензенттердің цифрлық құжаттарды бекіту операциясына қатысты деректерді тексеру арқылы бас тарту құқығынсыз қауіпсіздік қызметін қамтамасыз ете алады. Соңында, №10 Пайдалану кезеңінде пайдаланушыны бақылайды, бұл сандық құжатты жүйеден жүктеген және оны заңсыз таратқан пайдаланушыны анықтайды. Бұл жағдайда саусақ ізін алу әдістері қолданылады. Бұл пайдалану сценарийін тек әкімшілер ғана орындай алады және қаскүнемді анықтау үшін пайдаланылған құжаттың цифрлық көшірмесін және оның жүйеде сақталған түпнұсқа нұсқасын ұсынуы керек.

Нәтижелер мен талқылаулар. [1,5]-те көрсетілгендей, қауіпсіздіктің негізгі қауіптері екі аспектіде қарастырылады: бірінші - бұл пайдаланушының электрондық құжатқа рұқсатсыз қатынас құруы және пайдалануы, екінші - заңды пайдаланушылардың электрондық құжаттарды заңсыз көшіруі және таратуы. Құқықтарды цифрлық форматта басқару немесе Rights Management Digital (DRM) ақпараттық қауіпсіздік саласындағы өзекті тақырыптардың бірі болып табылады және қол жеткізу механизмінің аппараттық және бағдарламалық қамтамасыз етуінің үйлесімі арқылы оның өмірлік циклінде цифрлық ақпараттық контентке қол жеткізуді бақылауды жүзеге асырады. Оның мәні мынада: бірқатар қауіпсіздік технологиялары арқылы ол цифрлық өнімді рұқсатсыз көшіруге және пайдалануға жол бермеу үшін цифрлық контентті және оны тарату арналарын бақылайды. Қазіргі уақытта DRM зерттеулері мен қолданылуы негізінен электронды кітаптарда, ағынды Интернет-тасымалдаушыларда және электрондық құжаттарда қолданылады. Электрондық құжаттарды қорғау үшін қолданылатын DRM технологиясы рұқсат етілмеген пайдаланушылардың электрондық құжаттарға рұқсатсыз кіруіне және оларды пайдалануына жол бермейтін тиімді технология болып табылады.

Заңды пайдаланушылардың электрондық құжаттарды заңсыз тарату мәселесіне келетін болсақ, қолданыстағы DRM негізіндегі құжаттарды қорғау жүйесі бұл мәселені түпнұсқа құжаттардың пайдаланушы көшірмелерін шектеу арқылы шешуге арналған [8]. Модельдің негізгі идеясы-цифрлық дактилоскопия технологиясы жүйеде DRM-мен үйлеседі. Электрондық құжатқа цифрлық саусақ ізі ретінде қарастырылатын пайдаланушылардың сипаттамалары туралы ақпаратты енгізу арқылы жүйе пайдаланушыларға құжаттардың көшірмелерін пайдалануға мүмкіндік береді, әдетте электрондық құжат заңсыз ағып кеткен жағдайда сонымен бір мезгілде пайдалану-

шылардың жауапкершілігін анықтайды. Нәтижесінде, жүйе пайдаланушылардың құпия электрондық құжаттарды заңсыз таратуына белгілі бір шектеулер қоя алады. [6].

Жүйе моделі. Заңды пайдаланушыларды пайдаланудың және қауіпсіздік құжаттарын қорғаудың екі аспектісін ескере отырып, біз цифрлық саусақ ізі технологиясын DRM-мен біріктіреміз және электрондық құжат заңсыз берілгеннен кейін пайдаланушылардың жауапкершілігін анықтай алатын электрондық құжаттарды қорғау моделі әзірленді. Жүйе бес бөліктен тұрады: «Құжаттың тарату бөлігі», «Тарату сервері», «Цифрлық саусақ ізі сервері», «DRM-сервер» және «Құжаттарды пайдалану» (моделі 2-суретте көрсетілген. Цифрлық саусақ ізі сервері Саусақ ізін бақылау жүйесінен, Саусақ ізін кодтау жүйесінен және Үшінші тараптан тұрады. Дәстүрлі DRM негізіндегі электрондық құжаттарды қорғау жүйесінен айырмашылығы, тарату сервері мен сандық саусақ ізі сервері ұлғайтылған.



Сурет 2 – Жүйе моделі.

Жүйенің негізгі жұмыс процесі келесі түрге ие:

1. Құжаттың дистрибьюторлық жағы құжатқа лицензия жасайды. Лицензия құжаттарды басқару және қорғау саясатын қамтамасыз етеді және жеке басын растағаннан кейін лицензия DRM серверіне беріледі;

2. Құжаттың таратушы жағы пайдаланушының сәйкестендіру ақпаратын Цифрлық Саусақ ізі Серверіне беру үшін Цифрлық Саусақ ізі Серверіне қол жеткізе алады.

Цифрлық Саусақ ізі Серверіндегі саусақ ізін кодтау жүйесі пайдаланушының сәйкестендіру ақпаратын кодтайды, содан кейін кодтау тізбегін құжаттарды бөлудің Соңына жібереді, кодтау тізбегі құжатты бөлудің соңында пайдаланушының қолы ретінде бастапқы құжатқа енгізіледі;

3. Құжаттың көшірмесі құжаттарды таратудың соңында түрлендіріледі және шифрланады, ал көшірмесі DOM құжатына түрлендіріледі және тарату Серверіне жіберіледі. Дистрибьюторлық серверді құру пайдаланушылардың DRM құжаттарын басқа жолдардан алу мүмкіндігін болдырмай, DRM құжатының шығарылымын біріздендіруден тұрады. Бұл заңсыз тарату үшін жауапкершілікті анықтауға қол жеткізу үшін қажет;

4. Құжатты пайдаланатын пайдаланушы нақты пайдаланушының тіркеу жазбасын және файл атауын ұсынады, бұл жеке куәлікті растау кезінде қажет болады, және бұл - қажетті DRM құжатына «Ақырғы қол жетімділікті пайдаланатын құжат».

Лицензияларды құру, құжаттарды түрлендіру, құжаттарды шифрлау DRM-ге негізделген дәстүрлі электрондық құжаттарды қорғау жүйесіне ұқсас. Тарату серверін, саусақ ізін ендіруді және сандық саусақ ізі серверін іске асырудың негізгі функциялары мен әдістері төменде егжей-тегжейлі қарастырылады:

А. Цифрлық саусақ ізі сервері. Цифрлық саусақ ізі сервері саусақ ізін кодтау жүйесі мен саусақ ізін бақылау жүйесінен тұрады. Сонымен қатар, цифрлық саусақ ізі сервері үшінші тараппен бірге жеке тұлғаның аутентификациясын аяқтайды.

1. Саусақ ізін кодтау жүйесі. Саусақ ізін кодтау жүйесінің функциясы саусақ іздерін кодтау болып табылады, яғни саусақ ізін кодтау жүйесі саусақ іздерінің сәйкес реттілігін алу үшін пайдаланушы идентификаторын кодтайды.

2. Саусақ ізін бақылау жүйесі. Саусақ ізін бақылау жүйесі негізінен саусақ іздерін алуды және сәйкестендіруді аяқтайды. Алдымен жүйе саусақ іздерін құжаттан шығарады, содан кейін алынған саусақ ізін дерекқордағы сақталған жазбамен салыстырады. Саусақ іздерін алу және сәйкестендіру процесі: алдымен саусақ ізін алу алгоритмі арқылы электрондық құжаттан саусақ ізі тізбегі алынады; түзетілген саусақ ізі тізбегін алу үшін қателерді түзету үшін саусақ ізі тізбегі декодталады; саусақ іздерінің түзетілген тізбегін саусақ ізі дерекқорындағы саусақ іздерімен сәйкестендіру, қай пайдаланушының құжаттарды көшіргенін және таратқанын және бұл үшін кім жауап беруі керек екенін тексеру процесі орындалады. Бақылау процесі 3- суретте көрсетілген.

Сурет 3 – Саусақ ізін бақылау процесі.

B. Саусақ ізін енгізу. Ендірілген саусақ ізі-түпнұсқа құжаттың көшірмесіне пайдаланушы кодының басып шығару ретін ендіру. Авторлық құқықты бақылаудың негізі ретінде пайдаланушы кодының басып шығару реті түпнұсқа құжаттың әрбір көшірмесіне ендірілген. Ендіру процесі былайша түсіндіріледі: біріншіден, ендірілетін ақпарат пайдаланушы атынан, жұмыс блогынан, жалпыға ортақ кілттен және т. б. алынған нақты деректер болып табылатын пайдаланушының сәйкестендіру ақпараты бар саусақ ізі тізбегін алу үшін алдын ала өңделеді. Содан кейін пайдаланушының сәйкестендіру ақпаратының саусақ ізі тізбегі кодталған саусақ ізі тізбегін құруға негіз болады. Соңында, NEC алгоритмі сияқты саусақ ізін ендіру алгоритмін қолдана отырып, саусақ ізінің кодталған тізбегін құжат дистрибьюторы арқылы құжаттың көшірмесіне ендіреді.

Саусақ ізін ендірудің құжат дистрибьюторына орналастырылуының себебі мынада: егер саусақ ізін ендіруді цифрлық саусақ ізі сервері жүзеге асырса, онда цифрлық саусақ ізі сервері жалпы жүйеде тар жолдарды қалыптастыру үшін тым ауыр болуы мүмкін. Сонымен қатар, құжатты тарату орталығы мен цифрлық саусақ ізі сервері арасында түпнұсқа құжаттың көшірмесін беру кейбір қауіпсіздік мәселелерін туды-руы мүмкін.

C. Тарату сервері. Сервер-таратушы жүйені әзірлеу мен енгізудің ядросы болып табылады, ол негізінен қолданушыларды басқарудың ішкі жүйелерінен және құжат айналымының DRM ішкі жүйелерінен тұрады.

1. Пайдаланушыларды басқару. Қолданушыларды басқарудың ішкі жүйесі негізінен қолданушыларды басқаруды қамтамасыз етеді және пайдаланушыға кірген кезде жеке басын куәландыратын аутентификацияны орындайды. Әкімшілер тарату серверінде негізінен пайдаланушы тіркелгілері мен құпия сөздері туралы ақпаратты сақтайтын пайдаланушы дерекқорын жасайды. Тарату серверіндегі пайдаланушының сәйкестендіру ақпараты DRM серверінде және цифрлық саусақ іздері серверінде пайдаланушының сәйкестендіру ақпаратының дәйектілігін қамтамасыз ету үшін техникалық құралдарды қабылдай алады.

2. DRM құжат айналымын басқару. DRM құжат интеграцияланған процессор арқылы қорғалған арна бойынша дистрибуция серверіне жіберіледі, ал DRM құжаттарды басқарудың ішкі жүйесі құжатты және құжат туралы ақпаратты сақтайды және басқарады, мысалы, құжатты кодтау, құжаттың аты, құжатты пайдаланушы, құжат өндірушісі және күні және т. б.. Әрбір құжат өзінің заңды пайдаланушыларымен байланысты, сондықтан құжаттар жүйеде тиісті пайдаланушыға таратылады.

3. Құжаттарға қол жеткізу. Пайдаланушы құжатты алуға өтініш беруі қажет болған жағдайда келесі қадамдарды орындауы қажет:

– Пайдаланушы Тарату серверіне кіреді және жеке басын сәтті аутентификациялағаннан кейін құжаттың атын немесе құжат кодын хабарлайды;

– Тарату сервері құжаттардың ақпараттық дерекқорынан пайдаланушы енгізген құжат туралы ақпаратқа сәйкес құжат туралы ақпаратты сұрайды. Құжаттарға қол жеткізе алатын пайдаланушының сәйкестендіру ақпараты болмаған жағдайда, пайдаланушының сұраулары қабылданбайды; қарсы жағдайда Пайдаланушыға құжаттарды пайдалануға рұқсат етіледі, тарату сервері құжатты алады және пайдаланушының ақпаратымен белгіленген пайдаланушыға жібереді;

– Құжаттарды тарату туралы ақпаратты жазады, мысалы, берілген күні, пайдаланушының сәйкестендіру ақпараты және т. б.

Ең бастысы, цифрлық дактилоскопиялауда символдарды танудың басқа коды қолданылады-дактилоскопиялау цифрлық тасымалдағыштарға енгізіледі, содан кейін олар пайдаланушылар арасында таратылады [9,10]. Осылайша, бұл құпия электрондық құжаттарды қорғаудың тиімді құралы және негізгі технологияларының бірі болып табылады [2].

Қорытынды. Құжатқа енгізілген сандық саусақ ізін қолдан жасау қиын, өйткені деректерді бірнеше ондаған байтқа дейін қысу және оларды әрі қарай шифрлау (стегокілт)жүзеге асырылады. Саусақ ізі бойынша ақпаратты кодтау схемасы-бұл пайдаланушыға қатысты ақпарат шабуылға қарсы тұрудың белгілі бір қабілеті бар, кодтық сөздерді генерациялау үшін белгілі бір ережелерге сәйкес кодталатын процесс. Саусақ іздерін жақсы кодтау заңсыз таралуды бақылаудың негізгі факторы болып табылады, әр саусақ ізін кодтау схемасы тиісті бақылау жүйесіне ие. Қазіргі уақытта мәтінге негізделген кодтау әдісі мыналарды қамтиды: жылжуды кодтау әдісі, синонимдерді ауыстыру әдісі, ерекше белгілерді кодтау әдісі, түрлендіруді кодтау әдісі [3].

DRM электрондық құжаттарды қорғау технологиясы негізінде құжаттарды қорғауда цифрлық дактилоскопия технологиясы енгізілді, модельде құпия электрондық құжаттарды заңсыз көшіру және тарату үшін жауапкершілікті сәйкестендірудің жаңа тәсілі ұсынылды, сондай-ақ модельдің негізгі технологиялары зерделенді.

ӘДЕБИЕТ

1 Казангапова Б.А. Информационная безопасность компьютерных систем и сетей. //Алматы: ТОО «Power Print» – 2019. – С.119.

2 Чунг К., Чой С., Чой У., и др. Эффективное анонимное снятие отпечатков пальцев с электронной информации с улучшенной автоматической идентификацией распространителей. // Труды Третьей Международной конференции по информационной безопасности и криптологии. том 2015 LNCS.

3 Муноз-Хернандез М.Д., Гарсиа-Хернандез J.J. and Моралез-Сандовал, М. Исследование устойчивости цифровых документов с отпечатками пальцев к атакам с повторным вводом в частотной области // 9-й Международный конференция Int. технологии и обеспеченные транзакции (ICITST-2014). Лондон, Великобритания, 2014, 8–10 декабря. - С. 25-30. IEEE, Нью-Джерси, США.

4 Макарова Н.В. Компьютерное делопроизводство: учеб. курс / Н.В. Макарова, Г.С. Николайчук, Ю.Ф. Титова. – СПб.: Питер, 2005. – 411 с.

5 Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – М.: ДиаСофт, 2002. – 693 с.

6 Сабанов А.А. Некоторые аспекты защиты электронного документооборота // Connect! Мир связи. – 2010. – № 7. – С. 62–64.

7 Досмухамедов Б.Р. Анализ угроз информации систем электронного документооборота // Компьютерное обеспечение и вычислительная техника. – 2009. – № 6. – С. 140–143.

8 Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. – М.: Наука и техника, 2003. – 384 с.

9 Казангапова Б.А., Бапиев К.К. Концептуальный подход к безопасности для управления электронными документами на основе дактилоскопии. // Materials of the VI International

Scientific-Practical Conference «The Europe and the Turkic World: Science, Engineering and Technology» May 5-7 , 2021 Bursa (Turkey) p. 378-382

10 Казангапова Б.А., Бапиев К.К. Метод оценки безопасности автоматизированных систем электронного документооборота// Вестник КазАТК, №4 (115), 2020г. с.246-253

11 Закон РК «О Национальном архивном фонде и архивах»

12 Закон Республики Казахстан от 24 ноября 2015 года «Об информатизации»

13 Закон Республики Казахстан от 7 января 2003 года «Об электронном документе и электронной цифровой подписи»

14 Постановление Правительства Республики Казахстан от 31 октября 2018 года № 703 «Об утверждении Правил документирования, управления документацией и использования систем электронного документооборота в государственных и негосударственных организациях»

15 СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования».

16 https://rspectr.com/infographics/kolichestvo-kiberatak-v-mire-v-2022-godu-vyroslo-na-20

17 https://www.zakon.kz/6393340-kazakhstan-zanyal-sedmoe-mesto-v-mire-po-kolichestvu-kiberatak.html

REFERENCES

1 Kazangapova B.A. Information security of computer systems and networks. Almaty: Power Print LLP - 2019. – P.119.

2 Chung K, Choi S, Choi U, et al. Effective anonymous fingerprinting of electronic information with improved automatic identification of distributors. Proceedings of the Third International Conference on Information Security and Cryptology. Volume 2015 LNCS.

3 Munoz-Hernández, M.D., García-Hernández, J.J., and Morales-Sandoval, M. Investigation of the resilience of digital documents with fingerprints to frequency-domain re-entry attacks // 9th International Conference on Int. Technologies and Secured Transactions (ICITST-2014). London, UK, 2014, December 8–10. - P. 25-30. IEEE, New Jersey, USA.

4 Makarova N.V. Computer office work: textbook. course / N.V. Makarova, G.S. Nikolaychuk, Yu.F. Titova. - St. Petersburg: Peter, 2005. – 411 p.

5 Domarev V.V. Bezopasnost informatsionnykh tekhnologii [Security of information technologies]. Methodology for creating protection systems. – M.: DiaSoft, 2002. – 693 p.

6 Sabanov A.A. Some aspects of the protection of electronic document management // Connect! The world of communication. – 2010. – № 7. – S. 62–64.

7 Dosmukhamedov B.R. Analysis of threats to information systems of electronic document management // Computer support and computer technology. – 2009. – № 6. – S. 140–143.

8 Shcheglov A.Yu. – M.: Science and Technology, 2003. – 384 p.

9 Kazangapova B.A., Bapiev K.K. Conceptual approach to security for the management of electronic documents based on fingerprinting. Materials of the VI International Scientific-Practical Conference “The Europe and the Turkic World: Science, Engineering and Technology” May 5-7 , 2021 Bursa (Turkey) p. 378-382

10 Kazangapova B.A., Bapiev K.K. Method for assessing the safety of automated electronic document management systems // Bulletin of KazATK, No. 4 (115), 2020, pp. 246-253.

11 Law of the Republic of Kazakhstan “On the National Archival Fund and Archives”.

12 Law of the Republic of Kazakhstan dated November 24, 2015 “On Informatization”.

13 Law of the Republic of Kazakhstan dated 7 January 2003 “On Electronic Document and Electronic Digital Signature”

14 Decree of the Government of the Republic of Kazakhstan dated October 31, 2018 No. 703 "On Approval of the Rules for Documentation, Document Management and the Use of Electronic Document Management Systems in State and Non-State Organizations"

15 ST RK 1073-2007 "Means of cryptographic protection of information. General technical requirements".

16 https://rspectr.com/infographics/kolichestvo-kiberatak-v-mire-v-2022-godu-vyroslo-na-20

17 https://www.zakon.kz/6393340-kazakhstan-zanyal-sedmoe-mesto-v-mire-po-kolichestvu-kiberatak.html