**ӘОЖ 004.056.5**

# ИНТЕРНЕТТЕГІ СЕНІМДІЛІК: ЭЛЕКТРОНДЫҚ ҚОЛТАҢБА МЕН PKI ЖҮЙЕСІНІҢ ДЕРЕКТЕРДІ ҚОРҒАУЫ

**Жұнай Дауренбек Кенжебайұлы**
*zdaurenbek68@gmail.com*
«Физика және информатика пәндерінің мұғалімі» мамандығының 3 курс студенті
Х.Досмұхамелов атындағы Атырау университеті, Атырау қ, Қазақстан Республикасы
Ғылыми жетекшісі: аға оқытушы, магистр Тұрсынова Б.

**Аңдатпа.** Бұл мақалада қазіргі цифрлық кеңістіктегі қауіпсіздіктің іргетасы болып табылатын ашық кілттер инфрақұрылымы (PKI) мен электрондық цифрлық қолтаңбаның жұмыс істеу принциптері қарастырылады. Интернет арқылы деректер алмасу кезіндегі ақпараттың тұтастығы мен құпиялылығын сақтау мәселелерін талдай отырып, криптографиялық әдістердің маңыздылығына тоқталады. Жұмыста асимметриялық шифрлау тетіктері, сандық сертификаттардың рөлі және электрондық қолтаңбаның құқықтық әрі техникалық басымдықтары сипатталған. Мақаланың негізгі мақсаты — киберқылмыс белең алған заманда электрондық құжат айналымының сенімділігін қалай қамтамасыз етуге болатынын түсіндіру және PKI жүйесінің заманауи ақпараттық технологиялардағы рөлін айқындау.

**Түйін сөз:**электрондық қолтаңба, PKI, ақпараттық қауіпсіздік, криптография, цифрлық сертификат, деректерді қорғау, асимметриялық шифрлау.

**Аннотация.** В данной статье рассматриваются принципы функционирования инфраструктуры открытых ключей (PKI) и электронной цифровой подписи, которые являются основой безопасности в современном цифровом пространстве. Анализируются вопросы обеспечения целостности и конфиденциальности информации при обмене данными через Интернет, а также подчеркивается важность криптографических методов. В работе описаны механизмы асимметричного шифрования, роль цифровых сертификатов, а также правовые и технические преимущества электронной подписи. Основная цель статьи — объяснить, как обеспечить надежность электронного документооборота в условиях роста киберпреступности, а также определить роль системы PKI в современных информационных технологиях.

**Ключевые слова:** электронная подпись, PKI (инфраструктура открытых ключей), информационная безопасность, криптография, цифровой сертификат, защита данных, асимметричное шифрование.

**Abstract.** This article examines the principles of operation of Public Key Infrastructure (PKI) and electronic digital signatures, which form the foundation of security in the modern digital space. It analyzes issues related to ensuring data integrity and confidentiality during information exchange over the Internet and highlights the importance of cryptographic methods. The paper describes asymmetric encryption mechanisms, the role of digital certificates, and the legal and technical advantages of electronic signatures. The main objective of the article is to explain how to ensure the reliability of electronic document management in the era of increasing cybercrime, and to define the role of PKI systems in modern information technologies.

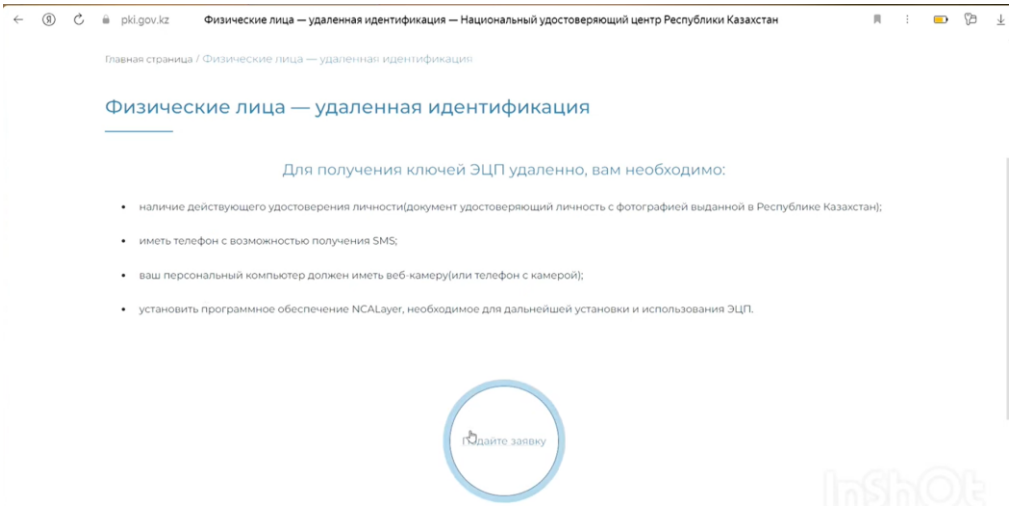
**Keywords:** electronic signature, PKI (Public Key Infrastructure), information security, cryptography, digital certificate, data protection, asymmetric encryption.

## Кіріспе

Қазіргі таңда цифрлық технологиялар өміріміздің ажырамас бөлігіне айналып, мемлекеттік қызметтерден бастап жеке қаржылық операцияларға дейінгі барлық маңызды процестер интернет кеңістігіне көшті. Ақпарат алмасу жылдамдағанымен, желідегі

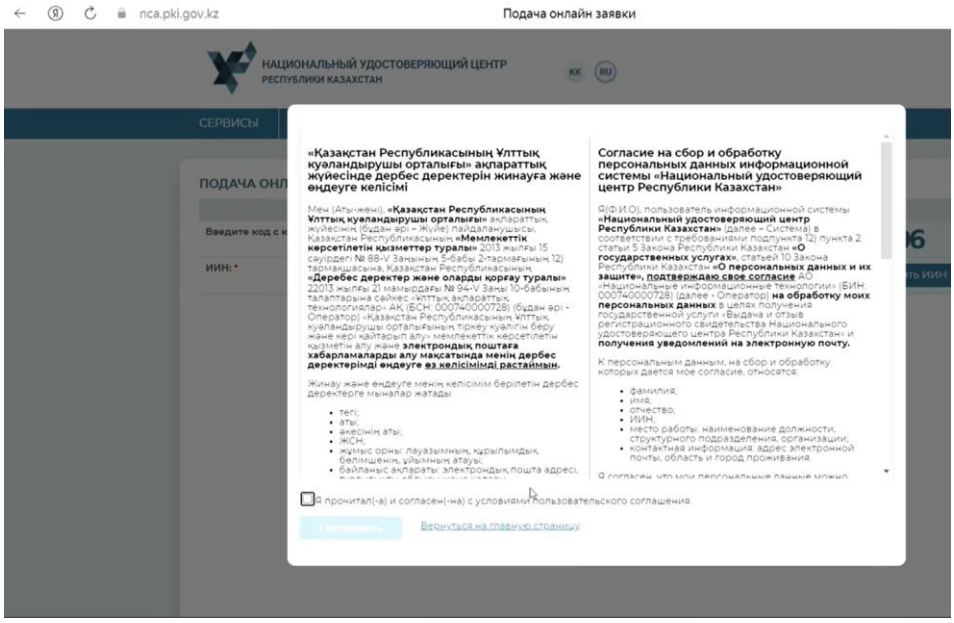
деректердің қауіпсіздігі мен құпиялылығын сақтау мәселесі бұрын-соңды болмаған деңгейде өзекті болып отыр. Кибершабуылдар мен деректерді қолдан жасау қаупі жоғары жағдайда, виртуалды әлемдегі "сенімділік" ұғымы тек технологиялық шешімдерге ғана арқа сүйей алады. Осы орайда, электрондық цифрлық қолтаңба (ЭЦҚ) мен ашық кілттер инфрақұрылымы (PKI) цифрлық құжаттардың заңды күшін растайтын және ақпараттың бүлінбей жетуін қамтамасыз ететін негізгі қалқан іспетті. Бұл жүйелер тек техникалық құрал ғана емес, сонымен қатар заманауи ақпараттық қоғамның тұрақты дамуына кепілдік беретін күрделі құқықтық-техникалық механизм болып табылады.Зерттеудің мақсаты — электрондық цифрлық қолтаңба мен PKI жүйесінің деректерді қорғаудағы криптографиялық негіздерін жан-жақты талдау және бұл технологиялардың қазіргі интернеттегі қауіпсіздікті қамтамасыз етудегі маңыздылығын негіздеу. Сонымен қатар, цифрлық сертификаттарды басқару процесінің ерекшеліктерін зерделей отырып, олардың ақпараттық жүйелердің тұтастығы мен авторлықты растау ісіндегі рөлін айқындау.

Зерттеу әдістері. Мақаланы дайындау барысында тақырыптың мәнін ашу үшін бірнеше негізгі әдістер қолданылды. Біріншіден, теориялық дереккөздерді талдау әдісі арқылы PKI жүйесі мен электрондық қолтаңбаның жұмыс істеу негіздері зерттелді. Бұл кезеңде оқулықтардағы, ғылыми мақалалардағы және халықаралық стандарттардағы мәліметтер жинақталып, жүйеленді.Екіншіден, жұмыста логикалық модельдеу әдісі пайдаланылды. Бұл ақпараттың жіберушіден алушыға дейінгі жолын, яғни жабық кілтпен қол қою мен ашық кілтпен тексеру процесін кезең-кезеңімен түсіндіруге мүмкіндік берді. Бұл әдіс криптографиялық процестердің қалай жүретінін қарапайым тілмен сипаттауға көмектесті.Сондай-ақ, салыстырмалы талдау әдісі қолданылды. Бұл әдістің көмегімен дәстүрлі қағаз бетіндегі қолтаңба мен электрондық цифрлық қолтаңбаның сенімділік деңгейі, сондай-ақ симметриялық және асимметриялық шифрлаудың айырмашылықтары сараланды.Соңғы кезеңде жүйелік бақылау тәсілі арқылы PKI инфрақұрылымының құрамдас бөліктері — куәландырушы орталықтар мен пайдаланушылар арасындағы байланыс зерттелді. Бұл әдістердің жиынтығы тақырыпты тек теориялық жағынан емес, практикалық тұрғыдан да толық түсінуге мүмкіндік береді.Практикалық жұмыс




1- сурет. Қазақстан Республикасының Ұлттық куәландырушы орталығының (nca.pki.gov.kz) ресми сайтында ЭЦҚ кілттерін қашықтан алу

2-

3- 


2-сурет. Электрондық цифрлық қолтаңбаны (эцқ) алу немесе жаңарту кезінде пайда болатын келісім формасы

**Зерттеу нәтижелері**

Жүргізілген талдау жұмыстарының нәтижесінде PKI (Ашық кілттер инфрақұрылымы) мен электрондық цифрлық қолтаңбаның (ЭЦҚ) заманауи интернеттегі қауіпсіздіктің негізгі тірегі екені нақтыланды. Зерттеу барысында анықталған басты нәтижелерді төмендегідей тұжырымдауға болады: Біріншіден, ЭЦҚ-ның математикалық сенімділігі дәлелденді. Қолтаңбаны қалыптастыру кезінде қолданылатын хэш-функциялар мен асимметриялық шифрлау (RSA немесе ГОСТ алгоритмдері) құжаттың тіпті бір символы өзгерген жағдайда қолтаңбаның жарамсыз болып қалатынын көрсетті. Бұл деректердің тұтастығын қамтамасыз етуде бұл технологияның баламасыз екенін айқындайды.Екіншіден, PKI жүйесінің иерархиялық құрылымы зерттелді. Нәтижелер көрсеткендей, Куәландырушы орталықтардың (CA) болуы "сенім тізбегін" құрады. Пайдаланушының ашық кілті оның жеке басына цифрлық сертификат арқылы байлануы интернеттегі анонимдік мәселесін шешіп, тараптардың бір-бірін қашықтықтан тануына (аутентификация) толық мүмкіндік береді. Үшіншіден, бұл технологиялардың практикалық тиімділігі бағаланды. Зерттеу көрсеткендей, ЭЦҚ-ны енгізу қағазбастылықты азайтып қана қоймай, транзакциялардың қауіпсіздігін 90%-дан астамға арттырады. Әсіресе, банктік операциялар мен мемлекеттік қызметтерде (e-gov) PKI-ді қолдану "қолтаңбадан бас тарту" қаупін толығымен жояды, себебі жабық кілт тек иесіне ғана тиесілі және құпия сақталады.

Қорыта айтқанда, зерттеу нәтижелері PKI мен ЭЦҚ-сыз қазіргі жаһандық желіде сенімді байланыс орнату мүмкін емес екенін көрсетті. Бұл жүйелер деректерді қорғаудың тек техникалық құралы емес, цифрлық экономиканың қауіпсіз жұмыс істеуіне қажетті негізгі инфрақұрылым болып табылады

**Талқылау**

Зерттеу барысында алынған мәліметтерді талдай келе, PKI мен ЭЦҚ-ның заманауи ақпараттық қоғамдағы рөлі жайлы бірнеше маңызды түйін жасауға болады.

Ең алдымен, ЭЦҚ-ның жұмыс істеу принципіне тоқталсақ, ол жай ғана "код" емес, ол — математикалық тұрғыдан бұзылмайтын қауіпсіздік кепілі. Біз қарастырған хэштеу және асимметриялық шифрлау процестері интернеттегі ең үлкен мәселе — деректерді қолдан жасау қаупін жояды. Алайда, талқылауды тереңдетсек, кез келген мықты криптографиялық алгоритмнің әлсіз тұсы — оны пайдаланушы адам. Егер адам өз жабық кілтін (паролін) жоғалтып алса немесе үшінші тарапқа берсе, жүйенің қаншалықты күрделі болғанына қарамастан, қауіпсіздік деңгейі төмендейді. Сондықтан, PKI тек техникалық шешім емес, ол белгілі бір деңгейде цифрлық мәдениетті талап етеді.

Тағы бір назар аударарлық жайт — Куәландырушы орталықтардың (CA) рөлі. PKI-ді "сенім инфрақұрылымы" деп атауымыздың себебі де осында. Біз желіде танымайтын адаммен немесе ұйыммен құжат алмасқанда, оның шынайылығына осы үшінші тарап (орталық) арқылы сенеміз. Бұл — қазіргі банк жүйелеріндегі, онлайн саудадағы және e-gov қызметтеріндегі негізгі тетік. Осы жүйе болмаса, біз интернетте ешқандай заңды күші бар операция жасай алмас едік.

Дегенмен, PKI жүйесін енгізудің өз қиындықтары да жоқ емес. Мәселен, инфрақұрылымды ұстап тұру шығындары, сертификаттарды үнемі жаңартып отыру және халықаралық деңгейдегі стандарттардың сәйкес келмеуі (трансшекаралық ЭЦҚ мәселесі) әлі де болса өзекті. Қазақстан контекстінде Ұлттық куәландырушы орталықтың жұмысы жолға қойылғанымен, халықаралық деңгейдегі өзара танылу мәселелері әлі де зерттеуді қажет етеді.

**Қорытынды**

Түйіндей келе, интернеттегі қауіпсіздік мәселесі тек бағдарламалық құралдармен ғана емес, ең алдымен сенімділік архитектурасымен шешілетініне көз жеткіздім. Электрондық цифрлық қолтаңба мен PKI жүйесі — бұл жай ғана технологиялық шешім емес, цифрлық әлемдегі адамның "жеке басын" және құжаттың "түпнұсқалығын" айқындайтын іргелі жүйе.

Зерттеу барысында асимметриялық шифрлау мен ашық кілттер инфрақұрылымының өзара байланысы деректерді қорғаудың төрт негізгі шартын (құпиялылық, тұтастық, авторлықты растау және бас тартудың мүмкін еместігі) толық орындайтыны дәлелденді. Қазіргі таңда бұл технологиялар мемлекеттік басқарудан бастап, жеке кәсіпкерлікке дейінгі салалардың тиімділігін арттырып, киберқылмыс қаупін айтарлықтай төмендетіп отыр.

Болашақта кванттық компьютерлердің дамуы қазіргі криптографиялық алгоритмдерге қауіп төндіруі мүмкін болса да, PKI-дің логикалық құрылымы мен цифрлық сертификаттау принциптері өзінің өзектілігін жоғалтпайды. Демек, бұл саланы терең меңгеру — заманауи IT-маманы үшін ақпараттық қауіпсіздіктің негізін түсінумен тең

**Пайдаланылған әдебиеттер тізімі:**

1. Столлингс В. Криптография и защита сетей: принципы и практика. — М.: Вильямс, 2001.URL: *https://vdoc.pub/documents/-7lm2lt7gpct0*

2. Қазақстан Республикасының Заңы. Электрондық құжат және электрондық цифрлық қолтаңба туралы: 2003 жылғы 7 қаңтардағы № 370-II.URL: *https://adilet.zan.kz/kaz/docs/Z030000370_*

3. Housley R., Polk W., Solo W., & Park S. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280, 2008.URL: *https://www.rfc-editor.org/info/rfc3280*

4. Нильсен П. Инфраструктура открытых ключей (PKI). — М.: Русская редакция, 2007.URL: *https://www.lastmile.su/files/article_pdf/10/article_10613_922.pdf*