МАЗМҰНЫ / СОДЕРЖАНИЕ / CONTENT

Мақала туралы мәлімет

Конференция атауы	«Жастар және ғылым: бүгіні мен болашағы» жас ғалымдардың халықаралық ғылыми-тәжірибелік конференция материалдар жинағы
Сборник	«Молодежь и наука: настоящее и будущее». Сборник материалов Международной научно-практической конференции молодых ученых
Conference	The collection of materials from the International Scientific and Practical Conference of Young Scientists «Youth and Science: Present and Future»
Өткізілген күні	7 сәуір 2025, Атырау
ISBN	978-601-262-587-5
Жинақтағы жариялану №	081
Жинақтағы беттері	377-381
ӘОЖ/УДК/UDC	ӘОЖ 344.13
Секция	Секция IV. II Адам құқығын қорғау – құқықтық және әділ мемлекет құрудың кепілі/ / Защита прав человека – залог создания правового и справедливого государства
Автор(лар)	Әбдеш Медина Айбарқызы
Мәртебесі	Студент
Ғылыми жетекші	Ғылыми жетекшісі, з.ғ.м, сеньор - лектор – Тажгарина Б.Қ.
Мақала атауы	КИБЕРҚЫЛМЫСТАР: ТҮРЛЕРІ ЖӘНЕ ОЛАРМЕН КҮРЕСУ ЖОЛДАРЫ

Этномедиация играет важную роль в построении стабильного и мирного общества, где представители различных этносов могут взаимодействовать на основе взаимоуважения и сотрудничества. Она способствует не только разрешению конкретных конфликтных ситуаций, но и снижает общий уровень межэтнической напряженности, укрепляя социальную сплоченность. В современных условиях, когда миграционные процессы и глобализация приводят к увеличению многонациональных сообществ, этномедиация становится неотъемлемым инструментом мирного сосуществования. Ее дальнейшее развитие требует подготовки квалифицированных медиаторов, совершенствования законодательной базы и активного внедрения медиационных практик в систему общественных и государственных институтов.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Закон Республики Казахстан «О медиации» от 28 января 2011 года
2. Электронный ресурс — https://time.kz/news/society/2024/10/28/etnomediator-kak-most-mezhdu-kulturami
3. Электронный ресурс — https://assembly.kz/ru/ank/deyatelnost-assamblei-naroda-kazakhstana

ӘОЖ 344.13

КИБЕРҚЫЛМЫСТАР: ТҮРЛЕРІ ЖӘНЕ ОЛАРМЕН КҮРЕСУ ЖОЛДАРЫ

Әбдеш Медина Айбарқызы
abdeshmedina05@gmail.com
«Құқық қорғау қызметі» білім бағдарламасының 3 курс студенті
Х. Досмұхамедов атындағы Атырау университеті, Атырау қ, Қазақстан Республикасы
Ғылыми жетекшісі, з.ғ.м, сеньор - лектор – Тажгарина Б.Қ.

Кіріспе

Бүгінгі күнде цифрлық технологиялар өмірдің барлық саласына еніп, адамзаттың өмір сүру салтын түбегейлі өзгертіп жатыр. Алайда технологиялық прогрестің оң әсерімен қатар, оның теріс салдары да байқалады. Солардың бірі – киберқылмыстардың кеңінен таралуы. Киберқылмыстар тек жеке тұлғалардың құқықтары мен дербес деректеріне ғана қауіп төндіріп қоймай, мемлекеттің қауіпсіздігі мен экономикалық тұрақтылығына да зиян келтіруде. Киберқылмыстардың таралуы заманауи қоғам үшін үлкен сын-тегеурінге айналып, жеке тұлғаларға, ұйымдарға және мемлекеттерге зор қауіп төндіріп отыр. Қазақстан үшін де бұл мәселе өзекті болып отыр. Елдегі цифрландыру үдерісінің кеңеюі жаңа қауіптерді болдырмау үшін заңнамалық базаны жетілдіруді талап етеді. Қазіргі таңда мемлекет киберқылмыстарға қарсы күрес жүргізу үшін бірқатар шараларды қолға алуда, бірақ бұл салада әлі де шешілмеген проблемалар бар. Осы мақалада киберқылмыстардың түрлері, олардың құқықтық табиғаты, Қазақстанның қылмыстық заңнамасындағы киберқауіпсіздікке қатысты нормалар және халықаралық тәжірибе қарастырылады. Сонымен қатар, киберқылмыстармен күрестің тиімділігін арттыруға бағытталған ұсыныстар беріледі.

Киберқылмыс – бұл ақпараттық-коммуникациялық технологияларды пайдалану арқылы жасалатын құқық бұзушылық. Киберқылмысқа жататын әрекеттер цифрлық құрылғылардың, интернет желісінің және бағдарламалық қамтамасыз етудің көмегімен жүзеге асырылады. Мұндай қылмыстардың негізгі мақсаты – заңсыз пайда табу, деректерді ұрлау, ақпаратты бүлдіру немесе қоғамға зиян келтіру. Киберқылмыстардың ерекшеліктері: (1)виртуалдылық: киберқылмыстар физикалық емес, виртуалды кеңістікте жасалады; (2)халықаралық сипаты: киберқылмыскерлер бір елдің шеңберінде әрекет етпей, халықаралық деңгейде жұмыс істей алады; (3)анонимділік: қылмыскерлердің кім екенін анықтау және

олардың орналасқан жерін табу қиын.(4)технологиялық күрделілік: заманауи құралдарды пайдалану арқылы оларды анықтау мен дәлелдеу қиынға соғады. Киберқылмыстың негізгі белгілері: цифрлық құралдарды пайдалану. Компьютер, смартфон, сервер немесе басқа технологиялар қолданылып жасалады. Ақпараттық ресурстарға бағытталған. Шабуыл ақпарат, деректер, бағдарламалар немесе жүйелерге зиян тигізуді көздейді. Құқық бұзушылық: қолданыстағы заңдарға қайшы әрекеттер жасалады (ақпаратты ұрлау, жүйені бұзу, алаяқтық). Шекаралық шектеулердің болмауы. Киберқылмыс жасаушы бір елде болуы мүмкін, ал құрбаны мүлдем басқа елде орналасуы мүмкін. Киберқылмыстар жеке тұлғаларға, бизнеске және мемлекетке әртүрлі зиян келтіреді: Жеке деректердің ұрлануы, қаржылық шығындар, беделге нұқсан келтіру. Құпия ақпараттардың жария болуы, қаржылық шығындар, жұмыс жүйесінің бұзылуы. Ұлттық қауіпсіздікке қатер, экономикалық шығындар, қоғамдық тәртіптің бұзылуы. **Киберқылмыстардың түрлері** жайында айтар болсақ, олар:

1. **Хакерлік шабуылдар (компьютерлік бұзулар):** Ақпараттық жүйелерге заңсыз кіру, деректерді ұрлау немесе бұзу. Мақсаты – деректерді жою, өзгерту немесе пайдалану.
2. **Фишинг:** Қолданушыларды алдап, жеке деректерін (құпиясөздер, банк картасының мәліметтері) алу. Әдетте жалған сайттар, электрондық хаттар немесе хабарламалар арқылы жүзеге асады.
3. **Интернет-алаяқтық:** Онлайн сауда немесе қызметтер арқылы адамдарды алдау. Жалған төлем жүйелері, инвестициялық платформалар арқылы қаражат ұрлау.
4. **Зиянды бағдарламалық жасақтама (вирус):** Компьютерлерге немесе желілерге енгізілетін бағдарламалар, олар деректерді жояды, құлыптайды немесе ұрлайды. Ransomware (файлдарды құлыптап, ақша талап ету) кең таралған.
5. **Дербес деректерді ұрлау:** Жеке тұлғалардың жеке немесе қаржылық ақпаратын заңсыз жинау және пайдалану.
6. **DDoS шабуылдары:** Веб-сайттарды немесе серверлерді шамадан тыс жүктеу арқылы олардың жұмысын тоқтату.
7. **Интернет арқылы жалған ақпарат тарату:** Қоғамдық тәртіпті бұзуға немесе жеке тұлғаларды алдауға бағытталған ақпарат тарату.
8. **Балаларға қатысты киберқылмыстар:** Кәмелетке толмағандарға қатысты интернет арқылы заңсыз әрекеттер (мысалы, құдалау, заңсыз материалдарды тарату).- деп бөлінеді.

Киберқылмыс тек құқықтық проблема емес, сонымен қатар әлеуметтік және экономикалық мәселе. Сондықтан онымен күресу үшін заңнаманы жетілдіру, киберқауіпсіздік жүйесін дамыту және халықтың цифрлық сауаттылығын арттыру маңызды.

2024 жылы Қазақстанда киберқылмыс жаңа биіктерге жетті. Мемлекеттік органдар мен жеке секторға көптеген деректердің бұзылуы мен кибершабуылдар, соның ішінде фишинг пен тыңшылық оқиғалары тіркелді. "ГТС" АҚ АҚ-ның 35 мың оқиғасын анықтады, оның 21 940-ы зиянды бағдарламамен байланысты. Пайдаланушылардың хабардарлығын арттыру үшін кибер гигиенаға ерекше назар аударылады. Кибершабуылдар IT және AI қолдану арқылы күрделене түседі, бұл қорғауды үнемі жетілдіруді қажет етеді. 2024 жылы маңызды инфрақұрылымдарға шабуылдардың өсуі болжануда.

Киберқауіпсіздік Қазақстанның цифрлық әлеміндегі басты аспектке айналуда. 2024 жылдың басында Қазақстан жаһандық киберқауіпсіздік индексінде 78-ші орынға ие болды, бұл осы саладағы шараларды күшейту қажеттігін көрсетеді. Қауіпсіздік деңгейін арттыруда АҚ саласындағы шешімдерді әзірлеумен айналысатын ірі компаниялар маңызды рөл атқарады.

Сондай-ақ Қазақстандағы оқиғалар бойынша түйінді сәттер туралы айтатын болсақ:

Фишингтік шабуылдар. 2023 жылы Қазақстанда фишингтік шабуылдардың айтарлықтай өсуі байқалды, олар, әдетте, пайдаланушылардың дербес деректерін ұрлауға бағытталған. Хакерлер фишингті корпоративті желілерге ену және банктік карта деректерін ұрлау үшін белсенді қолданды.

Кибер тыңшылық және деректердің бұзылуы. Ірі оқиғалардың бірінің шеңберінде

ірі спорт дүкенінің бірінің желісі клиенттерінің деректерінің ағуы тіркелді, оның ішінде Қазақстан азаматтарының 260 000-нан астам жазбалары бар. Сонымен бірге, мемлекеттік ұйымдарда кибершпиондардың іс-әрекеттері табылды, олар күрделі механизмдер арқылы құпия ақпаратты жасырын түрде жинап, байқалмай қалды.

IoT көмегімен шабуылдардың өсуі. 2023 жылы IoT құрылғыларына (IoT) шабуылдар әсіресе өзекті болды. Мысалы, MikroTik маршрутизаторларының осалдығы Қазақстанда осындай 5 мыңнан астам құрылғының хакерлер үшін нысанаға айналуына әкелді. Елде IoT таралуының өсуімен осы құрылғыларды басып алуға бағытталған кибершабуылдар қаупі де артып келеді[1].

Киберқылмыстарға қарсы күрестің құқықтық негіздері

Қазақстан Республикасында киберқұқық бұзушылықтарға қарсы күрес мақсатында бірнеше құқықтық нормалар мен заңдар қабылданған. Олардың ішіндегі негізгі заңдар:

- «Ақпараттандыру туралы» Заңы: Бұл заң ақпараттық жүйелер мен ресурстарды қорғау, киберқауіпсіздік шараларын реттеу, ақпараттық инфрақұрылымды дамытуға арналған. Заң ақпараттық қауіпсіздікті қамтамасыз ету бойынша мемлекеттік органдардың міндеттерін анықтайды.
- «Ақпараттық қауіпсіздік туралы» Заңы: Заң ақпараттық қауіпсіздікті қамтамасыз ету, киберқұқық бұзушылықтардың алдын алу, ақпараттық жүйелер мен желілердің қауіпсіздігін қорғау мақсатында қабылданған. Бұл заң киберқұқық бұзушылықтарды тергеу мен оларға жаза қолдану тәртібін реттейді.
- Қазақстан Республикасының Қылмыстық Кодексі: Бұл кодекс киберқұқық бұзушылықтарға жауапкершілікті белгілейді. 2014 жылғы өзгерістер бойынша, киберқұқық бұзушылықтар үшін жазалар қатайтылады, ал заңды тұлғаларға қатысты жауапкершілік енгізіледі. Мысалы, 197-бап "Компьютерлік ақпаратты жою немесе өзгерту" киберқұқық бұзушылықтары үшін қылмыстық жауапкершілікті белгілейді.

Халықаралық деңгейде киберқұқық бұзушылықтарға қарсы күрес Будапешт конвенциясы арқылы реттеледі. Бұл келісім киберқұқық бұзушылықтардың алдын алу, тергеу және жаза тағайындау механизмдеріне арналған. Будапешт конвенциясы ақпараттық технологиялардың халықаралық стандарттарын әзірлеу, киберқұқық бұзушылықтарды тергеу кезінде халықаралық ынтымақтастықты дамыту мақсатында қабылданған.

Қазақстандағы киберқылмысқа қарсы құқық қорғау органдары

Қазақстанда киберқұқық бұзушылықтарды зерттейтін және тергеумен айналысатын арнайы бөлімшелер құрылды. Олардың ішінде:

- Киберқауіпсіздік жөніндегі комитет: Бұл орган ақпараттық қауіпсіздікті қамтамасыз ету, киберқұқық бұзушылықтарды анықтау мен тергеу үшін жауапты. Комитет киберқауіпсіздік саласында мемлекеттік саясатты жүзеге асырады.
- Ұлттық қауіпсіздік комитеті (ҰҚК): Киберқұқық бұзушылықтарға қарсы күрес жүргізеді, құқық қорғау органдарының үйлестіруші рөлін атқарады. ҰҚК киберқұқық бұзушылықтарды тергеу, оларға құқықтық жауапкершілікке тарту шараларын жүзеге асырады.

Киберқұқық бұзушылықтарды тергеу механизмдері түрлі қадамдарды қамтиды. Бұларға жедел-іздестіру шаралары, ақпараттық жүйелер мен желілерді тексеру, құқық бұзушыларды ұстап, оларға қатысты қылмыстық іс қозғау жатады. Мұндай тергеулер құқық қорғау органдарының мамандарымен, киберқауіпсіздік жөніндегі эксперттермен бірлесе жүзеге асырылады[2].

Халықаралық тәжірибе

Киберқылмыстардың жаһандық сипаты оларға қарсы күресте халықаралық ынтымақтастықтың қажеттілігін айқын көрсетеді. Әр мемлекет өз заңнамасы мен технологияларын жетілдірумен қатар, басқа елдермен бірлесіп жұмыс істейді. Халықаралық тәжірибеде киберқылмыстарға қарсы бірнеше тиімді әдістер қалыптасқан. **Халықаралық келісімдер мен конвенциялар:**

1. **Будапешт конвенциясы (2001 ж.)** [3]

Бұл – киберқылмыстарға қарсы күрес бойынша ең маңызды халықаралық құжат. Ол киберқылмыстарды анықтау, алдын алу және жазалау мақсатында мемлекеттер арасында ынтымақтастық орнатуды көздейді. Конвенцияға мүше елдер киберқылмыстардың ортақ анықтамасын бекітіп, құқықтық нормаларын үйлестіреді. Қазақстан бұл конвенцияға әлі қосылған жоқ, бірақ қосылу мүмкіндігі қарастырылуда.

2. **INTERPOL және Europol қызметі**[4]

Халықаралық полиция ұйымдары киберқылмыстармен күрес бойынша елдерге көмек көрсетеді. INTERPOL-дің Киберқауіпсіздік бөлімі кибершабуылдарды бақылап, елдер арасында ақпарат алмасуды қамтамасыз етеді. Europol-дің EC3 (Еуропалық киберқылмыс орталығы) интернет-алаяқтық, балаларды қудалау және басқа да қылмыстармен күрес жүргізеді.

Киберқауіпсіздікті қамтамасыз ету бойынша ұлттық бағдарламалар:

АҚШ: Cybersecurity and Infrastructure Security Agency (CISA): АҚШ-та киберқауіпсіздікті қамтамасыз ету бойынша басты агенттік. Ұлттық киберқауіпсіздік стратегиясы арқылы мемлекет жеке және мемлекеттік сектор арасында ынтымақтастық орнатып, кибершабуылдардың алдын алуға бағытталған іс-шараларды жүзеге асырады.

Еуропалық Одақ: ЕО елдері үшін Киберқауіпсіздік актісі қабылданған. Бұл құжат арқылы қауіпсіздік стандарттары бекітіліп, ортақ киберқауіпсіздік стратегиялары жүзеге асырылады. ENISA (ЕО-ның Киберқауіпсіздік агенттігі): Еуропа елдері арасындағы ақпарат алмасуды басқарады және оларға техникалық көмек көрсетеді.

Қытай: "Ұлттық киберқауіпсіздік заңы" арқылы интернеттегі бақылауды күшейтіп, кибершабуылдарға қарсы тұру үшін жергілікті инфрақұрылымды жетілдіреді. Хакерлік әрекеттер мен интернет алаяқтықтарына қатаң шаралар қолданады.

Халықаралық ынтымақтастық және киберқауіпсіздік форумдары:

- "G7" және "G20" саммиттері: Киберқылмыстармен күрес мәселелері жиі талқыланады. Олар арқылы елдер арасында тәжірибе алмасу мен ортақ стратегия құру талпыныстары жасалады.
- "FIRST" (Incident Response Teams): Әртүрлі елдердегі оқиғаға жедел әрекет ету топтары бірігіп, кибершабуылдарға тез жауап береді[5].

Техникалық және құқықтық шаралар: Киберқауіпсіздік хабтарын құру: Мысалы, Сингапурда киберқауіпсіздікке арналған зерттеу орталықтары жұмыс істейді. Зиянды бағдарламаларды анықтайтын технологияларды дамыту: Ірі корпорациялар (Google, Microsoft) үкіметтермен бірлесіп кибершабуылдарды бақылауға арналған құралдар жасайды. Құқықтық жүйені үйлестіру: Халықаралық ынтымақтастық аясында елдер арасында киберқылмыскерлерді экстрадициялау және қылмыстық істерді бірлесіп тергеу мәселелері шешілуде.

Қазақстанның халықаралық тәжірибені пайдалану мүмкіндіктері:

Қазақстан халықаралық стандарттарға сай киберқауіпсіздік жүйесін дамытуға мүдделі. Будапешт конвенциясына қосылу, INTERPOL және Europol ұйымдарымен тығыз байланыс орнату, сондай-ақ кибершабуылдарға жедел әрекет ету жүйесін жетілдіру Қазақстанның киберқылмыстармен күрес әлеуетін арттыруға көмектеседі. Халықаралық тәжірибе көрсеткендей, киберқылмыстармен күресте тиімді нәтижеге қол жеткізу үшін елдер арасында ынтымақтастық пен заманауи технологияларды пайдалану басты рөл атқарады.

Қиындықтар мен мәселелер

Киберқылмыстарды анықтау және дәлелдеу – қазіргі құқық қорғау органдары мен сот жүйесінің алдында тұрған күрделі міндеттердің бірі. Бұл қиындықтар киберқылмыстардың табиғаты, технологиялардың күрделілігі және халықаралық сипатымен байланысты. Мысалы: киберқылмыстардың анонимділігі. Киберқылмыскерлер өздерінің әрекеттерін жасыру үшін прокси-серверлер, VPN, TOR сияқты анонимді желілерді пайдаланады. Бұл олардың нақты орналасқан жерін анықтауды қиындатады. Желіаралық шекаралардың болмауы. Киберқылмыстар жиі халықаралық деңгейде жасалады. Қылмыскер бір елде орналасса, оның

құрбаны мүлдем басқа елде болуы мүмкін. Мемлекеттер арасындағы құқықтық көмек көрсету келісімдерінің болмауы тергеу процесін қиындатады. Кейбір елдерде киберқылмыстарға қатысты нақты заңдар мен реттеулер жеткіліксіз. Халықаралық заңнамалық нормалардың үйлестірілмеуі қылмыскерлердің жауапкершіліктен жалтаруына мүмкіндік береді. Сонымен қатар көптеген елдерде құқық қорғау органдарының киберқылмыстарды анықтау үшін қажетті техникалық құралдары мен сарапшылары жеткіліксіз. Қылмыскерлер күрделі шифрлау және деректерді жою технологияларын қолданған жағдайда дәлелдерді жинау қиынға соғады. Киберқылмыстардың дәлелдері (электронды хаттар, желілік журналдар, деректер) тез өзгеруі немесе жойылуы мүмкін. Құқық қорғау органдары дәлелдерді жинау барысында заңнама талаптарын (мысалы, жеке деректерді қорғау туралы заңдарды) бұзбауы керек, бұл процесті қиындатады. Сараптамалық қорытындылардың күрделілігі киберқылмыстарды дәлелдеу үшін IT сарапшыларының көмегі қажет етеді. Алайда мұндай сараптамалар ұзақ уақыт алуы мүмкін және олардың нәтижелері әрдайым түсінікті бола бермейді. Кейбір жағдайларда сарапшылардың қорытындылары сот үшін жеткіліксіз немесе нақты емес болып саналады. Киберқылмыскерлер техникалық тұрғыда жоғары білімді және соңғы технологияларды меңгерген. Олар өз әрекеттерін жасырудың жаңа тәсілдерін үнемі жетілдіріп отырады. Оларға қарсы әрекет ету үшін құқық қорғау органдарының да біліктілігі жоғары болуы керек. Киберқылмыстардың салдары жылдам таралуы мүмкін (мысалы, зиянды бағдарламалар бірнеше минутта мыңдаған құрылғыны зақымдауы мүмкін). Мұндай жағдайларда қылмыскерлерді іздеу мен дәлелдерді жинау жылдам әрекетті талап етеді, бұл әрдайым мүмкін бола бермейді.

Шешу жолдары мен ұсыныстар

Киберқылмыстардың қарқынды өсуі оларға қарсы күресудің кешенді шараларын талап етеді. Технологиялардың дамуына сай қылмыскерлердің әдістері де күрделене түсуде, сондықтан шешу жолдары құқықтық, техникалық және әлеуметтік деңгейлерде жүзеге асырылуы қажет.

1. Құқықтық базаны жетілдіру. Киберқылмыстарға қатысты заңнаманы жетілдіру, жаңа қауіп-қатерлерді ескеретін нормативтік актілер қабылдау. Қазақстанның Будапешт конвенциясына қосылуы арқылы халықаралық стандарттарға сәйкес келу.

2. Жауапкершілікті күшейту. Киберқылмыстар үшін жазаны қатайту (мысалы, ақпараттық жүйелерге заңсыз кіру немесе деректерді ұрлау). Киберқылмысқа қатысы бар ұйымдар мен тұлғалар үшін әкімшілік немесе қылмыстық жауапкершілік енгізу.

3. Киберқауіпсіздік инфрақұрылымын дамыту. Мемлекеттік және жеке секторда ақпараттық жүйелерді қорғау үшін қауіпсіздік шараларын (Firewall, антивирус, шифрлау) енгізу. Кибершабуылдарға жедел әрекет ету орталықтарын (CERT) құру және олардың тиімді жұмысын қамтамасыз ету.

4. Заманауи технологияларды пайдалану. Жасанды интеллект пен Big Data технологияларын киберқылмыстарды анықтау және алдын алу үшін қолдану. Зиянды бағдарламаларды, фишингтік сайттарды және басқа да қауіп-қатерлерді анықтайтын автоматтандырылған жүйелерді дамыту.

5. Желілік қауіпсіздікті бақылау. DDoS-шабуылдарына қарсы құралдарды енгізу және зиянды трафикті бақылау. Мемлекеттік және ірі жеке ұйымдардың ақпараттық жүйелерін тұрақты түрде тестілеу және аудит жүргізу.

6. Цифрлық сауаттылықты арттыру. Халық арасында киберқауіптерден сақтану әдістері бойынша тұрақты тренингтер мен семинарлар өткізу. Әсіресе, балалар мен жастарды интернеттегі қауіпсіздікке үйрету.

7. Құқық қорғау органдарын оқыту: Тергеушілер мен IT-мамандарды киберқылмыстарды анықтау және тергеу бойынша арнайы оқыту. Мамандарды халықаралық тәжірибе алмасуға тарту.

8. Ақпараттық кампаниялар. Халыққа фишинг, алаяқтық және зиянды бағдарламалар туралы ақпарат беру. Кибершабуылдарға қарсы өзін-өзі қорғау әдістерін насихаттау.

Қорытындылай келе, Киберқылмыстар – ақпараттық технологиялардың дамуымен