ЦИФРЛЫҚ КЕҢІСТІКТЕГІ ҚЫЛМЫСТЫҚ ҚҰҚЫҚ БҰЗУШЫЛЫҚТАР

Мухаметжанова Ж.
«Құқықтану» білім бағдарламасы бойынша 3 курс студенті Е.А.Бөкетов атындағы Қарағанды ұлттық зерттеу университеті

Ғылыми жетекші: Алтайбаев С.Қ., з.ғ.к., қауымдастырылған профессор (доцент) Қылмыстық құқық, процесс және криминалистика кафедрасының қауымдастырылған профессоры

Цифрлық трансформация дәуірінде ақпараттық технологиялар адам өмірінің барлық саласына еніп, жаңа мүмкіндіктермен қатар жаңа қауіптерді де туындатуда. Интернет пен ақпараттық жүйелер арқылы жасалатын қылмыстар – қазіргі құқық қорғау органдарының ең өзекті мәселелерінің бірі. Мұндай әрекеттер «цифрлық кеңістіктегі қылмыстар» немесе «киберқылмыстар» деп аталады. Қазақстан Республикасының Қылмыстық кодексі бұл бағытта арнайы баптар арқылы жауаптылық көздейді.

Мақаланың мақсаты – цифрлық кеңістіктегі қылмыстардың мәнін ашу, олардың түрлерін, ерекшеліктерін, құқықтық реттелуін және қазіргі кездегі мәселелерін талдау.

Цифрлық қылмыстар - бұл дәуірдің басты қайшылығын көрсету: адамзат технология арқылы өмірін жеңілдеткен сайын, сол технология оның қауіпсіздігіне жаңа қатер төндіруде. Бүгінде ақпарат – билік пен байлықтың кілті. Ал оны қорғау – тек техникалық емес, ең алдымен құқықтық және адамгершілік міндет.

Цифрлық кеңістіктегі қылмыстар қоғамға көрінбейтін, бірақ нақты қауіп төндіреді: адамның жеке өміріне қол сұғу, жалған ақпарат тарату, қаржы алаяқтығы, ұлттық қауіпсіздікке қатер. Мұндай қылмыстардың қауіптілігі – олардың шекарасыз және анонимді болуы. Сондықтан мақаланың негізгі идеясы- технологиялық прогресс пен құқықтық сананың тең дамуы. Яғни, адамзат тек жаңа цифрлық құралдарды игеріп қана қоймай, сонымен бірге жауапкершілік мәдениетін де қалыптастыруы қажет.

1. Құқықтық негіздер

Қазақстанда цифрлық кеңістіктегі қылмыстарды реттейтін құқықтық база қалыптасқан. Негізгі құқықтық актілер қатарына Қазақстан Республикасының Қылмыстық кодексінің 205–213-баптары жатады, онда ақпараттық жүйелерге заңсыз кіру, ақпаратты өзгерту немесе жою, сондай-ақ жүйенің қызметін бұзу сияқты әрекеттер үшін жауаптылық белгіленген [1]. Сонымен қатар «Жеке деректер және оларды қорғау туралы» 2013 жылғы 21 мамырдағы №94-V ҚР Заңы жеке тұлғалардың ақпараттық қауіпсіздігін қамтамасыз етуге бағытталған [2].

Мемлекет киберқауіпсіздік деңгейін арттыру мақсатында «Қазақстанның киберқалқаны» тұжырымдамасын қабылдады [3]. Бұл құжат ұлттық ақпараттық инфрақұрылымды қорғау және цифрлық қауіптерге жедел ден қоюды көздейді.

Цифрлық қылмыстарды жасау үшін шекара, уақыт немесе қашықтық кедергі болмайды.

Мысалы, бір хакер басқа елден отырып-ақ банктің ақпараттық жүйесін бұзып, миллиондаған теңгені иемдене алады. Бұл қылмыстардың жасырын және трансшекаралық сипаты олардың анықталуын қиындатады.

Киберқылмыстар мемлекет пен бизнеске үлкен қаржылық шығын әкеледі:

• интернет-алаяқтық, фишинг, төлем жүйелерін бұзу;

• компаниялардың деректерін ұрлау немесе шифрлап, «шифрды шешу үшін ақша талап ету» (ransomware).

2024 жылы Қазақстандағы кибершабуылдардан экономикалық залал шамамен 15 млрд теңге деп бағаланған [KZ-CERT деректері].

Азаматтардың жеке деректері мен жеке өмірі қауіпке ұшырайды:

• банк картасының нөмірі, жеке куәлік, мекенжай немесе пароль ұрлануы мүмкін;

• интернеттегі фейк-парақшалар арқылы беделге нұқсан келтіру жағдайлары жиілеп кетті.

2025 жылы 16 миллион қазақстандықтың деректері интернетке тарап кеткен оқиға – соның айқын дәлелі. Кибершабуыл тек жеке адамдарға емес, мемлекеттік органдар мен инфрақұрылымға да бағытталуы мүмкін.

Мысалы: мемлекеттік сайттар мен деректер базасына шабуыл; энергетикалық, көлік немесе қаржы жүйелерін істен шығару.

Мұндай әрекеттер елдің тұрақтылығына тікелей қауіп төндіреді.

Цифрлық кеңістіктегі қылмыстарды дәлелдеу қиын, себебі: киберіздерді жасыру оңай; қылмыскерлер шетелдік серверлерді пайдаланады; электрондық дәлелдер тез жойылып кетуі мүмкін.

Бұл құқық қорғау органдарына қосымша жүктеме әкеледі. Мұндай қылмыстар көбейген сайын азаматтар интернет пен электрондық қызметтерге сенімін жоғалтады. Бұл өз кезегінде мемлекеттің «цифрлық экономика» және «электронды үкімет» жобаларына теріс әсер етеді.

Цифрлық кеңістіктегі қылмыстардың басты қауіптілігі – олардың жасырын, жаппай және шекарасыз сипатында. Олар жеке тұлғалардың құқығын, мемлекеттің қауіпсіздігін және экономиканың тұрақтылығын бұзады. Сондықтан бұл бағытта тек құқықтық емес, техникалық және білім беру шаралары да бір мезгілде жүргізілуі тиіс.

2. Цифрлық қылмыстардың негізгі түрлері

Цифрлық кеңістіктегі қылмыстардың негізгі түрлері төмендегідей: ақпаратқа, ақпараттық жүйеге немесе телекоммуникациялар желісіне құқыққа сыйымсыз қол жеткізу (ҚР ҚК 205-бап); ақпараттық жүйенің немесе телекоммуникациялар желісінің жұмысын бұзу (ҚР ҚК 207-бап); ақпаратты құқыққа сыйымсыз жою немесе түрлендіру (ҚР ҚК 206-бап); алаяқтық (ҚР ҚК 190-бап).

Соңғы жылдары интернет арқылы жасалатын алаяқтықтар саны күрт артты. Ішкі істер министрлігінің деректері бойынша, 2018 жылы киберқылмыстар саны 589 болса, 2021 жылы ол 21 479-ға дейін өскен [4]. Ал 2024 жылы ұлттық KZ-CERT тобы 68 100 оқиғаны тіркеген [5].

3. Тергеу және дәлелдеу ерекшеліктері

Цифрлық қылмыстарды тергеу барысында негізгі қиындықтардың бірі – электрондық дәлелдемелерді жинау мен бекіту. Тергеу органдары ақпараттық жүйелерге қол жеткізу үшін сот санкциясын алуы қажет. Электрондық пошта, әлеуметтік желілердегі хаттар, IP-адрестер мен лог-файлдар дәлелдеме ретінде қарастырылады.

Бірақ мұндай дәлелдерді алу кезінде деректердің өзгертіліп кету қаупі жоғары. Сондықтан криминалистика мен сот сараптамасында цифрлық дәлелдемелерді бекітудің арнайы әдістері қолданылуда [6].

4. Мәселелері мен шешу жолдары

Цифрлық кеңістіктегі қылмыстардың алдын алу мен тергеу саласында келесі мәселелер бар: халықаралық ынтымақтастықтың жеткіліксіздігі; техникалық мамандардың тапшылығы; азаматтардың цифрлық сауаттылығының төмендігі; дербес деректердің қорғалмауы.

Осы мәселелерді шешу үшін Қазақстанда киберқауіпсіздік саласында кадрларды даярлау, құқықтық актілерді жаңарту және халықаралық ұйымдармен серіктестік орнату бағытында жұмыс жүргізілуде [7].

5. Перспективалар

Болашақта цифрлық кеңістіктегі қылмыстармен күресті күшейту үшін құқық қорғау органдарының техникалық жабдықталуын арттыру, жасанды интеллект арқылы қауіптерді болжау, электрондық дәлелдемелерді автоматты түрде тіркеу жүйелерін енгізу жоспарлануда. Сондай-ақ халықтың ақпараттық қауіпсіздік мәдениетін арттыру басты бағыттардың бірі болып қала береді [8].

6. Құқықтық-реттеушілік шаралар

1.1. Қылмыстық және процессуалдық нормаларды жаңарту

• ҚК-ге жаңа технологиялар (AI, блокчейн, криптовалюта) қолданылатын қылмыс түрлерін нақтыратын баптар қосу;

• Электрондық дәлелдемелерді алу және сақтауға қатысты процессуалдық рәсімдерді айқындау (сот санкциясы, электрондық мөрлеу, уақытша блоктау тетіктері).

Іске асыру: заң жобаларын дайындау, қоғамдық талқылау, парламент мақұлдауы.

Жауапты: Парламент, ҚДМ, Бас прокуратура.

1.2. Мәліметтерді қорғау және міндетті хабарлау. Деректердің бұзылуы (data breach) анықталғанда міндетті түрде уақытылы хабарлау механизмін енгізу (мысалы 72 сағат ішінде);

• Техникалық және әкімшілік талаптарды (шифрлау, рұқсат етілген қолжетімділік) заңда бекіту.

Жауапты: Ұлттық заң шығарушы органдар, Цифрлық даму министрлігі.

1.3. Жазалардың сәйкестігі мен профилактика. Киберкриминал үшін жазаларды экономикалық тиімді тоқтатпайтындей, превенцияны ынталандыратын түрде реттеу.

Жауапты: Заң шығарушы және сот жүйесі.

1.4. Техникалық және институционалдық шаралар. KZ-CERT институтын техникалық, кадрлық және қаржылай қамтамасыз ету; өңірлік және секторлық CSIRT-тер құру.

Жауапты: Үкімет, министрліктер, іскер орта.

Инфрақұрылымды нығайту (жүйелік аудиттар және стресс-тестілеу). Мемлекеттік және маңызды инфрақұрылымдарға периодтық пентест және қауіпсіздік аудиттары міндетті болуы.

Жауапты: Министрліктер, операторлар, тәуелсіз аудит фирмалары.

Кибербәкітілген платформа және қауіп-анықтау (SIEM, EDR). Үлкен деректерді талдайтын SIEM жүйелерін енгізу, эндпойнт қорғау (EDR), желілік мониторинг.

Жауапты: Ұлттық инфрақұрылым операторлары, коммерциялық сектор.

Сандарды және криптографияны қолдану. Құпиялылық пен деректер тұтастығын шифрлау арқылы қорғау; күшті аутентификация (MFA) енгізу.

Жауапты: Банк секторы, IT-компаниялар.

1.5. Құзыреттілік пен кадрлар даярлау. Киберқауіпсіздік мамандарын даярлау

• Университеттерде мамандандыру, кәсіптік курстар, сертификаттау (мемлекеттік гранттар мен ынталандырулар).

Жауапты: Білім министрлігі, ЖОО, жеке сектор.

Тергеушілер мен сот сарапшыларын оқыту

• Сандық криминалистика курстары, шетелдік тәжірибе алмасу, лабораториялар жабдықтау.

Жауапты: ІІМ, Бас прокуратура, сот сараптамасы институты.

1.6. Халықаралық ынтымақтастық

Халықаралық келісімдер мен ақпарат алмасу

• Еуропа Кеңесі, Интерпол, CERT-тер арасында жылдам ақпарат алмасу хаттамаларын енгізу.

Жауапты: Сыртқы істер министрлігі, ІІМ.

Техникалық көмек және тәжірибе алмасу

• Қаржылық және техникалық көмек алу, бірлескен тренингтер мен операциялар.

Жауапты: Үкімет, халықаралық серіктестер.

1.7. Қоғамдық білім және алдын алу (awareness)

Жаппай ақпараттандыру кампаниялары

• Азаматтарға фишингтен, пароль қауіпсіздігінен, интернет-алаяқтықтан қорғанудың қарапайым ережелерін үйрету.

Жауапты: Цифрлық даму министрлігі, БАҚ, коммерциялық сектор.

Мектептер мен ЖОО-ларда кибергигиена

• Бағдарламалау мен қауіпсіздік негіздерін ерте жастан оқыту.

Жауапты: Білім министрлігі, мектептер.

1.8. Превенция және бизнес-арадағы келісімдер

Міндетті қауіпсіздік стандарттары және сертификаттау

• Ақпараттық жүйелерге арналған ұлттық стандарттар (немесе халықаралық ISO 27001 тәрізді талаптар) енгізу.

Жауапты: Стандарттау органдары, министрліктер.

• Тергеу барысында серверлер мен домендерді уақытша бұғаттау, халықаралық сұраныстарды жедел орындау механизмдері.

Жауапты: ІІМ, Бас прокуратура, соттар.

1.9. Технологиялық инновацияларды қолдану

• Жасанды интеллект және машиналық оқыту. Аномалияларды анықтайтын модельдер арқылы шабуылдарды алдын ала анықтау.

• Блокчейн негізінде сенімді аудит. Құжаттардың тұтастығын және жолдарын тіркейтін блокчейн-решенияларды енгізу (мысалы электронды мөрлеу).

Жауапты: Қаржы және мемлекеттік қызмет саласы.

Қорытындылай келе, цифрлық кеңістіктегі қылмыстар қазіргі қоғам үшін үлкен қауіптің бірі болып табылады. Бұл қылмыстардың сипаты шекарасыз және ауқымды болғандықтан, онымен күресу тек ұлттық деңгейде ғана емес, халықаралық деңгейде де үйлестірілуі қажет. Қазақстанда құқықтық база қалыптасқанымен, тәжірибеде оны қолдану мен техникалық қамтамасыз ету әлі де жетілдіруді қажет етеді. Цифрлық ортадағы қауіп тек жеке тұлғаға ғана емес, тұтас қоғамның экономикалық, ақпараттық

және ұлттық қауіпсіздігіне тікелей әсер етеді. Сондықтан мұндай қылмыстармен күрес тек құқық қорғау органдарының міндеті емес — бұл мемлекет, қоғам және әрбір азаматтың ортақ жауапкершілігі.

Бүгінгі таңда басты мақсат – технологияны шектеу емес, оны қауіпсіз әрі жауапкершілікпен қолдану мәдениетін қалыптастыру. Қылмыстық заңнаманы жетілдіру, цифрлық сауаттылықты арттыру, халықаралық ынтымақтастық пен киберқауіпсіздік инфрақұрылымын дамыту- осы бағыттағы негізгі басымдықтар болып табылады. Шын мәнінде, цифрлық кеңістіктегі қауіпсіздік тек техникалық қорғаныс жүйелеріне емес, адамның сана деңгейіне және құқықтық мәдениетіне байланысты. Егер әрбір азамат өз ақпараттық мінез-құлқына саналы түрде жауап беруді үйренсе, цифрлық қылмыстардың алдын алу әлдеқайда тиімді болар еді.

Сондықтан XXI ғасырдағы басты міндет – технологиялық прогресс пен құқықтық жауапкершілікті үйлестіре отырып, қауіпсіз және сенімді цифрлық қоғам құру.

Әдебиеттер тізімі:

1. Қазақстан Республикасының Қылмыстық кодексі. 2014 жылғы 3 шілде № 226-V. https://adilet.zan.kz/kaz/docs/K1400000226
2. «Жеке деректер және оларды қорғау туралы» Қазақстан Республикасының Заңы. 2013 жылғы 21 мамыр №94-V. https://adilet.zan.kz/kaz/docs/Z1300000094
3. ҚР Үкіметінің «Қазақстанның киберқалқаны» тұжырымдамасы туралы қаулысы. 2017 ж. https://adilet.zan.kz/kaz/docs/P1700000407
4. ҚР ІІМ ресми деректері, 2021 ж. Киберқылмыстар статистикасы. https://www.gov.kz/memleket/entities/maidd/press/news/details/765931
5. KZ-CERT ұлттық тобының есебі, 2024 ж. https://aifc.kz/wp-content/uploads/2024/09/aifc_kaz_final-1.pdf
6. Сот сараптамасы институтының «Цифрлық дәлелдемелерді пайдалану» әдістемелік нұсқаулығы, 2023 ж. https://adilet.zan.kz/kaz/docs/Z100000261_
7. ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігінің есебі, 2024 ж. https://adilet.zan.kz/kaz/docs/V2400034739
8. Eurasian Research Institute. “Cybersecurity Trends in Kazakhstan”. 2025 ж. https://www.nucamp.co/blog/coding-bootcamp-kazakhstan-kaz-kazakhstan-cybersecurity-job-market-trends-and-growth-areas-for-2024

БҰЛТАРТПАУ ШАРАЛАРЫН ҚОЛДАНУДЫҢ НЕГІЗДЕРІ МЕН ШАРТТАРЫ

Абзалбекова М. Т. Қылмыстық құқық, процесс және криминалистика кафедрасының аға оқытушысы, Заң ғылымдарының магистрі

Болат Д.Б. Оңтүстік Шығыс ПБ тергеу бөлімшесінің тергеушісі, полиция лейтенанты

Нариманқызы Н. Соттық және прокурорлық қызмет білім беру бағдарламасының 3 курс студенті

Академик Е. А. Бөкетов атындағы Қарағанды ұлттық зерттеу университеті

Қазақстан Республикасының қылмыстық процесіндегі бұлтартпау шарасын құқықтық реттеу саласындағы ғылыми зерттеулердің ең негізгі бағыты болып келесідей маңызды сұрақтарды жүзеге асырылуы табылады. Қылмыстық іс жүргізу барысында құқықтық және заңдылық тәртіптің сақталуы қылмысты ашудың тиімділігін қамтамасыз ететін негізгі алғышарттардың бірі. Себебі дәл осы қағидатты ұстану құқықтық мемлекет құрудың іргетасын қалау болып табылады. Заңдылық пен тәртіп сақталуы әділ шешім шағырудың басты кепілі.

Қылмыстық іс жүргізу басталғаннан сәттен бастап, ақиқатты ту етіп, кінәлі тұлғаны жауапкершілікке тарту, ал кінәсіз адамды кінәсіздік презумпциясына негізінде ақтап алу заңдылықтың басты белгісі. Осы сәтте қылмыстық іс жүргізу барысында бұлтартпау шаралары маңызды орын алады. Сот әділдігін қамтамасыз етіп, субъектілердің негізгі құқықтарын қорғайды.

Қылмыстық процестегі бұлтартпау шаралары – күдікті немесе айыпталушының іс жүргізуден жалтармауын, әділ сот талқылауын қамтамасыз етуге бағытталған қылмыстық іс жүргізу мәжбүрлеуінің