

11 Luzhinskaya Ye. L. *Algoritm deystviy eksperta na etape issledovaniya tsifrovyykh foto- i videoizobrazheniy. //Materialy Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Vostok-Zapad: partnerstvo v sudebnoy ekspertize. Aktual'nyye voprosy teorii i praktiki sudebnoy ekspertizy», g. Almaty, 27 oktyabrya 2016 g. - Almaty: MU RK. Tsentr sudebno-meditinskoy ekspertizy, 2016. – S. 263-266.*

12 Shved A. YA. *Vidy zakonov, sostavlyayushchikh predmet teorii sudebnoy ekspertizy. //Materialy Mezhdunarodnoy nauchno-prakticheskoy konferentsii «Vostok-Zapad: partnerstvo v sudebnoy ekspertize. Aktual'nyye voprosy teorii i praktiki sudebnoy ekspertizy», g. Almaty, 27 oktyabrya 2016 g. – Almaty: MU RK. Tsentr sudebno-meditinskoy ekspertizy, 2016.- S. 463-466.*

13 *Tsifrovoy Kazakhstan - Gosudarstvennaya programma. Prinyat postanovleniyem Pravitel'stva Respubliki Kazakhstan ot 12 dekabrya 2017 goda № 827. //https://adilet.zan.kz/rus/docs/P1700000827/ Utratil silu postanovleniyem Pravitel'stva Respubliki Kazakhstan ot 17 maya 2022 g. № 311. (data obrashcheniya: 18.11.2024 g.).*

14 *Pravila primeneniya nauchno-tekhnicheskikh sredstv fiktsatsii khoda i rezul'tatov sledstvennykh deystviy. - Utverzhdeno prikazom General'nogo prokurora Respubliki Kazakhstan ot 22 sentyabrya 2013 goda № 91//https://adilet.zakon.kz>rus>docs/ (data obrashcheniya: 18.11.2024).*

МРНТИ: 10.79.01.  
УДК: 343.1

10.51889/2959-6181.2024.78.4.009

*Т.Б. Хведелидзе<sup>1</sup>, Э.П. Кенжибекова<sup>1\*</sup>*

*<sup>1</sup>Абай атындағы Қазақ ұлттық педагогикалық университеті  
(e-mail: khvedelidze\_tima@mail.ru, \*danaestai@mail.ru)*

## **ҚЫЛМЫСТЫҚ ІСТЕР БОЙЫНША СОТ САРАПТАМАСЫ ОБЪЕКТІЛЕРІ РЕТІНДЕ ЦИФРЛЫҚ ТЕХНОЛОГИЯЛАРДЫ ЗАҢСЫЗ МАНИПУЛЯЦИЯЛАУ**

### *Аңдамна*

Қазақстанда цифрлық технологияларды енгізудің бірден бір дәлелі болып 2017-2022 жылдар аралығына бағытталған 2017 жыл 12 желтоқсанындағы «Цифрлы Қазақстан» Мемлекеттік бағдарламасын жүзеге асыру табылады. Аталған бағдарламаның негізгі бағыттары болып: жоғары әлеуметтік сұраныстарға ие болатын қаржы-экономикалық қатынастар табылады. Осыған орай, цифрландыру еліміздің тиісті қаржы-экономикалық құрылымдарының әкімшілік-басқару аппаратын күнделікті жұмыстан босатуға, пайдаланушыға транзакциялардың жылдамдығына ғана емес, сонымен қатар деректер базасына оңай қол жеткізу, сенімділігі мен рұқсат етілмеген әрекеттерден қорғалуына кепілдік беруге арналған үлкен деректер базасын заңсыз пайдаланудың нақты қаупіне ұшырады. Цифрлық технологиялар саласына рұқсатсыз ену фактілерін танудың сот-сараптама тәжірибесімен әзірленген қолданыстағы әдістері қылмыскерлердің цифрлық технологияларды қылмыстық айла-шарғыдан қорғаудың кез келген жаңартылған жағдайлары мен әдістерін имитациялау қабілетінің жоғары болуына байланысты тез ескіруде. Қылмыстық істер бойынша ақпараттық – байланыс технологиялар саласында күрделі сараптамалық зерттеулер жүргізуді қажет етеді.

**Түйін сөздер:** қылмыстық істер бойынша дәлелдеу, ақпараттық-байланыс технологиялар, сот сараптамасы, арнайы ғылыми білімдер, киберқауіпсіздік, мәліметтер базасына рұқсатсыз қол жеткізу.

Т.Б.Хведелидзе <sup>1</sup>, Э.П.Кенжибекова <sup>1</sup>

<sup>1</sup>Казахский национальный педагогический университет имени Абая

## НЕПРАВОМЕРНЫЕ МАНИПУЛЯЦИИ ЦИФРОВЫМИ ТЕХНОЛОГИЯМИ КАК ОБЪЕКТЫ СУДЕБНЫХ ЭКСПЕРТИЗ ПО УГОЛОВНЫМ ДЕЛАМ

### *Аннотация*

Внедрение в Казахстане цифровых технологий является одним из результатов реализации Государственной программы «Цифровой Казахстан» от 12 декабря 2017 года, рассчитанной на период 2017-2022 гг. Основными приоритетами названной Программы являлись: финансово-экономические отношения, обусловленные высоким социальным запросом. Наряду с этим, цифровизация, призванная освободить административно-управленческий аппарат соответствующих финансово-экономических структур страны от рутинной работы, гарантировать пользователю не только быстроту совершаемых операций, но и надежность и защиту базы данных от неправомерного доступа, на поверку оказалась под реальной угрозой незаконного манипулирования базами больших данных. Существующие способы распознавания фактов несанкционированного вторжения в область цифровых технологий, наработанные судебно-экспертной практикой, быстро устаревают ввиду того, что криминалитет обладает высокими способностями мимикрии к любым обновленным условиям и способам защиты цифровых технологий от преступного манипулирования ими. Доказывание по уголовным делам нуждается в производстве сложных экспертных исследований в области информационно-коммуникационных технологий.

**Ключевые слова:** доказывание по уголовным делам, информационно-коммуникационные технологии, судебная экспертиза, специальные научные знания, кибербезопасность, несанкционированный доступ к базам данных.

*T.B. Khvedelidze<sup>1</sup>, E.P. Kenzhebekova<sup>1</sup>*

<sup>1</sup>*Abai Kazakh National Pedagogical University*

## UNLAWFUL MANIPULATION OF DIGITAL TECHNOLOGIES AS OBJECTS OF FORENSIC EXPERTISE IN CRIMINAL CASES

### *Abstract*

The introduction of digital technologies in Kazakhstan is one of the results of the implementation of the State Programme 'Digital Kazakhstan' dated 12 December 2017, designed for the period 2017-2022. The main priorities of the named Programme were: financial and economic relations due to high social demand. At the same time, digitalisation, designed to free the administrative and management apparatus of the relevant financial and economic structures of the country from routine work, to guarantee the user not only the speed of operations, but also the reliability and protection of the database from unlawful access, turned out to be a real threat of illegal manipulation of big data databases. The existing methods of recognition of the facts of unauthorised intrusion into the field of digital technologies, developed by forensic practice, are quickly becoming obsolete due to the fact that criminals have a high ability of mimicry to any updated conditions and ways to protect digital technologies from criminal manipulation of them. Evidence in criminal cases requires the production of sophisticated expert research in the field of information and communication technologies.

**Keywords:** evidence in criminal cases, information and communication technologies, forensic expertise, special scientific knowledge, cyber security, unauthorised access to databases.

### *Негізгі ережелер*

2017 жылғы 12 желтоқсандағы «Цифрлы Қазақстан» мемлекеттік бағдарламасын жүзеге асыру (әрмен қарай - Бағдарлама), өз өзектілігін 2022 жылға дейін сақтады [1]. Осы аталған Бағдарлама арқасында түрлі өмір сүру мен қоғамдық қызметтер аясын цифрландыру деңгейі мен сапасы бойынша, замануи Қазақстан елі әлемдік мемлекеттер рейтингінде көшбасшы орындардың бірін иеленетіндігі баршамызға белгілі. Цифрландыру барысы мен оның қамтитын қоғамдық қатынастар саласы мен ортасы өсу мен жетілдірілу тенденцияларына тікелей байланысты. Цифрландыру бағдарламасын жүзеге асыру елімізде ақпараттық-коммуникациялық технологияларды кеңейту, жаңғырту және меңгеру бойынша жұмысты аяқтаған жоқ. Цифрландыру әлеуметтік құбылыстан әлеуметтік маңызды құбылысқа айналды, бұл қоғамның цифрландырудың жүріп жатқан процестерді бақылау және басқарудағы артықшылықтарына саналы көзқарасымен байланысты.

Цифрландыру процесі тойтарылмайтын күшке айналғаны баршамызға белгілі болды. Аталған мән-жайлар осы бағытта жаңа шешімдер қабылдау мен жаңа қадамдар жасауды талап етті. Нәтижесінде 2023 жылы 28 гаурызда 2023-2029 жылдарға арналған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар мен киберқауіпсіздік саласын дамыту тұжырымдамасы (бұдан әрі – Тұжырымдама) қабылданды [2]. Тұжырымдаманың негізгі ұстанымдарының бірі цифрлық технологиялар саласындағы киберқауіпсіздікті қамтамасыз ету бойынша міндеттер кешенін шешу болып табылады.

Қаржылық операциялады жүзеге асырудың жаңа шарттарына сай және киберқауіпсіздікті қамтамасыз ету бойынша мәліметтер базасына заңсыз кіру фактілері өзектеле бастады. Болып жатқан құбылыстарды талдаудың жәй ғана негізі болып, ол киберқауіпсіздікті ескертудегі болжам жасау бағдарламаларын құру табылады. Дегенмен, өзін-өзі білдіріп жатқан киберқауіпсіздік қылмыстық ниетті анықтау және дәлелдеу әдістері мен тәсілдерін сондай-ақ, оларды жасыру жолдарын әзірлеуді талап етті. Тергеу және сот тәжірибесі ең тиімді және сенімді дәлелдемелерді табу үшін, қылмыстық істер бойынша жүргізілген сот сараптамалары бола алатынын көрсетті.

### *Кіріспе*

2023-2029 жылдарға арналған цифрлық түрлендіру, ақпараттық-коммуникациялық технологиялар саласын және киберқауіпсіздікті дамыту тұжырымдамасы Қазақстан Республикасы Мемлекет басшысының 2018 жылғы 15 ақпандағы Жарлығымен бекітілген 2025 жылға дейінгі ұлттық даму жоспарында көзделген құжат болды [3]. Осы Ұлт жоспарын іске асыру объективті түрде 2024 жылғы 30 шілдеде Қазақстан Республикасының 2029 жылға дейінгі жаңа Ұлттық даму жоспарын қабылдауға әкелді [4]. Жоғарыда аталған құжатқа сәйкес технологиялық үрдістер деп танылады:

- бизнестің бәсекеге қабілеттілігінің негізгі факторлары ретінде оларды пайдалануды қамтамасыз ететіндей дамыған цифрлық технологиялар;

- электрондық коммерцияға және қаржылық технологияларға сұраныстың өсуі, сондай-ақ, цифрландыру салдарында тиісті функцияларды жүзеге асырудың баламасыз тәсілі ретінде орын алатындығы мәлім. Осы зерттеу контексінде ең алдымен өзіне назар аударалығы, ол 3.3. бөлімі, яғни цифрлық технологияларды дамытуға орай жасалған Ұлттық жоспары табылады. Осыған орай, қарастырылып отырған цифрландыру деңгейінің жоспарлы түрде жүзеге асырылуына кедергі келтіретін мән-жайлар ретінде ұсынылады: 1) ақпараттық – технологиялар саласында білікті мамандардың жеткіліксіздігі; 2) цифрлық технологияларды әзірлеу және қолдану процесінде жаңа тәуекелдердің қалыптасуы және сол арқылы киберқауіпсіздікті қамтамасыз етумен байланысты келеңсіз мәселелердің шиеленісуі.

Жоғарыда аталған және өзге де мән-жайлар қылмыстық істер бойынша сапалы сот сараптамаларын дәлелдеу мақсатында қолдануды ұсына отырып, ақпараттық – коммуникациялық технологиялар саласындағы заңсыз бұрмалаудың алдын алу және жолын

кесумен байланысты зерттелетін мәселелер деңгейлерінің өте жоғары екендіктерін куәландырады.

АКТ саласында мамандардың тапшылығына орай хаккерлік әрекеттер де қатар өсуде. Бұл кемшілік киберқауіпсіздік саласындағы сарапшылардың жұмыс күштеріне де кері әсерін тигізуде.

#### *Материалдар мен әдістер*

Қарастаралып отырған мәселелеге орай авторлар тікелей қатысы бар ресми статистикалық мәліметтерді, нормативтік – құқықтық актілердің мәтіндерін, үкіметтік құжаттарды пайдаланған. Негізгі зерттеу әдісі ретінде динамика мен дамудағы ғылыми және қолданбалы мәселені қарастыруға мүмкіндік беретін диалектикалық тәсіл таңдалды. Аталған әдістеме шегінде құқықтық зерттеу саласындағы дәстүрлі әдістер қолданылады: логикалық-құқықтық талдау, салыстырмалы құқықтық тәсіл, қайнар көздерді сыни талдау.

#### *Нәтижелер мен талқылау*

Қазақстан көлемді қоғамдық қатынастар аясын компьютеризациялау мен цифрлық технологияны ендіру ісінде өте жоғары нәтижелерге қол жеткізді. Бұл жөнінде осы бағыттағы еліміздің жеткен жетістіктерін сипаттайтын ресми құжаттарда айтылған. Яғни 2022 жыл аясында Қазақстанда АКТ саласында 10 989 IT-компаниясының жұмыс жасағаны көрсетілген [2]. Фактордың өзі көп мәнді болып табылады және рұқсат етілмеген айла-шарғы жасау объектілерінің ауқымы да 10 989 IT- компанияға тең болғандықтан ғана оң және теріс аспектіде түсіндірілуі мүмкін. Мәселен, 2023 жылдың басында Қазақстан киберқауіпсіздік индексі бойынша елдер рейтингінде осы рейтингке қатысқан 195 мемлекеттің арасында 31-ші орынға ие болды. Тұжырымдамада қоғам өмірі мен қызметінің әлеуметтік маңызды салаларын, оның ішінде мемлекеттік басқару саласын ақпараттық-коммуникациялық технологиялармен қамту ауқымының кеңдігін көрсететін деректер келтірілген. Мысалы, «Электронды үкімет» бағдарламасы тәжірибелік тұрғыдан қызығушылық тудырады [2].

Дегенмен цифрлық технологияларды қолданумен байланысты жағымды күмәнсыз нәтижелердің болуымен қатар, құқыққорғау органдары киберқауіпсіздіктің өсіп кеткендігін атап өтеді. Жалпы 2023-2024 жылдар аралығында қылмыстық әлем киберқылмыстарды жасау мақсатында объектілерді заңсыз манипуляциялау үшін неғұрлым қолжетімді деп мынадай бағыттарды таңдады: БАҚ – 19%; мемлекеттік органдар – 12%; қаржы органдары – 12%; телекоммуникация – 7% [5]. Бұқаралық ақпарат құралдарына жасалған шабуылдардың артуы DDOS (denial-of-service attack: бұл хакерлік шабуыл негізінде 2023 жылы жасалған кибершабуыл толқынымен түсіндіріледі. Аталған шабуыл нысаны болып: веб-ресурсқа заңсыз кіруден қорғау бағдарламаларын бір уақытта өшіріп, осы ресурс жұмысын тоқтату үшін сұраулардың көп санын жіберу түріндегі хакерлік шабуыл табылады). Статистикаға сүйенсек, ҚР Қылмыстық кодексінің 190 бабымен (алаяқтық) сараланып әрбір екінші қылмыс, цифрлық технологияларды қолданумен байланысты, яғни, әңгіме кибералаяқтық туралы болып отыр. Басқаша айтқанда, кибералаяқтықтың үлесі жалпы алаяқтық сомасының 48,6 пайызын құрайды. 2023 жылы кибералаяқтықтан келтірілген материалдық шығын 17,5 млрд теңгені құрады. Жалпы, соңғы бес жылда киберқылмыстардың саны 2,8 есеге өскені атап өтіледі [6].

Жоғарыда келтірілген мәліметтерге жүгінсек, түрлі құқықтық қатынастар саласында АКТ-ні қолдану қажеттіліктерін кеңейтуде цифрлық технологияларды қылмыстық жолмен қолданумен байланысты тәуекелдердің болуымен куәландырады. Бұл дегеніміз өз кезегінде қылмыстық істерді тергеу барысында кәсіби сапалы сот сараптамаларын жүргізуге сұраныстардың өсетінін білдіреді. Аталған мәндеттерді шешу келесідей факторлармен күрделенеді: бірінішіден, АКТ саласындағы білікті мамандардың жетіспеушілігі; екіншіден, сараптамалық зерттеулерді жүргізу әдістерін әзірлеудің постфактуалды сипаты, ол сараптамалық зерттеудің жаңа әдістерін әзірлеу қажеттілігі қылмыскерлердің ақпаратқа заңсыз қол жеткізудің жаңа әдісін пайдаланған кезде ғана пайда болуымен байланысты объективті жағдай екенін көруге болады. Киберқылмыстардың жасалу әдістерін танып білуде

сот сарапшысынан жоғары кәсіби біліктілікті талап етеді; үшіншіден, Мемлекеттік техникалық қызмет жүйесінде 2018 жылдан [7] бері жұмыс істеп келе жатқан Ақпараттық қауіпсіздік жөніндегі ұлттық үйлестіру орталығы (бұдан әрі – ҰҚҚҮО) ақпараттық жүйелерге заңсыз кіруден қорғауды қамтамасыз ету үшін жеткіліксіз. ҰҚҚҮО міндеттеріне жатады: «Электронды Үкімет» ақпараттары объектілерінің қорғалу деңгейін зерттеу; ақпараттық қауіпсіздікті мониторингілеу (АҚ); мемлекеттік ақпараттық жүйе қауіпсіздігін мониторингілеу. Осы зерттеу контекстінде киберқауіпсіздікті жүзеге асыруға кедергі келтіретін немесе ҰҚҚҮО қызметін қиындататын факторларды анықтау маңызды болып көрінеді:

- ақпараттық-коммуникациялық технологияларға қызмет көрсететін қызметкерлерді қоса алғанда, Қазақстан халқы ұсынатын АКТ тұтынушының цифрлық және құқықтық сауаттылығының жеткіліксіздігі;

- жеке мәліметтердің қорғалу кепілдіктерінің тиімсіздігі;
- тұрақты жасалып жатқан кибер шабуыл санының өсу тенденциялары;
- бірыңғай ұлттық қосалқы (резервтік) платформасы бар ақпараттық қауіпсіздік жөніндегі қосымша ұлттық үйлестіру орталығының болмауы.

Ақпараттық - коммуникациялар технологиясы саласында тікелей жасалып жүрген, және өзге де цифрлық технологиялармен байланысты орын алып жүрген қылмыстық құқықбұзушылық түрлері тұрақты өсу тенденциясына ие болып отыр. Ондай құқықбұзушылықтардың ең кең тараған түрлері мен жаслау әдістеріне жатады:

- зиянды бағдарламаларын жасау және пайдалану (ЗБ);
- электрондық құралдарды пайдалана отырып жасалған алаяқтық (кибералаяқтық);
- интернет арқылы есірткі заттарын сату;
- халық арасында дүрбелең тудыру мақсатында террористік шабуылдар туралы жалған хабарларды қашықтықтан тарату;

- ойын бизнесін заңсыз ұйымдастыру және өткізу;
- хакерлер арқылы жасалған қылмыстар (мысалы, Ресей Федерациясында 2021 жылы хакерлердің әрекеттерінен келтірілген залал 150 миллиард рубльге жетті);

- қызмет көрсету саласы (көбінесе білім беру, медициналық, жыныстық);
- жеке тұлғаның ар-намысы мен қадір-қасиетін қорлау;
- басқа түрлері.

ҚР ПМ-нің мәліметтері бойынша, 2023 жылы киберқылмыстарды ашу олардың жалпы санынан 22 %-ын құрады: тіркелген 9 мың қылмыс ішінен тек қана 2 мыңы ашылған [8]. Қазақстан Республикасы Ішкі істер министрінің орынбасары А.Рысбаевтың мәліметінше, соңғы жеті жылда Қазақстанда киберқылмыс 10 есеге өскен [9]. Жасалған қылмыстардың жалпы көлеміндегі киберқылмыстардың үлесі қауіпті динамикаға ие: егер 2016 жылы ол 2%-дан аз болса, 2020 жылы ол өсіп, 25%-дан астам құра бастады. Қазақстанда 2024 жылы киберқылмыстан келген шығын 21 млрд теңгені құрады. Киберқылмыстық істердің тек 5%-ы ғана сотта қаралуға дейін барады. Қылмыстық істердің басым көпшілігі ҚР Қылмыстық кодексінің 205 бабы ақпаратқа, ақпараттық жүйеге немесе ақпараттық-коммуникациялық желіге заңсыз қол жеткізу бойынша сараланады. Қаралып отырған құқық бұзушылықтардың әлеуметтік қауіптілігі азаматтар мен ұйымдардың құқықтары мен заңды мүдделерін, қоғам мен мемлекеттің ақпарат саласындағы заңмен қорғалатын мүдделерін бұзуда, ақпараттық ресурстардың құпиялылығына, тұтастығына, қауіпсіздігіне және ақпараттық жүйелер мен коммуникациялық инфрақұрылым қолжетімділігіне зиян келтіруде болып табылады [10, б. 377-378].

Сот сараптамасына қатысты айта кететін жайт, сотқа дейінгі тергеп-тексерудің аяқталуы мен қылмыстық істі мәні бойынша сотта қарау үшін сотқа жіберудің аз пайызы көптеген түрлі себептерден сонымен қатар, тергеушілер қойған сұрақтарға сот-медициналық сарапшылардың жан-жақты жауап бере алмайтындығы фактілерімен түсіндіріледі. Бұдан басқа, кейінгі

сараптамалық зерттеулер үшін материалдарды қамтамасыз етуге байланысты жеке тергеу әрекеттерін жүргізудің тергеу әдістері мен тактикасы саласындағы криминалистикалық білімді оқшаулаудың аса қажеттілігі туындайды. Қазіргі таңда біздің ойымызша, компьютерлік криминалистиканы (шартты атауы) бөліп алу қажеттілігі туындады. 1990-2005 жылдардағы ақпаратты компьютерлік өңдеу және жинақтау объектілеріне қылмыстық ықпал етудің бастапқы көріністері кезеңінде қаралып жатқан қылмыстық істер бойынша сот сараптамаларының атауында қисынды түсіндірілетін біртұтастық іс жүзінде болған жоқ. Әртүрлі криминалистикалық қайнар көздерде сараптамалар әртүрлі аталды: кейде компьютерлік-техникалық, кейде ақпараттық-технологиялық, кейде ақпараттық-техникалық, кейде бағдарламалық-техникалық; әртүрлі сараптамалық және криминалистикалық топтарға жататын, мысалы, инженерлік-техникалық немесе тауартану-техникалық және т.б. топтарына жатады. Қазіргі жағдайда цифрлық технологиялардың өзі дамып, олардың әлеуметтік тәжірибеге кеңінен енгізілуімен, сондай-ақ қалыптасуымен сандық кеңістікке қылмыстық ықпал етудің әртүрлі әдістері мен тәсілдерін, заңсыз манипуляциялаумен (қол жеткізумен, пайдаланумен) цифрлық кеңістікке байланысты қылмыстарды жасаудың мән-жайларын анықтау үшін қолданылатын сараптамалық зерттеулердің санаттары және олардың түрлері анықталады және қалыптасады.

Терминологиялық аппаратты біріздендіру және ретке келтіру процестеріне 2017 жылғы 10 ақпандағы «Сот-сараптама қызметі туралы» Қазақстан Республикасының Заңының қабылдануы ықпал етті [11]. Аталған заңның 55-бабына сәйкес Қазақстанда Сот-сараптамалық зерттеулер әдістемесінің мемлекеттік тізілімі құрылды. Осы норманы әзірлеу кезінде Қазақстан Республикасы Әділет министрлігінің 2017 жылғы 27 наурыздағы № 306 бұйрығымен сот сараптамасы органдары жүргізетін сот сараптамаларының және Қазақстан Республикасының Әділет Министрлігінің беретін сарапшылық мамандықтардың тізбесін бекітті [12]. Аталған Тізбенің 12-тармағына сәйкес тиісті сот сараптамалары «Сот-технологиялық сараптама» түріне жатады.

Украиналық криминолог В.Ю. Балашов атап өткендей, киберкеңістік саласындағы қылмыстар өзінің терең ерекшелігіне байланысты 2007-2008 жылдардан бастап ресми түрде киберқылмыстар деп атала бастады [13]. Ю.В. Балашовтың айтуынша, ақпараттық-коммуникациялық криминалистика арқылы киберқылмыстарды тергеп-тексеру тергеуші мен жедел қызметкерден арнайы білімді, ал сарапшыдан «информатика, телекоммуникация, ақпараттық қауіпсіздік және компьютерлік техника» саласында арнайы ғылыми білімінің болуын талап етеді» деген болатын [13, б. 94].

Дербес зерттеу дәлелдемелерді жинауда ерекшеліктер мен қиындықтарды талап етеді. Олар келесі жағдайларға байланысты болады:

- сот сараптамасының объектісі сараптамалық зертханада орналаспаса. Зерттелетін объект пен сарапшы арасындағы цифрлық байланыс арнасында алынған ақпараттың сенімділігі бойынша тиісті сенімділік белгілері болмаса;

- қашықтықтан зерттеу қазіргі ақпараттық жүйелер мазмұнының жоғары динамикасымен күрделенеді, бұл талап етілетін ақпараттың әртүрлі мазмұнын көрсетумен қатар жүреді. Демек, талаптарға сай сараптамалық қорытынды беру ықтималдылығы салыстырмалы түрде болады.

Криминалистердің теория және практика салаларында ұсынып отырған «компьютерлік криминалистика» ұғымы – ол деген криминалистика тарихындағы замануы мәселелердің бірі. Аталған ұғымның мазмұны мен түсінігі цифрлық құралдардан табылған дәлелдемелерге жататын цифрлық криминалистиканың саласы болып табылады. Яғни, оның құрамына жатады:

- стационарлық комптерлер;
- ноутбуктер;
- смартфондар;

- планшеттер;
- камералар;
- әртүрлі гаджеттер мен деректерді сақтау құрылғылары.

Сарапшылардың пікірінше, компьютерлік криминалистика есептеу жүйелеріне қатысты кең ауқымды салаларда білім мен дағдыларды қажет етеді, мысалы: бірнеше операциялық жүйелерді білу, әртүрлі файлдық жүйелерді білу, желілерді түсіну, шабуылдар мен қауіптердің түрлерінің мағынасын түсіну [14] ].

Сот-сараптама қызметінің маңызды құрамдас бөлігі сотқа дейінгі тергеп-тексеруді жүзеге асыратын уәкілетті тұлға тұжырымдаған сұрақтар тізбесі болып табылады. Мұндай сұрақтардың нақтылығы мен дұрыстығы сарапшы үшін маңызды және сараптамалық зерттеудің мәніне әсер етеді. Осыны ескере отырып, бірқатар криминалистер бұл жағдай тергеушінің цифрлық технологиялар саласында айтарлықтай білімі мен біліктілігін қажет етеді деп есептейді. Керісінше, Қазақстан Республикасы Қылмыстық-процестік кодексінің 113-бабында (жол берілгендігі, қатыстылығы, дұрыстығы және жеткіліктілігі) көзделген дәлелдемелерді бағалау критерийлеріне сай болмаса заңды күші жоқ деп тану туралы мәселені шешу үшін негіз бола алады. Әрине, тергеушінің бұл салада белгілі бір білімі мен дағдысы болуы керек. Бірақ бұл мәселенің шегі болуы керек. Олай болмаса, бұл тәсіл арқылы тергеуші ғылым мен техниканың әртүрлі салаларында кең ауқымды білімі бар энциклопедист бейнесінде көріну қаупі бар. Бұл ретте функцияларды ауыстыруға заңмен тыйым салынады: тергеуші сарапшыға жүктелген міндеттерді өз мойнына ала алмайды. Сондықтан мұндай ұсыныстарды жүзеге асыру мүмкін емес. Бұл жағдайдан шығу үшін заңнамалық рұқсат бар: сараптамалық зерттеу объектілерін жинау және сараптамалық зерттеуге жататын сұрақтарды қою кезінде квазиконсультант рөлінде тиісті сарапшының қатысуына жол беріледі және оған осы сараптаманы жүргізу тапсырылады.

Киберқылмыстар бойынша сарапшылардың міндеттері мыналар:

- сараптамаға жататын ақпаратты ол цифрлық құрылғыларда қамтылған және құқық бұзушылық жасау үшін пайдаланылған сақталған нысанда алу;
- сараптама тағайындау кезінде тергеуге белгілі мән-жайларды ескере отырып, сараптамаға ұсынылған ақпаратты зерделеу, оны талдау және түсіндіру.

Сараптамалық зерттеулер үшін цифрлық ақпаратты жинау қажетті дәлелдемелердің өзгеріссіз барынша мүмкін сақталуын қамтамасыз ете алатын тәсілдер мен әдістер негізінде жүзеге асырылуы тиіс. Цифрлық технологияларды қылмыстық манипуляциялау, цифрлық іздер жойылса да, цифрлық кеңістікте қалады. Мәселе оларды анықтаудың тиімді құралдары мен әдістерін әзірлеу және қолдану болып табылады [15].

#### *Қорытынды*

1. Әлеуметтік тәжірибеге жағдайында цифрлық технологияларды кеңінен енгізу, ақпараттық-коммуникациялық технологияларға рұқсатсыз қол жеткізу қаупінің дәрежесі, киберқылмыстар санының тұрақты өсу тенденциясы байқалады, сонымен қатар, киберқылмыспен келтірілген залал көлемі өсуде. Заманауи жағдайларда киберкеңістіктің қауіпсіздігін қамтамасыз ету мәселелері өте өзекті болуда. Сонымен қатар, цифрлық сақтау құралдарына, деректер қорларына қылмыстық қол сұғушылық және заңсыз манипуляциялау объектілеріне қатысты сот сараптамадан өткізуге сұраныстар артып отыр.

2. Киберқылмыстарды тергеу дәлелдемелерді жинауды қамтиды және сараптамалық тұрғыдан бағалауды қамтиды. Тергеу тәжірибесі сандық технологиялармен ауыртпалықпен дәлелдейтін ақпаратты жинау мен сақтаудың жаңа криминалистикалық-тактикалық әдістері мен тәсілдерін әзірлеуді талап етеді. Сараптамалық тәжірибе цифрлық технологияларды қылмыстық манипуляциялаумен байланысты сараптамалық зерттеулерді өндірудің жаңа әдістерін әзірлеуді қажет етеді.

3. Қылмыстық істер бойынша тергеу мен дәлелдеудің ерекшеліктері, цифрлық технологиялармен байланысты, жаңалықты – компьютерлік криминалистиканы –

криминалистиканың тәуелсіз бөліміне бөлуді көздейді, оның шеңберінде киберқылмыстарды тергеу әдістерін әзірлеу кезінде қолданылатын криминалистикалық маңызды білімдер шоғырланатын болады.

*Пайдаланылған әдебиеттер тізімі*

1 «Цифрлық Қазақстан» мемлекеттік бағдарламасы. – Қазақстан Республикасы Үкіметінің 2017 жылғы 12 желтоқсандағы № 827 қаулысымен бекітілген. Күші жойылды - ҚР Үкіметінің 2022 жылғы 17 мамырдағы № 311 қаулысымен. [Электрон. ресурс]. – 2017. – URL: <https://www.gov.kz/memleket/entities/mdai/activities/14764?lang=kk> (өтініш берілген күн: 16.10.2024.).

2 2023-2029 жылдарға арналған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар мен киберқауіпсіздік саласын дамыту тұжырымдамасы. – Қазақстан Республикасы Үкіметінің 2023 жылғы 28 наурыздағы № 269 қаулысымен бекітілген. [Электрон. ресурс]. – 2023. – URL: [https://online.zakon.kz/Document/?doc\\_id=32540304](https://online.zakon.kz/Document/?doc_id=32540304) (өтініш берілген күн: 16.10.2024.).

3 Қазақстан Республикасының 2025 жылға дейінгі ұлттық даму жоспары. – ҚР Президентінің 15.02.2018 № 636 Жарлығымен бекітілді. Күші жойылды - ҚР Президентінің 30.07.2024 № 611 Жарлығымен. Электрон. ресурс]. – 2017. – URL: <https://adilet.zan.kz/kaz/docs/U1800000636> (өтініш берілген күн: 16.11.2024.).

4 Қазақстан Республикасының 2029 жылға дейінгі ұлттық даму жоспары. – Қазақстан Республикасы Президентінің 2024 жылғы 30 шілдедегі № 611 Жарлығымен бекітілген Электрон. ресурс]. – 2024. – URL: <https://www.gov.kz/memleket/entities/ecogeo/press/news/details/836261?lang=kk> (өтініш берілген күн: 16.10.2024.).

5 Қазақстанның орнықты дамуы үшін киберқауіпсіздіктің маңызы [Электрон. ресурс]. – 2024. – URL: <https://dalanews.kz/kz/article/qazaqstannin-orniqti-damui-ushin-kyberqauipsizdiktin-manizi.html> (өтініш берілген күн: 16.10.2024.).

6 Қазақстан кибершабуылдар бойынша Әлемде 7-ші орында. [Электрон. ресурс]. – 2024. – URL: [https://forbes.kz/articles/kolichestvo\\_kiberatak\\_v\\_rk\\_vyiroslo\\_vdvoe](https://forbes.kz/articles/kolichestvo_kiberatak_v_rk_vyiroslo_vdvoe) (өтініш берілген күн: 16.10.2024.).

7 Мемлекеттік техникалық қызметтің кейбір мәселелері туралы. Қазақстан Республикасы Үкіметінің 2013 жылғы 28 қаңтардағы № 49 қаулысы. Электрон. ресурс]. – 2013. – URL: <https://adilet.zan.kz/kaz/docs/P1300000049> (өтініш берілген күн: 16.10.2024.).

8 В Казахстане раскрыли только 22 % киберпреступлений в этом году. В МВД рассказали о сложностях в расследований [Электрон. ресурс]. – 2024. – URL: <https://kz.kursiv.media/2023-07-17/Insh-raskryvaemost/> (өтініш берілген күн: 16.10.2024.).

9 В МВД Казахстана создали структуру по борьбе с киберпреступностью [Электрон. ресурс]. – 2024. – URL Режим: <https://polisia.kz/ru/v-mvd-sozdan-departament-protivodejstviyu-kiberprestupnosti/> (өтініш берілген күн: 16.10.2024.).

10 Борчашвили И. Ш. Комментарий к Уголовному кодексу Республики Казахстан / Под общей редакцией А. К. Даулбаева. В двух томах. Особенная часть (том 2). – Алматы: Жети Жарғы, 2015. – 1120 с.

11 Сот-сараптама қызметі туралы. – 2017 жылғы 10 ақпандағы Қазақстан Республикасының Заңы. № 44-V [Электрон. ресурс]. – 2017. – URL: [https://online.zakon.kz/Document/?doc\\_id=36434384](https://online.zakon.kz/Document/?doc_id=36434384) (өтініш берілген күн: 16.10.2024.).

12 Сот сараптамасы органдары жүргізетін сот сараптамаларының түрлерінің және Қазақстан Республикасының Әділет министрлігі біліктілік беретін сарапшылық мамандықтардың тізбесі. – Қазақстан Республикасы Әділет министрлігінің 2017 жылғы 27 наурыздағы бұйрығымен бекітілген. № 306 [Электрон. ресурс]. – 2017. – URL <https://law.gov.kz/client/#/doc/74171/rus/26.01.2015> (өтініш берілген күн: 16.10.2024.).



13 Балашов В. Ю. Проблемы судебной экспертизы при расследовании киберпреступлений// *Материалы Международной научно-практической конференции «Восток-Запад: партнерство в судебной экспертизе. Актуальные вопросы теории и практики судебной экспертизы»*. – г. Алматы, 27 октября 2016 года. – Алматы, 2016. – С. 93-95.

14 Компьютерная криминалистика [Электрон. ресурс]. – 2024. – URL: <https://forensic.gov.kz/ru/news/kompyuternaia-kriminalistika/> (өтініш берілген күн: 16.10.2024).

15 Toleubekova B., Khvedelidze T. Signs of Emergens of new Corruption Zones Risks Associated with Manipulation of Digital Technologies in Higher Education Institutions// *Znanstvena Misel, Slovenia, Ljubljana, Vol. 2, N 63, 2022. Pp. 37-40.*

#### References

1 «Cifrlyқ Қазақстан» мемлекеттік бағдарламасы. – Қазақстан Республикасы Үкіметінің 2017 жылғы 12 желтоқсандағы № 827 қаулысымен бекітілген. Қысқашы жойылды - ҚР Үкіметінің 2022 жылғы 17 мамырдағы № 311 қаулысымен. [Электрон. ресурс]. – 2017. – URL: <https://www.gov.kz/memleket/entities/mdai/activities/14764?lang=kk> (қаралым мерзімі: 16.10.2024.).

2 2023-2029 жылдарға арналған цифрлық трансформация, ақпараттық-коммуникациялық технологиялар мен киберқауіпсіздік саласын дамыту тұжырымдамасы. – Қазақстан Республикасы Үкіметінің 2023 жылғы 28 наурыздағы № 269 қаулысымен бекітілген. [Электрон. ресурс]. – 2023. – URL: [https://online.zakon.kz/Document/?doc\\_id=32540304](https://online.zakon.kz/Document/?doc_id=32540304) (қаралым мерзімі: 16.10.2024.).

3 Қазақстан Республикасының 2025 жылға дейінгі ұлттық даму жоспары. – ҚР Президентінің 15.02.2018 № 636 Жарлығымен бекітілді. Қысқашы жойылды - ҚР Президентінің 30.07.2024 № 611 Жарлығымен. [Электрон. ресурс]. – 2017. – URL: <https://adilet.zan.kz/kaz/docs/UI1800000636> (өтініш берілген күн: 16.11.2024.).

4 Қазақстан Республикасының 2029 жылға дейінгі ұлттық даму жоспары. – Қазақстан Республикасы Президентінің 2024 жылғы 30 шілдесіндегі № 611 Жарлығымен бекітілген [Электрон. ресурс]. – 2017. – URL: <https://www.gov.kz/memleket/entities/ecogeo/press/news/details/836261?lang=kk> (қаралым мерзімі: 16.10.2024).

5 Қазақстанның орнықты дамуы үшін киберқауіпсіздіктің маңызы [Электрон. ресурс]. – 2024. – URL: <https://dalanews.kz/kz/article/qazaqstannin-orniqti-damui-ushin-kyberqauipsizdiktin-manizi.html> (қаралым мерзімі: 16.10.2024).

6 Қазақстан кибешабуылдар бойынша Әлемде 7-ші орында. [Электрон. ресурс]. – 2024. – URL: [https://forbes.kz/articles/kolichestvo\\_kiberatak\\_v\\_rk\\_vyiroslo\\_vdvoe](https://forbes.kz/articles/kolichestvo_kiberatak_v_rk_vyiroslo_vdvoe) (қаралым мерзімі: 16.10.2024).

7 Мемлекеттік техникалық қызметтің кейбір мәселелері туралы. Қазақстан Республикасы Үкіметінің 2013 жылғы 28 қаңтардағы № 49 қаулысы. [Электрон. ресурс]. – 2013. – URL: <https://adilet.zan.kz/kaz/docs/P1300000049> (қаралым мерзімі: 16.10.2024).

8 V Kazahstane raskryli tol'ko 22 % kiberprestuplenij v jetom godu. V MVD rasskazali o slozhnostjah v rassledovanij [Электрон. ресурс]. – 2024. – URL: <https://kz.kursiv.media/2023-07-17/lnsh-raskryvaemost/> (қаралым мерзімі: 16.10.2024).

9 V MVD Kazahstana sozdali strukturu po bor'be s kiberpestupnost'ju [Электрон. ресурс]. – 2024. – URL: <https://polisia.kz/ru/v-mvd-sozdan-departament-po-protivodejstviyu-kiberprestupnosti/> (қаралым мерзімі: 16.10.2024).

10 Borchashvili I. Sh. Kommentarij k Ugolovnomu kodeksu Respubliki Kazahstan / Pod obshhej redakciej A. K. Daulbaeva. V dvuh tomah. Osobennaja chast' (tom 2). – Almaty: Zheti Zhargy, 2015. – 1120 s.

11 Sot-saraptama қызметі туралы. – 2017 жылғы 10 ақпандағы Қазақстан Республикасының Заңы. № 44-V [Электрон. ресурс]. – 2017. – URL: [https://online.zakon.kz/Document/?doc\\_id=36434384](https://online.zakon.kz/Document/?doc_id=36434384) (қаралым мерзімі: 16.10.2024).

12 Sot saraptamasy organdary zhyrgizetin sot saraptamalarynyñ tyrleriniñ zhәne Қазақстан Республикасының Әділет министрлігі биліктілік беретін сарапшылық мамандықтардың тізбесі. – Қазақстан Республикасы Әділет министрлігінің 2017 жылғы 27 наурыздағы бұйрығымен бекітілген. №

306 [Jelektron. resurs]. – 2017. – URL <https://law.gov.kz/client/#!/doc/74171/rus/26.01.2015> (қаралым мерзімі: 16.10.2024).

13 Balashov V. Ju. Problemy sudebnoj jekspertizy pri rassledovanii kiberprestuplenij//Materialy Mezhdunarodnoj nauchno-prakticheskoy konferencii «Vostok-Zapad: partnerstvo v sudebnoj jekspertize. Aktual'nye voprosy teorii i praktiki sudebnoj jekspertizy». – g. Almaty, 27 oktjabrja 2016 goda. – Almaty, 2016. – S. 93-95.

14 Kompjuternaja kriminalistika [Jelektron. resurs]. – 2024. – URL: <https://forensic.gov.kz/ru/news/kompyuternaia-kriminalistika/> (қаралым мерзімі: 16.10.2024).

15 Toleubekova B., Khvedelidze T. Signs of Emergens of new Corruption Zones Risks Associated with Manipulation of Digital Technologies in Higher Education Institutions//Znanstvena Misel, Slovenia, Ljubljana, Vol. 2, N 63, 2022. Pp. 37-40.

МРНТИ: 10.81.35  
УДК 343.98

10.51889/2959-6181.2024.78.4.010

А. М. Хлус<sup>1\*</sup>

<sup>1</sup> Белорусский государственный университет  
(e-mail: \* [hlus.home@mail.ru](mailto:hlus.home@mail.ru))

## КРИМИНАЛИСТИЧЕСКИЙ АСПЕКТ В УСТАНОВЛЕНИИ ОБСТОЯТЕЛЬСТВ СОВЕРШЕНИЯ ВЗЯТОЧНИЧЕСТВА (на основе анализа законодательства Беларуси и Казахстана)

### Аннотация

На основе анализа законодательства Беларуси и Казахстана рассмотрены обстоятельства, подлежащие выявлению и доказыванию в процессе расследования взяточничества. Установление обстоятельств, предусмотренных нормами уголовно-процессуальных кодексов Беларуси и Казахстана, не обеспечивает полноты раскрытия рассматриваемых преступлений. Наряду с этим соответствующие нормы уголовно-процессуального права составляют основу процесса их предварительного расследования. Проведенное исследование позволяет представить обстоятельства, подлежащие установлению, в качестве системы взаимосвязанных элементов, обеспечивающих объективное раскрытие взяточничества. Познание обстоятельств совершения взяточничества основывается на криминалистических знаниях, способствующих их конкретизации в каждом конкретном случае расследования. Сделан вывод, что в процессе раскрытия и расследования взяточничества наиболее эффективным является метод криминалистического анализа деятельности должностного лица и организации, в которой проходит его служба.

**Ключевые слова:** расследование, взяточничество, криминалистика, обстоятельства, предмет доказывания.

А.М.Хлус<sup>1</sup>

<sup>1</sup> Беларусь мемлекеттік университеті

## ПАРА АЛУ ЖАҒДАЙЛАРЫН АНЫҚТАУДАҒЫ КРИМИНАЛИСТИКАЛЫҚ АСПЕКТ (Беларусь пен Қазақстан заңнамасын талдау негізінде)

### Аннотация

Беларусь пен Қазақстан заңнамасын талдау негізінде парақорлықты тергеу процесінде анықтауға және дәлелдеуге жататын мән-жайлар қаралды. Беларусь пен Қазақстанның