***Ашимбаев Д.А.***

**Докторант, заң ғылымдарының магистрі,**

**Қонаев Университетінің аға оқытушысы**

**Киберқылмыстық құқық бұзушылықтарды алдын алу мәселелері**

**\***

**Problems of prevention of cybercrime offenses**

**Аңдатпа**

*Қазіргі уақытта жасанды интеллект жүйелері, нейросеть және де басқа да ақпараттық қауіпсіздік көздері арқылы соның ішінде дипфейк «Deepfake» (дауыс пен бейнені салу) техникалық жетістіктерін қолдану арқылы биометриялық ақпараттарға қол жеткізіп, солар арқылы интеграцияланған мемлекеттік ақпараттық базаларға ену арқылы дербес деректерге қол жеткізіп киберкеңістік шеңберінде қылмыстық ойын жүзеге асырады. Көп жағдайда аталған қылмыстық құқық бұзушылықтар виртуалды кеңістікте жасалғандықтан, қылмыстық қауіптің шығу қайнар көзін анықтау қиындықтар туығызады.*

*Киберкеңістікте жасалатын қылмыстар бір-түрден екінші түрге айналып, оларды құрықтау құқық қорғау органдары үшін үлкен мәселе болып тұр. Сол себепті заңнамалық тұрғыда аталған жаңа түсініктерге құқықтық баға беріліп, криминологияның қылмыстылықпен күрсе тәсілдерін тиімді пайдалану шарт. Одан бөлек, мұндай қылмыстар алыс-жақын орналасқан шетелдер арқылы жасалатын болғандықтан, бұндай қылмыстармен күрес құқықтық көмек беру шарты арқылы халықаралық ынтымақтастықты нығайтуды қажет етеді.*

**Кілтті сөздер:***киберқылмыстар, киберкеңістік, ұйымдасқан топ, қылмыстық топ, трансұлттық қылмыстық қоғамдастық, қылмыс, ақпарат, технология, интернет, дербес деректер.*

**Annotation**

*Currently, through artificial intelligence systems, neurosets and other sources of information security, including deepfake, access to biometric information using the technical achievements of Deepfake (voice and video construction), and through them access to personal data through integrated state information bases, the Criminal game is carried out within cyberspace. Since in most cases these criminal offenses are committed in the virtual space, it becomes difficult to determine the source of the criminal threat.*

*Crimes committed in cyberspace are turning from one type to another, and arresting them is a big problem for law enforcement agencies. It is therefore necessary to make a legal assessment of these new concepts in the legislative context and to effectively use the methods of Criminology to combat criminality. In addition, since such crimes are committed through far and near abroad, the fight against such crimes requires strengthening international cooperation through the conditions of legal assistance.*

**Key words:** *cybercrime, cyberspace, organized group, criminal group, transnational criminal Community, Crime, Information, Technology, Internet, personal data.*

Киберқылмыс — бұл ақпараттық технологиялар мен интернетті пайдалана отырып жасалатын қылмыс түрі. Киберқылмыстарда қылмыскерлер компьютерлер, желілер, деректер базалары, бағдарламалық қамтамасыз ету және басқа да цифрлық құралдарды пайдаланып, заңға қайшы әрекеттер жасайды. Бұл қылмыстардың ауқымы өте кең, және олар әртүрлі тәсілдермен жүзеге асуы мүмкін.

Киберқылмыстың кейбір түрлеріне мыналар жатады:

1. **Алаяқтық** (фишинг, онлайн алаяқтық) – пайдаланушылардың жеке ақпараттарын (мысалы, банк картасының деректері) ұрлап алу мақсатында алаяқтық сайттар немесе хаттар жіберу.
2. **Деректерді ұрлау** – жеке немесе коммерциялық ақпараттарды заңсыз түрде алу, мысалы, компаниялардың клиенттерінің деректерін ұрлау.
3. **Кибершабуылдар** (DDoS, вирус тарату) – жүйелерді немесе серверлерді жүктеп, жұмыс істеу қабілетін бұзу үшін жасалатын шабуылдар. Вирустар, трояндар және басқа да зиянды бағдарламалар қолданылуы мүмкін.
4. **Ақпараттық қауіпсіздікті бұзу** – жеке немесе мемлекеттік ақпараттық жүйелердің қауіпсіздігін бұзу арқылы құпия ақпараттарды ұрлау.
5. **Рансомware (құрылғыны құлға айналдыру)** – қылмыскерлер қолданушының немесе ұйымның деректерін шифрлап, оны қайта ашу үшін ақша талап етеді.
6. **Интернет-терроризм** – белгілі бір саяси немесе идеологиялық мақсатты жүзеге асыру үшін киберқұралдарды қолдану.

Киберқылмыстардың алдын алу үшін ақпараттық қауіпсіздікті нығайту, құқық қорғау органдары мен ұйымдардың бірлескен жұмысы және жалпы қоғамның саналы ақпараттық мінез-құлықты қалыптастыруы маңызды.

 Киберқылмыстардың алдын алу мәселесі бүгінгі күннің ең өзекті тақырыптарының бірі болып отыр. Бұл проблеманың кеңеюі мен күрделенуі ақпараттық технологиялардың дамуымен тікелей байланысты. Киберқылмыстардың алдын алу үшін бірнеше маңызды шараларды қарастыру қажет:

1. **Ақпараттық қауіпсіздікті қамтамасыз ету**: Әрбір пайдаланушы мен ұйымның деректерін қорғау үшін, күрделі парольдер мен екі факторлы аутентификация сияқты қауіпсіздік шаралары қажет. Сонымен қатар, жүйелерді үнемі жаңартып, жаңа қауіптерге қарсы қорғау бағдарламаларын қолдану маңызды.
2. **Киберқылмысқа қарсы заңнаманы жетілдіру**: Мемлекеттер киберқылмыстарға қарсы арнайы заңдар мен ережелер қабылдауы тиіс. Бұл заңдар киберқылмыстарды анықтау, тергеу және жазалау процестерін тиімдірек етеді.
3. **Халықты ақпараттандыру**: Пайдаланушыларды киберқауіптер мен фишинг сияқты алаяқтық әдістер туралы хабардар ету маңызды. Әсіресе, жастар мен тәжірибесіз пайдаланушыларға қауіпсіздік шараларын түсіндіру қажет.
4. **Киберқылмыскерлермен күресу**: Ұлттық және халықаралық деңгейде киберқылмыскерлермен күресетін арнайы ұйымдар мен топтар құрылуы тиіс. Бұл ұйымдар өзара байланысып, халықаралық деңгейде қылмыскерлердің әрекеттерін бақылауға алады.
5. **Құқық қорғау органдарының дайындығы**: Киберқылмыстарды тергеу мен тоқтату үшін құқық қорғау органдарының мамандары заманауи құрал-жабдықтармен жабдықталуы және арнайы тренингтерден өтуі керек.

Киберқылмыстардың алдын алу тек мемлекеттік немесе жеке сектор деңгейінде емес, сонымен қатар қоғамның әрбір мүшесінің жауапкершілігінде болуы керек.

 Соңғы уақытта жасанды интеллект жүйелері, нейросеть және де басқа да ақпараттық қауіпсіздік көздері арқылы соның ішінде дипфейк «Deepfake» (дауыс пен бейнені салу) техникалық жетістіктерін қолдану арқылы биометриялық ақпараттарға қол жеткізіп, солар арқылы интеграцияланған мемлекеттік ақпараттық базаларға ену арқылы дербес деректерге қол жеткізіп киберкеңістік шеңберінде қылмыстық ойын жүзеге асырады. Көп жағдайда аталған қылмыстық құқық бұзушылықтар виртуалды кеңістікте жасалғандықтан, қылмыстық қауіптің шығу қайнар көзін анықтау қиындықтар туығызады. Мысалға, жасөспірімдердің психикасы мен жалпы дамуына қауіпті әсер ететін интернет ойындары бар, соның ішінде балардың өмірімен қоштасуына алып келетін «Синий кид» және де Schoolboy Runaway ойындарын айтсақ болады. Мұндай қылмыстар Қазақстан Республикасының Қылмыстық кодексінің 105 бабымен өзін-өзі өлтіруге дейін жеткізу бабымен сараланады. Бұндай қылмыстар бойынша негізгі мәселе, осы ойындарды құрастырушы, яғни күдіктілерді анықтау сатысында туындайды. Басым көп жағдайда аталған қылмыстар алдын ала сөз байласқан топтар мен немесе ұйымдасқан қылмыстық топтармен жасалады және де олардың қылмыс жасау кеңістігі бүкіл әлемнің кезкелген нүктесі болуы мүмкін. Мұндай да не істемек керек және қандай алдын алу немесе ескерту шаралары аталған қылмыстарға тосқауыл немесе жасалуына ықтимал мүмкіндік бермейтін іс-әрекеттер болып табылады. Осы мәселені қарау барысында аталған қылмыстың алдын алу үшін келесідей мән-жәйға мән беру керек деп ойлаймын. Біріншіден, азаматтардың құқықтық сана-сезімі мен құқықтық мәдениетін құқық қолдану деңгейінде жетілдіру; Екіншіден, осы қылмыстылықтың алдын алумен айналысатын құзыретті органдарды заманауи техникалық құрал-жабдықтармен қамтамасыз ету; Үшіншіден, азаматтардың заңмен қорғалатын дербес деректерімен жұмыстарын байланыстыратын заңды тұлғалар мен квазимемлекеттік сектор саласы қызметіне заңмен айқындалатын қатаң талаптар қою; - деп түсінеміз.

 Жасанды интеллект жүйесінің дамуы IT-мамандарының өз білімдері мен қызметтерін асыра немесе теріс пайдалану мүкіндігі артқанын байқауға болады. Қылмыс көп жағдайда әлеуметтік құбылысы болғандықтан, теріс пиғылды адамдардың заманауи техникалар мен ғылымдағы жетістіктерді қылмыстық пиғылдарына қолдану жүйесі кең тарап отыр. Ол дегеніміз, теріс пиғылды адамдардың заңға құрметпен қарайтын адамдармен әділ бәсекеге түскенде, біріншілердің байлық пен өмірлік құныдылықтарға қылмыстық пиғылмен қол жеткізуінде. Ол туралы, криминология ғылымы қылмыскер тұлғасын зерттеу бқлімінде кеңінен тоқталады.

 1839 жылы Франция полицейі Фрегер Г.А. өзінің «Қауіпті адамдар тобы және үлкен қала тұрғындары» атты еңбегінде қылмыскерлердің моральді топографиясын сүреттеген, соның ішінде қылмысты әлеуметтік құбылысқа теңеп, қоғамның әлжуаз топтарын, яғни әл-ауқаты төмен адамдар мен отбасыларын қылмыскерлер қандай қауіп төндірсе оларда сондай қауіп төндіреді деп өз тұжырымын берген.

 Біз зерттеп отырған мәселенің негізгі аспектісі де осы топтасып жасалған киберқылмыстарды ескертудегі және оларды ашудағы мәселелер болатын. Киберқылмыстарды қылмыстық топ құрамында жасау кезде олардың құрылымының негізгі белгілеріне ұйымдасқан топтың қылмыстарды қайталануы соның ішінде қауіпті қайталануымен (рецидив), жоғары ұйымдастырылуымен, топтық белгілерімен және қатаң иерархиялық тәртіптің болуымен, сонымен қоса топ мүшелерінің тығыз жеке қарымқатынасы (межличностное) деңгейінде құрылуымен айқындалады.

 Себебі, аталған киберқылмыстар күрделі жолдармен жасалып, қалдырылған қылмыстық іздерді табу мен бекіту тергеу органдары үшін процестік шешімін таппаған күрделі мәселе болып отыр.

 Салдарынан осындай қылмыстылықтардың латентті күйге түсіп, оларды ашу мен кінәлі тұлғаларды жауапқа тарту қылмыстық процестің міндеті өз құзыретінің қағидасына сәйкес жүргізе алмауына алып келуде. Бұндай құқықтық деформация азаматтардың конституциялық құқықтары мен бостандықтарына нұқсан келтіреді. Жалпы құқық қорғау органдарының киберкриминал топтардың алдында шарасыздығын байқатады, ол өз кезегінде құқық қорғау органдарына деген халықтың сенім білдіру индексациясын тым төмендетеді. Ол дегеніміз құқықты сыйлау және жария құқықтық қатынастар сбуъектілірінің құзыреті мен абыройына елеулі зиян келтіреді деп түсінеміз.

 Соған орай, киберқылмыстарды ескерту мен алдын алу мәселелеріне мемлекет пен құзыретті органдар тарапынан нәтижелі де әсерлі шаралар батыл қолданып, керек шешімдер дереу қабылдануы қажет. Осындай сипатта атқарылған жұмыстар негізінде киберкеңістікте жасалатын қылмыстық құқық бұзушылықтардың алдын алуды түбегейлі өзгерістер жасауға болады.

 Дегенмен айта кеткен жөн, қазіргі соңғы интернет құралдарын меңгеру көпшілік адамның базалық білімінің болуына қарамастан, үй жағдайында игеру мүмкіндігін байқатады. Ол дегеніміз киберқылмыстық құқық бұзушылықтармен арнайы ұйымдасқан топтар ғана емес жеке тұлғаларда айналысу ықтималдығы бар екенін түсінеміз. Қазіргі жаңдайда әлем бойынша, соның ішінде Орта Азия елдеріне киберкриминал ұйымдасқан топтардың интернет желілері мен құралдарын пайдаланып хаккерлік шабуылдар (хакерская атака) жиі жасалынып жатқанын байқап отырмыз. Ол туралы статистикада көңіл көншітпейді, сол себепті болса керек Қазақстан Республикасының Президенті Қасым-Жомарт Тоқаев Қазақстан Республикасының Киберқалқан (Кибершит) мемлекеттік бағдарламасын бекіткен болатын.

Қазақстан Республикасының Ұлттық қауіпсіздік комитетінің арнайы сайтында келесідей ақпарат ұсынылған: «Киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқалқаны») (бұдан әрі – Тұжырымдама) Қазақстанның әлемнің ең дамыған 30 мемлекетінің қатарына кіруі жөніндегі «Қазақстан-2050» стратегиясының ұстанымдарын ескере отырып, Қазақстан Республикасы Президентінің «Қазақстанның үшінші жаңғыруы: Жаһандық бәсекеге қабілеттілік» Жолдауына сәйкес әзірленді.

Осы Тұжырымдаманы орындау қазақстандық қоғамды одан әрі жаңғыртуға қызмет етеді және Қазақстанның БҰҰ жаһандық киберқауіпсіздік бағдарламасын іске асыруға қосқан үлесі болады”,- делінген.

Осыдан-ақ байқауға болады, еліміздің бүкіл әлем алдындағы міндеттемелерімен қатар ел қауіпсіздігі үшін ел азаматтары алдындағы жауаптылығын.

Киберқылмыстардың алдын алуда ақпараттық қамтамасыз ету бірінші орында тұр десем артық айтқаным болмас. Соңғы кездері киберқылмыстар қашықтықтан жасалып, видеобайланыс немесе телефон арқылы жасалып жатқаны белгілі. Осындай қылмыстардың жиіліп кеткені бәрімізге мәлім. Енді оның алдын алу үшін барлық құқық қорғау органдары мен Ақпарат және коммуникациялар министрлігінің негізі міндеті болып табылады.

Азаматтарға киберкеңістікте жасалатын киберқылмыстарға қарсы тұру үшін сандық технологиялар мен IT-технологиялар саласында білімін жетілдіру парыз. Себебі барлық киберқылмыстар интернет пен гаждеттер арқылы жасалуда. Соңғы уақытта дамып келе жатқан жасанды интеллект жұмысы да адам баласына қауіп төндіруде. Соның ішінде киберқылмыстардың көбеюуіне әкелуде. Хакерлік шабуылдар белгілі бір бағдарламаларды жою мен қатар ақпараттарды ұрлаумен айналысады. Бұл дегеніміз ұлттық қауіпсіздігімізге қауіп төндіріп тұр. Соның шінде азаматтардың дербес деректеріне де қол сұғылып, биометрикалық дерктерге де қол жеткізу қауіпі бар. Биометрикалық деректерге қол жеткізу сол адамдардың атынан мәмілелер мен банктік қарыз (займ) шарттары рәсімделген қылымыстық оқиғалар тіркелуде. Бұл дегеніміз банк жүйесінің де киберқылмыстарға қарсы тұру бағдарламасын жасауды немесе өзінің жүйесін құруды талап етеді. Себебі алдағы күндері киберқауіпсіздік өз деңгейінде болмаса, азаматтардың банкте сақталған жинақтары бір күнде жоқ болукы мүмкін. Әрине оның алдын алуда, арнайы шарттар мен талаптар бар. Бірақ ол талаптар қазіргі таңда аздық етеді.

Сол үшін барлық құқық қорғау органдары өзара тығыз іс-қимыл жасап, күдікті деген интернет сайттар мен шлюздер жабылуы тиіс.

Қорыта келгенде киберқылмыстарды тергеу және олардың алын алу бір мемлекеттің ғана мүддесі емес, бүкіл әлемнің алдында тұрған глобалды мәселе.

**Әдебиеттер тізімі**

1. Қазақстан Республикасының қылмыстық кодексі 3 шілде 2014 жылы No 226-В ЗРК.
2. ҚР Ұлттық қауіпсіздік комитеті, 2024 жыл [Киберқалқан](https://www.gov.kz/memleket/entities/knb/activities/250?lang=kk)
3. Об утверждении Плана мероприятий по реализации Концепции кибербезопасности («Киберщит Казахстана») до 2022 года

Постановление Правительства Республики Казахстан от 28 октября 2017 года No 676

1. Журнал предупреждение преступности № 3 2014 жыл.
2. Нормативные постановление верховного суда РК.
3. Криминология изд. «Юрист» г. Москва, профессор В.Е. Эминов